ISCTE IUL

Instituto Universitário de Lisboa

Departamento de Ciências e Tecnologias da Informação

USING KERBEROS

FOR ENTERPRISE CLOUD AUTHENTICATION

Ronivon Candido Costa

Dissertation presented in partial fulfillment of the Requirements for the Degree of
Master in Information Systems Management

Supervisor
Doutor Professor Carlos José Corredoura Serrão
Assistant Professor

December 2013

Instituto Superior de Ciências do Trabalho e da Empresa
Departamento de Ciências e Tecnologias da Informação

USING KERBEROS FOR ENTERPRISE AUTHENTICATION IN THE CLOUD

Ronivon Candido Costa

Dissertation presented in partial fulfillment of the Requirements for the
Degree of
Master in Information Systems Management

Supervisor
Doutor Professor Carlos José Corredoura Serrão

December 2013

Abstract: The Kerberos authentication protocol has a maturity of approximately thirty years, being widely used in IT systems in the corporate environment, mainly due to its adoption by Microsoft in its operating systems. Moreover, the practical application of the Cloud computing and its concepts is in its early days regarding its adoption by organizations, especially the large companies. This study aims to investigate the practical applications of the Kerberos protocol for authentication of enterprise applications deployed in the cloud, looking from both the functional and security perspective. To achieve this goal, it will be necessary to evaluate its applicability to the Cloud and assess whether it keeps the security characteristics found when using it only inside the corporate network.

Resumo: O protocolo de autenticação Kerberos apresenta uma maturidade de aproximadamente trinta anos, sendo amplamente utilizado nos sistemas de TI no meio corporativo, principalmente devido à sua adopção pela Microsoft nos seus sistemas operativos. Por outro lado, a aplicação prática dos conceitos de computação na nuvem encontra-se nos seus primeiros passos no que diz respeito à adopção pelas empresas, principalmente as de grande porte. Este estudo propõe-se a investigar as possibilidades práticas do protocolo Kerberos para autenticação de aplicações corporativas implementadas na nuvem, do ponto de vista funcional e de segurança. Para alcançar esse objectivo, será necessário avaliar sua aplicabilidade à nuvem e fazer um levantamento para validar se o protocolo mantêm as características de segurança encontrada quando utilizado somente na rede corporativa.

DEDICATION

To

Casimiro and Maria Moreira,
my parents,

who started it all long time ago.
I will be forever grateful to them…

To my son, Jean Vitor,
Who provides me with inspiration to learn…

And to my two jewels and the most important ladies in my life,
Karina and Maria Luísa.

Table of Contents

1 Introduction ....- 1 -
2 Review of the State of the Art in Kerberos Corporate Authentication ....- 5 -
2.1 Definition of Cloud ....- 5 -
2.2 Cloud Computing Use Cases ....- 7 -
2.3 Authentication and Identity in the Cloud ....- 10 -
2.4 Kerberos Network Authentication Protocol ....- 12 -
2.4.1 How does Kerberos Works? ....- 12 -
2.4.2 How Secure is Kerberos? ....- 14 -
2.4.3 Authentication Using Kerberos APIs and GSS-API ....- 16 -
2.5 Single Sign-On Taxonomy ....- 17 -
2.6 Cloud Security ....- 18 -
2.7 Security Assessment and Evaluation for the Cloud ....- 20 -
2.8 The Software for the Use Cases ....- 22 -
3 Defining the Scope and the Methodology ....- 25 -
3.1 Kerberos for Enterprise Authentication in the Cloud Use Cases ....- 29 -
3.2 The Use Cases (Models) ....- 32 -
3.3 The Security Assessment ....- 35 -
3.4 The Metrics ....- 38 -
3.5 Laboratory Setup for the Use Cases ....- 42 -
4 Results and Discussion ....- 45 -
5 Conclusions and Future Work ....- 53 -
Bibliographic References ....- 57 -
Annex A – Kerberos-compatible Applications ....- 61 -
Annex B – STAR Report - Baseline Model ....- 64 -
Annex C – STAR Report: Cloud Use Case 1 ....- 68 -
Annex D - STAR Report: Cloud Use Case 2 ....- 72 -
Annex E - STAR Report: Baseline Model After Migration ....- 76 -
Annex F – OpenVAS Assessment Reports ....- 78 -
E1 - 10.0.4.1 - Default router for the tenant in the Cloud ....- 78 -
E2 - 10.0.4.6 - Corp WebPortal in the Cloud, tested from malicious tenant ....- 80 -
E3 - 10.100.100.1 – Corp internal DMZ router, tested from the Intranet ....- 81 -
E4 - 85.243.111.91 - Corp WebPortal in the Intranet, tested from the Internet ....- 83 -
E5 - 192.168.1.254 – Corp External DMZ router, tested from the Intranet ....- 84 -
E6 - 192.168.56.142 – Corp default router, tested from the Intranet ....- 85 -
E7 - Appsrv.corp.intranet - Application Server in the Intranet tested from the Intranet ...- 86 -
E8 - Appsrvcloud.corp.intranet - Application Server in the Cloud, tested from the Intranet - 87 -
E9 - Appsrvcloud.corp.intranet – Corp AppServer Server in the Cloud, tested from a Malicious Cloud tenant ....- 88 -
E10 - Cloud0.dyndns-web.com/dashboard – Cloud Dashboard tested from the Internet .- 89 -
E11 - Cloud0.dyndns-web.com/Corp - Corp Public WebPortal tested from the Internet .- 90 -
E12 - Kdc2k8.corp.intranet – Corp Kerberos Distribution Center tested from the Intranet - 91 -
E13 - 10.100.100.123 – Corp Public WebPortal in the Corp Network tested from the

Intranet - 92 -
E14 - Win2k8clt.corp.intranet – Corp User’s workstation tested from the Intranet ..- 93 -
E15 - win-rodc.corp.intranet – Read-Only Domain Controller in the Cloud tested from the Intranet....- 94 -
E16 - win-rodc.corp.intranet – Read-Only Domain Controller in the Cloud tested from a Malicious Cloud tenant ....- 96 -

Index of Tables

Table 1: Taxonomy of SSO systems and its properties ....- 18 -
Table 2: rav Related Concepts....- 39 -
Table 3: Security metrics compared for all Models ....- 47 -
Table 4: Porosity....- 47 -
Table 5: Limitations....- 48 -
Table 6: Description of Mapping OSSTMM x OpenVAS....- 48 -
Table 7: Mapping OSSTMM x OpenVAS....- 48 -

Index of Figures

Figure 1: Cloud Service Models and Implementation Strategies....- 7 -
Figure 2: Use Case 3.2 - Enterprise to Cloud to End User....- 9 -
Figure 3: Use Case 3.3 - Enterprise to Cloud....- 9 -
Figure 4: The Kerberos Protocol....- 14 -
Figure 5: Intranet Model (Baseline)....- 25 -
Figure 6: Enterprise to Cloud Model....- 26 -
Figure 7: Kerberos Over the Internet ....- 27 -
Figure 8: Point-to-Point VPN....- 28 -
Figure 9: Lan-to-Lan VPN ....- 28 -
Figure 10: Enterprise Authentication in the Cloud – Kerberos Use Case 1....- 30 -
Figure 11: Enterprise Authentication in the Cloud – Kerberos Use Case 2....- 31 -
Figure 12: Cloud Exposed Surface - Visual Representation ....- 33 -
Figure 13: OSSTMM Process Flow ....- 38 -
Figure 14: Making a rav from a security test ....- 40 -
Figure 15: Exploring Attack Surfaces ....- 50 -
Figure 16: Exploring Internal Attack Surfaces....- 50 -
Figure 17: Reducing Porosity by Farming Out Resources....- 51 -
Figure 18: The Architecture and Attack Vectors ....- 65 -
Figure 19: The Architecture and Attack Vectors ....- 69 -
Figure 20: The Architecture and Attack Vectors ....- 73 -

ACKNOWLEDGMENTS

Working in a project such as this one is mostly an introspective journey, it is the time we must look inside ourselves to extract the results of years of living experiences, which started dozens of years ago in high school, and kept growing through the college, work, travels… It is also the time we must be humble, forget what we know, and be open minded to search for and find better explanations, better solutions, recognize that other solutions and explanations as being better, and improve ourselves from this new experience.

Through this journey, I lived this experience, and even though the journey is mostly a lonely walk, we have to walk that path. When we don't know it, we need someone to point it to us. When we know the path but realize is too rough, we may be lucky enough to have someone to make it soft, cleaner and well-lighted so to make it walkable and even pleasant. When all of this is gone, and you think there is no reasons anymore to keep walking the path, then you remember that, no matter that everything else is gone there will be always someone somewhere that deserves you dedication, will always recognize your effort and be proud of all the work you have done. So, we keep walking the path, and we finally see the end of the road.

I want to acknowledge the person who has pointed me the path when I did not know it, and believed in my project since day one when it was still a rudimentary idea, and gave me all the support and assistance to make it a quality work. For all of this valuable contributions, I am sincerely grateful to my thesis supervisor, the Professor Carlos Serrão.

I want to acknowledge the person who made my path walkable. This person has supported me with comprehension, patience and understanding all the hours I had to spend by myself, researching and writing, during endless nights and weekends. Thanks to my lovely wife, Karina Silva.

I want to acknowledge the person who, even without knowing it, has been ultimately, the reason I am doing this. They are the person that will always recognize and be proud of my accomplishments. I believe that every father wants to be a mirror to his sons, and I am no exception. I believe that my father and mother also share this feeling, and I want let them know that I embrace this belief, that I accept them as my mirror, and I want to be just like they are: pure, simple, generous, dedicated to their family. Thank you Casimiro and Maria Moreira, my father and mother, for everything you made possible in my life. I truly hope I can give you back enough in this life.

And last but not least, I want to thanks Jean Vitor, my son, for being such a good boy, for giving me the reasons to try to be a better father every day, and the person for whom I try to be an example of life.

1 Introduction

The Kerberos authentication protocol offers a maturity of approximately thirty years, being widely used in the corporate environment IT systems, mainly due to its adoption by Microsoft in its operating systems (Foley 2010, De Clercq 2004, p. 133). Parallel to that, the practical application of the Cloud computing concepts is beginning to spread around companies.

This work proposes to investigate the practical possibilities of using the Kerberos protocol for authentication into enterprise applications hosted in the Cloud, from a functional and security perspective. To achieve this goal, it is necessary to identify real practical scenarios in today's intranet-based applications that make use of Kerberos, propose use cases for equivalent services in the Cloud and assess its security to validate the models according to acceptable security and functional standards. This validation methodology will provide enough evidences that the models are secure enough for corporate adoption.

One of the main features of the Kerberos protocol is its capability to provide single sign-on inside a trusted domain, making it possible to provide users with better user experience when using several different applications by reducing the number of logons required during a work day or work session. The single sign-on feature will be one of the central points in this work, which must be viable in all models that will be eventually proposed and implemented during the validation phase.

Traditionally, integration of enterprise services with Cloud services have been approached using Federated Authentication[1], mainly using the SAML protocol (OASIS 2005) and more recently with OAuth (IETF 2010) and OpenID (OPENID 2012). While there is nothing wrong with these approaches, it is focused on integrating applications using APIs and other methods such as Web Services, and is not appropriate to all types of applications mainly because these protocols will require changes in the existing applications or the development of new components (interfaces) between them.

The approach of this work is to analyze existing applications in the enterprise that are using Kerberos for authentication, understand which ones can be migrated to a public Cloud, and have them working as they were before the migration in a transparent manner. In this

[1] Federated authentication and the related protocols (SAML, OAuth and OpenID) are discussed in chapter 2.

work, it will not be considered the development of new software, neither the modification of any existing application. The main goal is to understand how security is affected when moving applications from one environment to another, and to accomplish this objective, the applications must be kept unchanged. Therefore, most (if not all) changes in the security characteristics will be due to environment changes and not due to application changes.

The difficulty in analyzing complex systems security is recognized in this work, as well as the problem of analyzing one contained, controlled model and later try to generalize the results to other systems. The metrics resulted from a security assessment carried out over a specific environment will not correctly represent the security of any other environment due to their specifics characteristics. At the same time, comparing assessments of different environments may be a problem, since there must exist a methodology that will adequately support this process. In this current work, these issues were addressed, and the security metrics obtained from the assessment of different environments are subsequently related to each other by means of a security gap indicator, which will provide data to decision makers about the viability of Cloud adoption in terms of security properties.

The security properties of an environment are affected by every one of its individual components (Yildiz et al, 2009), and according to this definition, the move of one component from one site to another will change both site’s security properties, since the moving component will take with itself its security strengths or weaknesses to the destination location. The moving component (target) will benefit from a more secure environment, or lessen from it, following the location tendency to have more or less security.

The above concept can be generally expressed by the following metaphor: There are three safes, each one protecting valuable assets: Gold, Silver and Bronze. There is not enough space in the owner’s house to store all three safes, so the owner will have to rent space somewhere to store one of the safes. The decision about which safe will be stored in the rented space must be based on:

a) the importance of its contents;
b) how well protected it is now;
c) how well protected will it be in the new place.

The public knowledge of a safe existence and place of storage is a risk factor, and therefore should be avoided. For example, if is brought to a thief knowledge about the existence of a safe full of valuable assets made of bronze stored in a given place, all of the other two safes will also be at risk of being stolen since they are all stored in the same physical location. If the safe with bronze assets is stored in different location, and someone tries to steal its contents, the other two safes will not be at risk.

The presented metaphor illustrates three other concepts used in this work (chapter 3 and 4), which are:

- Risk transfer;
- Improved security by limiting the number of visible targets;
- Influence of the surrounding environment over the asset's security.

The influence of the surrounding environment over the assets is the main reason why it was chosen to calculate and use the delta of the security between two models, instead of the actual security metrics of each environment. Using a delta (that is, a positive or negative percentage value relative to the baseline security metric) will more clearly show how much the security will benefit or be compromised after the changes since it make it possible to have an exact perception of the security difference derived from that environment's influence. Therefore, the method used in this work will result in a percentage value, which will be the final metric to ultimately take the conclusions about how security is affected after migrating services to the Cloud. This percentage can therefore, be applied by different organizations, or by the same organization in different projects when evaluating the viability of moving resources to that Cloud. The metric is valid only for that Cloud, but different assessments can be performed for other Cloud infrastructures for comparison[2].

Protecting the containers of important information is a critical rule and should not be disregarded but the Kerberos protocol also protects the interactions between users and the services using encryption. The encryption is carried out using tokens generated after a first authentication with an authentication service, and these tokens will persist in the computer disk until renewed or deleted. Kerberos tickets must be protected, and this should be accomplished by protecting the computers where they are stored (Garman 2003, p.102).

[2] The concepts introduced here will be explored in more details in chapters 2 and 3.

2 Review of the State of the Art in Kerberos Corporate Authentication

In this chapter, the assessment of the most relevant scientific and professional contributions in the field of study is presented. Some objectives to be investigated have been defined, namely, how Kerberos can be used by organizations when they move their applications to the Cloud, and the security properties of these new scenarios. Given these objectives, it is possible to identify the subjects and technologies that will be reviewed in the literature during this chapter:

- The Kerberos authentication protocol;
- The use of Kerberos in organizations (some use cases);
- The use of Kerberos in the Cloud (some use cases);
- Security assessment methodologies.

2.1 Definition of Cloud

The National Institute of Standards and Technology (NIST) is an organization that reports to the U.S Department of Commerce and is responsible for developing standards and guidelines to be used by Federal agencies. These documents are openly published and can be accessed by interested parties, including public and corporative use. The NIST Special Publication 800-145, “The NIST Definition of Cloud Computing” (NIST 2011), defines Cloud computing:

> *“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model is composed of five essential characteristics, three service models, and four deployment models.”*

The five essential characteristics of a Cloud according to NIST are (NIST 2011, p. 2):

- On-demand self-service. The resources as allocated by the user, without the provider's assistance or interference.

- Broad network access. The resources are used remotely, with the users connecting to them through a network, including the Internet in some models.
- Resource pooling. Users consume resources from a pool of shared resources. Users have the feeling that the resources are infinite.
- Rapid elasticity. Additional capacity can be added or removed from existing resources. This will help Cloud solutions to keep up with high demands, and decrease with low demand.
- Measured service. Cloud models usually charge by the minute. Also, users can suspend the use of Cloud services at any time. This characteristic imposes the requirement to measure the consumption of services to correctly charge for its use.

The three service models of Cloud computing according to NIST are (NIST 2011, p. 2-3):

- Software as a Service (SaaS). In this model, the service provider publishes a catalog of applications, which run on the provider's infrastructure.
- Platform as a Service (PaaS). The provider publishes a catalog of tools, programming languages and services running in their infrastructure. Customers can develop their own applications using these supported resources and services.
- Infrastructure as a Service (IaaS). This is the most flexible of the Cloud models, but also the one which will require the most knowledge from the consumer as the service provided is a pool of physical and virtual resources that can be allocated by the users to implement their own operating systems and applications. "*The consumer does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).*" (NIST 2011, p. 3).

Cloud computing can be deployed according to four models (NIST 2011, p. 3):

- Private Cloud. Usually devoted to a single organization and its internal departments. Can be deployed using the company's internal or external resources.
- Community Cloud. Deployed by one or more organizations and shared between other organizations with similar objectives and policies.
- Public Cloud. The Cloud resources are available to the general public. The infrastructure can be owned by a public enterprise or other organization.

- Hybrid Cloud. Hybrid Clouds are an aggregation of two or more of the others Cloud models that are interconnected to accomplish specific objectives.

Figure 1 illustrates the Cloud models (on the left) and implementation strategies (on the right) as defined by NIST.

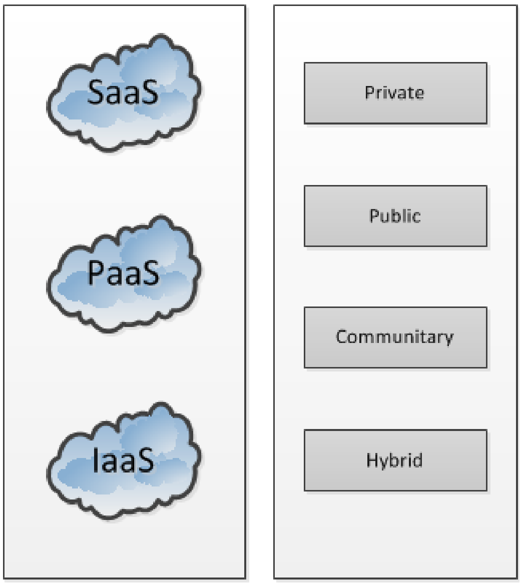


Figure 1: Cloud Service Models and Implementation Strategies

2.2 Cloud Computing Use Cases

Cloud Computing permits the implementation of different possible use cases, involving the organization and its employees, partners, customers, and others. The Cloud Computing Use Case Discussion Group (CCUCDG 2010) (which is a work in progress) has produced a series of possible different scenarios for Cloud usage, ranging from customers to the organization point of view. This group addresses the importance "*to highlight the capabilities and requirements that need to be standardized in a Cloud environment to ensure interoperability, ease of integration and portability*" (CCUCDG 2010, p. 4), which should be implemented using open source and standard technologies. The use cases presented were not supposed to represent only existing scenarios, but also to anticipate future scenarios and even technologies required to implement them.

The scenarios are classified using the following groups (CCUCDG 2010, p. 18-19):

- End User to Cloud

- Enterprise to Cloud to End User
- Enterprise to Cloud
- Enterprise to Cloud to Enterprise
- Private Cloud
- Hybrid Cloud

A series of practical case studies are revealed (denominated “customer scenarios” by the authors) where actual experience using some of the Cloud use cases are detailed in terms of problem solved, requirements and capabilities, and finally the portability concerns (CCUCDG 2010, p. 33-39).

This current work can be mapped to two of the scenarios presented in (CCUCDG 2010), namely use case “3.2 Enterprise to Cloud to End User” (CCUCDG 2010, p. 20) (Figure 2) and use case “3.3 Enterprise to Cloud” (CCUCDG 2010, p. 23) (Figure 3). In the use case 3.2, enterprise applications are hosted on the Cloud, and can be accessed by both employees from inside and outside the company, and also by the enterprise’s customers via the Internet. In use case 3.3, the enterprise’s Cloud-hosted applications are integrated with the internal enterprise IT capabilities, but access to the Cloud applications are limited to users from inside the company. Both use cases shown in that scenario would provide the following characteristics (CCUCDG 2010, p. 23-24):

- *Using Cloud storage for backups or storage of seldom-used data*
- *Using virtual machines in the Cloud to bring additional processors online to handle peak loads (and, of course, shutting down those VMs when they're not needed anymore)*
- *Using applications in the Cloud (SaaS) for certain enterprise functions (email, calendaring, CRM, etc.).*
- *Using Cloud databases as part of an application's processing. This could be extremely useful for sharing that database with partners, government agencies, etc.*

As it is possible to observe both in Figure 2 and Figure 3, both scenarios are similar. However, scenario 3.2 adds up the external access capability to resources within the Cloud. Therefore, scenario 3.2 and 3.3 share the same characteristics regarding to the internal capabilities, while scenario 3.2 has some additional capabilities, which is to provide external access to the enterprise resources via the Internet.

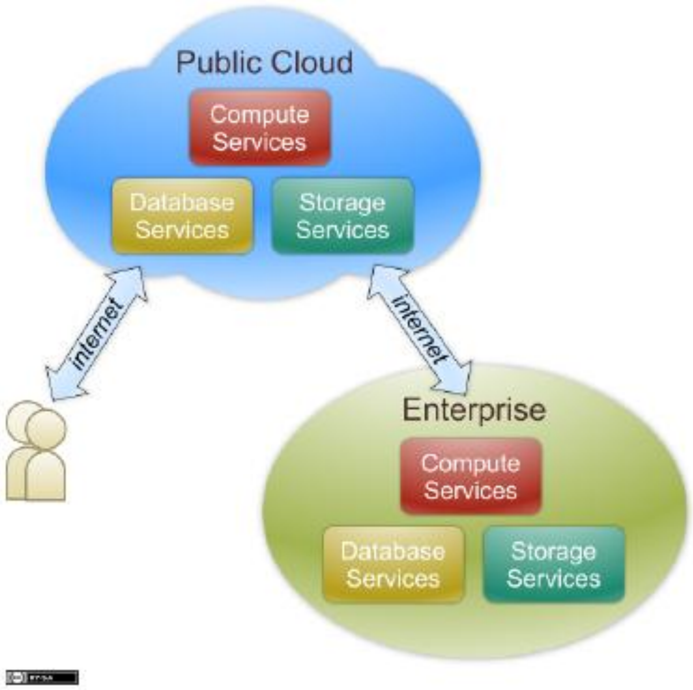


Figure 2: Use Case 3.2 - Enterprise to Cloud to End User
(Source: CCUCDG 2010, p. 21)

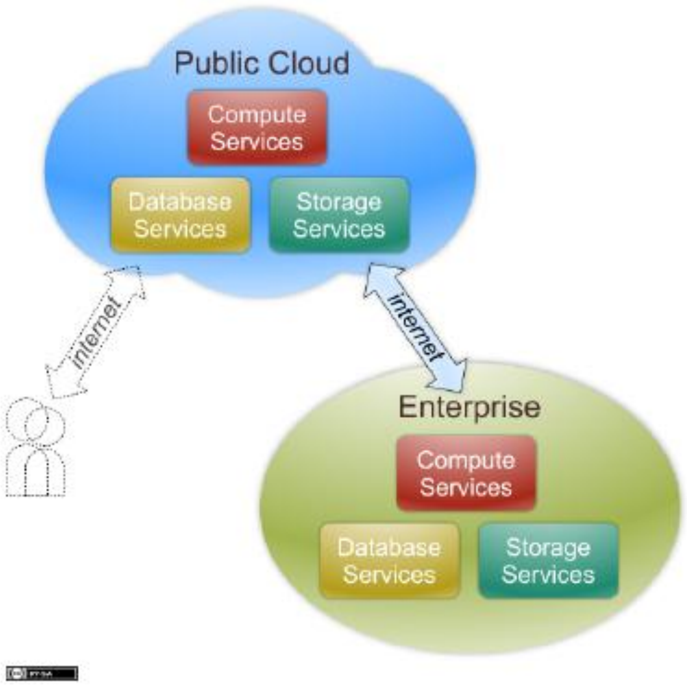


Figure 3: Use Case 3.3 - Enterprise to Cloud
(Source: CCUCDG 2010, p. 23)

2.3 Authentication and Identity in the Cloud

Authentication in Information Systems has in the multitude of services, accounts and users the main challenge to provide the right service to the right person with an acceptable level of security. Several open standard authentication protocols have been developed to address these challenges, such as SPML (OASIS 2006), SAML (OASIS 2005), OAUTH (IETF 2010) and OPENID (OpenID 2012). Although these protocols address specific needs in an enterprise to Cloud scenario, all of them have also specific requirements and applications.

In order to deploy a solution using any of the above mentioned authentication protocols, one must have to develop specific code to glue existing systems in terms of authentication and secure user information exchange. These protocols were created to allow developers to design new applications that can securely exchange identity information over the web, and also, to allow the existing ones to be changed, adapted and make them compatible with the new paradigm of a global interconnected network of users, services and applications.

The need to change applications may decrease as these protocols become widely acceptable and more applications are developed from scratch to support them. Such characteristics are already present in the Kerberos protocol.

In his doctorate thesis, Daniels, (2011) says that "*identity management technologies are not mature and cause security concerns among Cloud computing adopters*", at same time that he recognizes that "*virtualization and Cloud computing technologies have established themselves in the enterprise architecture environment*". Although the two arguments seem contradictory, the later is an undeniable fact verified by the number of companies that provide Cloud services backed by virtualization, such as Amazon, Google, HP, IBM, Microsoft, Rackspace, Salesforce.com and others.

In his work, Daniels (2011) has focused on assured identity in the Cloud, taking this principle as mandatory in order to allow the enterprises to consume and provide services in a secure way. One of the problems introduced by the author is "*how can identity and access management controls be designed to support Cloud computing systems*", where some points covered includes "*How do we determine who is authorized to be on the Cloud*" and "*How do we interoperate with different identity and access mechanisms in a global enterprise?*".

To answer those questions, Daniels (2011) designs use cases to describe the systems behavior under analysis, validated by SysML diagrams[3] and tested using a prototype system AIMS (Assured Identity Management System). That study concludes with a series of SysML artifacts, also called by the author as Uses Cases, to be used as templates by organizations as a starting point for consuming Cloud infrastructures with a security mindset (Daniels 2011, p. 147-148).

The Organization for the Advancement of Structured Information Standards (OASIS) has produced a standard-candidate (not yet approved) entitled “Identity in the Cloud Use Cases Version 1.0” (OASIS 2012) to approach the subject identity and authentication for the Cloud. In that document, several use cases are identified, and the Use Case 11 (Enterprise to Cloud Single Sign-On) and Use Case 15 (Access to Enterprise’s Workforce Applications Hosted in Cloud) should be highlighted as being relevant to this work.

The Use Case 11 describes the capabilities desired by users who want to login into the corporate network, and later consume both services hosted inside the company and on the Cloud. The aspects and categorizations of systems needed to accomplish this use case involve Authentication, Federated Identity Management, Single Sign-On (SSO), Cloud Application Identity Federation Services, and Cloud Application Authorization Services among others (OASIS 2012, p. 41-42).

The second use case related to this work is Use Case 15, which disclaims about the enterprise users accessing browser-based and API-based applications deployed on the Cloud. Two scenarios using Kerberos are derived from this Use Case, “Scenario 1: Enterprise Employee Outbound”, targeted for employees authenticated with the internal Authentication Service (AS), and “Scenario 2: Consumer/customer (Inbound into Enterprise-run service)”, targeted for external customers that are authenticated by an external AS. (OASIS 2012, p. 51-53).

It is important to note that the use cases presented by OASIS are part of an unfinished work; the open specifications are still subject to further evaluation and in most part describe specifications that still need to be implemented, or changes to be made in current protocols in order to achieve the desired goals.

The problem of identity and trust between Cloud environments are also approached in (Casola et al, 2010), where the authors discuss the challenge of interconnecting different

[3] SysML (Systems Modeling Language, SysML) is a general purpose modeling language for systems engineering applications. It extends Unified Modeling Language (UML) as a profile (dialect). Source: http://www.sysml.org/

Clouds while minimizing security issues, and recognize the fact that the trust relationship mechanism between Clouds are complex, and at same time, a necessary step in such scenarios. Taking into consideration that such tasks are currently manual, which goes against a fundamental characteristics of Cloud computing, the paper proposes a solution based on identity federation and digital certificates.

2.4 Kerberos Network Authentication Protocol

According to the Internet Engineering Task Force (IETF) draft RFC4120 (IETF 2005) which defines the specification of the Kerberos Network Authentication Service version 5 and (Garman 2003), the Kerberos model has emerged as a research project at Massachusetts Institute of Technology (MIT) in the early 1980s. The protocol was based on a previous work of Needham and Schroeder entitled "Using Encryption for Authentication in Large Networks of Computers" (Needham and Schroeder 1978) with the modifications proposed by Denning and Sacco in their paper "Timestamps in Key Distribution Protocols" (Denning and Sacco 1981).

Kerberos was developed to overcome a number of issues at that time, most notably, passing passwords and sensitive data over an unsecure network as clear text. Kerberos can be defined as a Network Authentication Protocol that "*provides a secure, single-sign-on, trusted, third-party mutual authentication service*" (Garman 2003).

2.4.1 How does Kerberos Works?

Kerberos is an authentication protocol developed in the 80s that uses symmetric key encryption (the same encryption key is used to encrypt and decrypt messages between a client and a server). The authentication process is based on the fact that if the server can decrypt a client's message, and the message results in the client name with little (acceptable) time offset compared with the server's own clock, the server will believe the client is really who it says it is, because only the actual client could have encrypted that information (De Clercq 2004, p. 139-140). There is a very important assumption for this to hold: the encryption key K is only known by the client and the server, which constitute a challenge in the protocol implementation, since the encryption key must be shared between both entities before an authentication communication could even start.

Kerberos uses a third-party entity to provide initial keys to clients, named Kerberos Distribution Center (KDC). KDCs are used to generate keys for all entities that want to consume services in a domain, and they must be trusted by all service providers in that domain. KDCs also allows for scalability, otherwise the number of keys would be unmanageable in a large environment with hundreds or thousands of users that need to communicate with everyone else (De Clercq 2004, p. 141).

All communications between the parts are encrypted using shared keys. There is a special key, the Master key, which is used by the KDC to encrypt the initial logon session. A successful logon process will result in a new key, Ticket Granting Ticket (TGT) that will be used to protect further communication with the KDC (such as to request new tickets for services). The TGT will reduce the use of the master Key on the network, and have a relatively short life span, which helps protecting against brute force attacks to crack the ticket (De Clercq 2004, p. 142-149).

The Kerberos protocol is specified as follows (De Clercq 2004, p. 150-151):

Phase 1: Authentication Service Exchange (occurs once for every logon session)

Step 1: Authentication Server Request (KRB_AS_REQ). Alice logs on to the domain from her local machine. A TGT request is sent to a KDC.

Step 2: Authentication Server Reply (KRB_AS_REP). The KDC returns a TGT and a session key to Alice.

Phase 2: Ticket-Granting Service Exchange (occurs once for every resource server)

Step 3: TGS Request (KRB_TGS_REQ). Alice wants to access an application on a server. A ticket request for the application server is sent to the KDC. This request consists of Alice's TGT and an authenticator.

Step 4: TGS Reply (KRB_TGS_REP). The KDC returns a ticket and a session key to Alice.

Phase 3: Client-Server Authentication Exchange (occurs once for every server session)

Step 5: Application Server Request (KRB_AP_REQ). The ticket is sent to the application server. Upon receiving the ticket and the authenticator, the server can authenticate Alice.

Step 6: Application Server Reply (KRB_AP_REP). The server replies to Alice with another authenticator. On receiving this authenticator, Alice can *authenticate the server.*

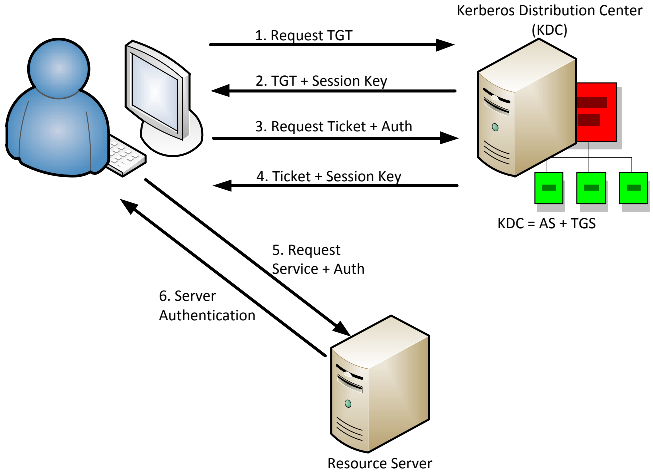


Figure 4: The Kerberos Protocol

(Source: De Clercq 2004, p. 151)

The above description (Figure 4) presented the authentication process for a single domain. However, Kerberos supports multi-domain scenarios with delegated authentication when the different domains have a trust relationship between them. That means that any user from a domain A can consume services from domain B as long as A and B trust each other. The domain administrators must establish this trust relationship once, and all users will benefit from it thereafter.

2.4.2 How Secure is Kerberos?

Kerberos security has been formally analyzed in a series of previous papers for its security properties (Tsay 2008, Bella and Riccobene 1997, Butler et al 2006). "*These methods allowed us to prove numerous properties of Kerberos 5, in particular authentication, confidentiality and structural soundness, hence confirming that it is a robust and well-designed protocol*" according to (Butler et al 2006, p. 84). Equally positive feedback was delivered by (Butler et al 2004) cited by (Backes et al 2006), which says that "*This analysis of Kerberos 5 showed that: a detailed specification of the core protocol enjoys the expected authentication and secrecy properties except for some relatively innocuous anomalies*".

Despite the conclusion from the above-mentioned investigation, Kerberos has in fact some security issues. The protocol can be attacked using dictionary attacks, brute-force attacks, replay-attacks and Man-in-the-Middle attacks (Garman 2003, p. 103-109). Such attacks were very effective in Kerberos version 4, but version 5 has added features to mitigate these vulnerabilities, being the most noticeable (Garman 2003, p. 103-109) the following:

- The addition of stronger encryption such as RC4 and AES in replacement of the now weak DES. Due to the vast resources and time needed to break an 128 bits or higher AES key, dictionary and brute-force attacks are less likely to succeed;
- Pre-authentication, what forces the clients to prove their identity before issuing tickets. Kerberos 4 did not have this feature, consequently, any attacker could request a key for any valid client, and then try to break the key off-line;
- Addition of IP address field in tickets, time-based authenticators and replay cache on the servers prevents tickets from being used more than once, thus mitigating the replay-attacks.

A typical attack against several authentication protocols, including Kerberos, is the Man-in-the-Middle attack. Kerberos already has built-in defense against this type of attack by design, since only someone who knows what the encryption key is can open the encrypted tickets. Since all messages are encrypted using the destination’s key, only the legitimate user can read the messages. This process is used to implement a mutual authentication, where each part in a conversation must prove its identity before the actual conversation actually takes place by successfully encrypting and exchanging a small piece of information, such as the current time (Garman 2003, p. 109).

Apart from its proven security characteristics, Kerberos is an extremely successful and popular authentication protocol due to other characteristics and circumstances, such as its single sign on (SSO) capabilities and the fact that it was adopted as the default authentication protocol in Windows 2000 (De Clercq 2004, p. 133), which has helped with its wide spread adoption inside organizations all over the world. According to an IDC survey from 2009 cited by (Foley 2010), Windows Servers had the large market share with 73.9% participation in the world market. Considering that Kerberos is the authentication protocol native for all of those servers, it is therefore the most used authentication protocol nowadays.

Besides being a leader in the server market share (Foley 2010), and thus contributing to the dissemination of Kerberos, Microsoft has also released its Cloud platform named Azure which has among its characteristics the capability to integrate the authentication of

Cloud applications with on premises[4] Active Directory). Microsoft SQL Server, for example, is known to support Kerberos authentication (Microsoft 2012a) and can be deployed on Azure. Also, another set of official Microsoft documents (Microsoft 2012b, Microsoft 2012c, Microsoft 2012d) demonstrates how to deploy and integrate an Azure Active Directory with the enterprise Active Directory. The solution delivered by Microsoft allows for applications deployed on Azure to authenticate corporate users using existing credentials in the enterprise Active Directory. The authentication repository can be either on-premises, in the Cloud, or both (replicated from the enterprise internal Active Directory to an Azure replica). Such integration will have a positive side-effect of not requiring any changes to existing applications, which will keep working with Kerberos on Azure if it already had this characteristic when deployed on the enterprise internal infrastructure.

2.4.3 Authentication Using Kerberos APIs and GSS-API

Kerberos is an integral part of Windows servers, providing authentication services for the domain participants (that is, workstations and users), and can also be used to authenticate Microsoft applications such as Microsoft SQL Server (Microsoft 2012a, Microsoft 2013b). Applications developed for web servers and web portals can also benefit from Kerberos by simply enabling this feature on the Microsoft Information Services web server (Microsoft 2013a).

However, there is a whole different ecosystem of applications that are developed using different languages such as Java or C that can also take advantage of Kerberos for authentication and single sign-on. Such applications can use the existing Kerberos API[5], or instead, use a simpler, generic authentication API named Generic Security Service Application Program Interface (GSS-API). GSS-API is a specification that can be found on (IETF 2000), and it is a generic API for doing client-server authentication (faqs.org 2000).

GSS-API provides an optional, easier to use generic mechanism to authenticate with different authentication providers, thus minimizing the development effort and complexity by using a common API. Since most Kerberos distributions have available a GSS-API implementation, most applications that are said to support GSS-API will also support Kerberos (faqs.org 2000).

[4] On Premises means that the organization is using its own internal resources, for example, its own data center to host the applications.

[5] Application Programming Interface is a protocol intended to be used as an interface by software components to communicate with each other. (http://en.wikipedia.org/wiki/Application_programming_interface).

2.5 Single Sign-On Taxonomy

Before moving towards a Cloud model of single sign using Kerberos, it necessary to understand which are the models available for the enterprise intranet networks. One difficult step in this phase was to find empiric work about intranet single sign on solutions, although commercial solutions can be easily found and are well documented.

One important source of information relevant for this thesis was the work carried Pashalidis and Mitchell (2003) in their paper “A Taxonomy of Single Sign on Systems”. This paper provides some empiric work necessary to help classifying the SSO solutions. In their work, they identified four generic architectures for single sign-on (SSO), which will be used as a foundation for the practical intranet scenarios in this work.

The architectures, as defined by (Pashalidis and Mitchell 2003) are the following:

- Pseudo-SSO, in which the authentication is carried out by a system in behalf of the user, and has such a characteristic that allows (or force) the user to have a credential for every system.
- True-SSO, in which the Authentication Service Provider (ASP) becomes a fundamental part in the architecture, as well as the trust delegation principle. The ASP becomes a trusted third party, which has trusted relationship with the service providers (SP) that the user will be requesting services from.

Pashalidis and Mitchell (2003) later subdivide the pseudo-SSO and true-SSO into four main categories:

- Local pseudo-SSO systems;
- Proxy-based pseudo-SSO systems;
- Local true SSO systems;
- Proxy-based true SSO systems.

All local SSO schemas implies in a subsystem running on the user’s system, which will store a local copy (usually encrypted) of the credential database (local pseudo-SSO) or authenticate in behalf of the user (local true-SSO).

Proxy-based pseudo-SSO adds a remote component with a credential database. The user must first authenticate to the proxy, which will authenticate into the SP in behalf of the user using a set of credentials from its credential database. In a proxy-based true-SSO architecture, a remote third-party trusted component would act as the Authentication Service Provider (ASP), authenticate the user and provide a proof of authentication, which the user can send along its requests for services to SPs that maintain a trust relationship with the ASP.

Very important to our investigation is also the fact that (Pashalidis and Mitchell 2003) will further classify the Kerberos authentication protocol in the proxy-based true SSO category, which is the subject of the current study. Concluding the work, they also provide a matrix of properties for the identified SSO schemas, reproduced below.

	Local pseudo-SSO	Proxy-based pseudo-SSO	Local true-SSO	Proxy-based true SSO
Pseudonymity and Unlinkability	**cannot be guaranteed**	**cannot be guaranteed**	**can be guaranteed**	**can be guaranteed**
Anonymous Network Access	**needs additional services**	**can be integrated**	**needs additional services**	**can be integrated**
Support for User Mobility	**needs additional services**	**under suitable authentication method**	**needs additional services**	**under suitable authentication method**
Use in Untrusted Environment	**not supported**	**under suitable authentication method**	**not supported**	**under suitable authentication method**
Deployment Costs	**low**	**low**	**high**	**high**
Maintenance Costs	**potentially high**	**potentially high**	**low**	**low**
Running Costs	**low**	**high**	**low**	**high**
Trust Relationships	**dynamically changing**	**dynamically changing**	**concrete and consistent**	**concrete and consistent**

Table 1: Taxonomy of SSO systems and its properties
(Source: Pashalidis and Mitchell 2003, p. 262)

2.6 Cloud Security

Securing a Cloud infrastructure requires a new systems security perspective because it adds several new attack vectors to a traditional IT infrastructure.

Jensen et al (2009) analyses Cloud security issues focusing on its basic elements, such as the web browsers, encryption technologies and others standards such XML and Web Services. The author’s approach is to analyze individual components for its weaknesses in order to provide a big picture of Cloud security. The topics covered are Web Services security, TLS and encryption to provide secure access to Cloud resources, XML issues, browser security associated with Cloud authentication and others general concepts such as malware injection, spoofing adapter for Cloud and flooding to accomplish denial of services.

A more holistic approach is given by Yildiz et al (2009), proposing that Cloud security can be broken down in five layers, and covered both horizontal and vertical, dynamic policies, implemented with tools to automate the process of securing the Cloud. The five layers are the Network Layer, Processing host layer (Servers), Storage Layer, Systems Management Layer and Application Layer:

- Network layer must definitely be assessed for its security, since it is the main venue for all traffic with the Cloud.
- Processing host (Servers) must assure tenant[6] isolation at all levels (processing, memory, network and storage). This component will have the security assessment results provided by means of a SLA.
- Storage layer includes all data hosted in the Cloud, in the form of system images, and the enterprise data (including data at rest). The assessment for the Storage layer will have a component provided by SLA.
- Systems Management layer will be covered by SLA and by the enterprise processes. The SLA should cover aspects such as Virtual Machine availability and performance, but also security aspects such as intrusion detection events.
- Application layer is mostly the responsibility of the Cloud customer, not including the Management Interface (or Dashboard). The Cloud Dashboard is a very important application in this layer, and it is the Provider’s responsibility to ensure it is secure and available according to contracted SLAs.

A practical investigation of Cloud security was performed by a team of investigators in the paper “Analysis on Cloud-Based Security Vulnerability Assessment “ (Chung-li et al 2010). This team performed a series of standard tests in a Cloud base infrastructure, running the tests from inside and outside of the local network. The conclusion of the tests shown more vulnerabilities when the tests were performed from inside the network than from the outside. The tests were performed using the tools NMAP[7], Nessus[8] and Nikto[9].

[6] Tenant, in the context of Cloud computing, may be a customer or a consumer. Tenant is also defined as a “project” in the context of an OpenStack Cloud implementation (http://docs.openstack.org/trunk/openstack-compute/admin/content/users-and-projects.html).

[7] NMAP (“Network Mapper”) is an open source tool for network exploration and security auditing

2.7 Security Assessment and Evaluation for the Cloud

Systems security can be evaluated or it can be assessed. The former evaluates and ranks systems according to pre-defined assurance levels (Coelho 2007, p. 2) and may or may not imply in being further certified by a third party organization. Security assessments, on the other hand, can be seen as a tool to help identify and understand the organizations and its assets risk levels (NIST 2010, p. 1), and have no strict association with certification. Security assessment is a process to gather information, which can be used by the organization to accomplish several objectives such as assisting in identifying systems weaknesses and deficiencies and later prioritizing risk mitigation decisions (Coelho 2007, p. 3).

There are several evaluation, risk and assessment methodologies available, as well as guidance to improve systems security. In this section, an overview to some of these methodologies is provided, going in more detail for the ones that are suited for Cloud.

OWASP (2012) has started a new project denominated “Cloud-10 Project” to approach Cloud security risks. OWASP top ten lists are important because they help the enterprises to focus on the most serious web applications risks, and the Cloud-10 projects is a work in progress (Pre-Alpha) to address this new paradigm in enterprise computing. The risk “R2 – User Identity Federation” focuses on this important subject of managing identities across different domains once the enterprise moves their services to external Cloud providers, highlighting the importance of maintaining a single user repository in order to avoid multiple islands of identity data. OWASP top ten lists are maintained by a community of users and experts in every domain, and are ranked by criteria such as (OWASP 2012):

- Easily Executable
- Most Damaging
- Incidence Frequency (Known)

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a methodology for risk-based information security strategic assessment and planning that proposes to help practitioners to understand which are their assets risks, and once those risks

(http://nmap.org/book/man.html#man-description).

[8] Nessus is a vulnerability scanner for networks, systems, data and applications (http://www.tenable.com/products/nessus).

[9] Nikto is a vulnerability scanner for web servers (http://www.cirt.net/nikto2).

are identified, to help them build mitigation plans (Alberts and Dorofee 2001, p. 7). OCTAVE was designed for large organizations, although there is a version for smaller organizations (OCTAVE-S), and yet another method specifically for Information assets (OCTAVE Allegro).

OCATAVE Allegro is a risk assessment methodology organized in eight steps and four phases (Caralli et al 2007b, p. 5), which can be conducted in a series of workshops and supported by the guidance book, worksheets, and questionnaires that are included in the method. The methodology objectives are to establish risk measurement criteria (phase 1), identify and classify assets (phase2), identify threats (phase 4), identify and mitigate risks (phase 4) (Caralli et al 2007b, p. 4-5).

The OCTAVE Allegro methodology has eliminated the need to run vulnerability tests as part of the assessment process. This decision came due to the fact that such tests not always results in "*significant additional information that cannot be obtained through scenario identification*" (Caralli et al 2007b, p. 13). Also, with the introduction of the *relative risk score*, OCTAVE Allegro allows the comparison between different risks in the enterprise (Caralli et al 2007b, p. 14), thus facilitating the prioritization of risks that must be mitigated.

The Open Source Security Testing Methodology or OSSTMM (Herzog 2010) has its focus on operational effectiveness (Herzog 2011, p. 2). OSSTMM3 is an evolution from a penetration testing methodology (Herzog 2011, p. 2) which evolved to more than a best practices framework by 2005 (Herzog 2010, p. 11) and finally into a more contemporary security assessment methodology that prioritizes tests (avoiding guesses), concentrates on the interactions and its required protections, and balance between security and operations (Herzog 2011, p. 2).

OSSTMM has redirected its focus in the earlier releases from testing physical resources such as firewalls and routers to verifying operational security and its related channels, such as Human, Physical, Wireless, Telecommunications, and Data Networks (Herzog 2010, p. 11) in the latest versions of the methodology. OSSTMM also introduces its own measurement metrics called *ravs*[10], which provides graphical representation of system's

[10] Rav: The rav is a scale measurement of an attack surface, the amount of uncontrolled interactions with a target, which is calculated by the quantitative balance between porosity, limitations, and controls. In this scale, 100 rav (also sometimes shown as 100% rav) is perfect balance and anything less is too few controls and therefore a greater attack surface. More than 100 rav shows more controls than are necessary which itself may be a problem as controls often add interactions within a scope as well as complexity and maintenance issues (CCUCDG 2010, p. 22).

states and system state changes over time, and are suitable to be used in operational monitoring consoles. The *rav* metric and other OSSTMM concepts will be further discussed in chapter 3.

Security assessment can have different approaches. Information Security Systems Assessment Framework (ISSAF) (Rathore et al 2006) from the Open Information Systems Security Group (OISSG) intends to be an end-to-end solution in security assessment (Rathore et al 2006, p. 18), comprising guidance in security related assessment, process definition, baseline definition, identification of risks, evaluation of controls for the various security domains, people education for both assessing and securing resources and more (Rathore et al 2006, p. 19). It is a complex and extensive framework that proposes a guidance for a complete security assessment including detailed penetration testing techniques for several physical devices and resources, such as password cracking, physical device assessment (switches, routers, firewall, etc.), services and software assessment such as VPNs, anti-virus, wireless LANs and so on (Rathore et al 2006).

The Cloud Security Alliance (CSA) is a non-profit organization engaged in providing security awareness and tools to adopters. CSA has a specific publication providing guidance to Cloud security, "Security Guidance for Critical Areas of Focus in Cloud Computing" (CSA 2009), which is structured around thirteen domains covering several aspects of Cloud security, including Identity and Access Management.

Guidance is provided by the US Government, and targeted to U.S. Federal Agencies but publicly available. The "Proposed Security Assessment and Authorization for U.S. Government Cloud Computing" has a strong focus on authorization, defines a baseline of security controls and a monitoring process, and also proposes a framework to assess Cloud security during vetting of Cloud Service Providers (U.S CIO 2010, p. 46-79).

2.8 The Software for the Use Cases

The software to be used in the Use Cases has to be relevant to the industry, of common use and have support for Kerberos. These days, with the predominance of the Internet, the web servers and web application servers are widespread and used for business and non-business applications, and therefore are perfect subject of study in the models. However, IT systems are composed also of an operating system layer[11], which has been

[11] http://en.wikibooks.org/wiki/A-level_Computing/AQA/Computer_Components,_The_Stored_Program_Concept_and_the_Internet/F

contemplated in this study by using the Microsoft Windows and Linux. Regarding the applications, the choice was performed after some careful analysis of some options available as illustrated by the list in the Annex A. The list contains applications that are classified as proxy-based true SSO authentication according to Pashalidis and Mitchell (2003), since Kerberized applications are classified in this category. It was defined using practical observation from the existing applications in several organizations (IBM Portugal, Barclays PLC, Liberty Seguros, Montepio Geral), complemented by some Internet research, the reading of some software's manual and also from a list provided by (De Clercq 2010, p. 186). The research resulted in a list of software that supports Kerberos or GSS-API authentication. From that research, it was possible to create a table of applications, which has the following structure:

Category	App. Name	References

The "references" column for each entry contains enough evidences that the application in fact supports Kerberos.

It is important to clarify that this list was never supposed to be a comprehensive list of all applications supporting Kerberos, and such list would never be possible, since "kerberized" applications can (and may be) being developed every day thanks to resources such as the GSS-API, the authentication modules for the HTTPD servers and the Application Servers (Annex A - Kerberos-compatible Applications, Web Application Servers category). The objective with this list is to gather a list of applications that work as a foundation, on top of which several other application software and systems are deployed. This characteristic expands significantly the importance of the chosen items in the list, since every item in itself represents a vast ecosystem of applications that it can be mapped to.

Next, the reasons to choose some of the applications in selected categories, are presented:

- Operating Systems – Operating systems that supports Kerberos will allow their users to authenticate on a Kerberos Distribution Center (such as Active Directory), and will also provide support for its applications to authenticate using Kerberos;

undamentals_of_Computer_Systems/Classification_of_software

- HTTPD – Web Servers applications that provide Kerberos in its core will allow every developed content running on it to authenticate users using Kerberos. In this category of applications, thereafter, it's included all web portals, web front-ends[12] for applications and standalone web pages that requires authentication.
- Java/Web Application Server – Applications servers are systems that provide logic and resources for the development and processing of customer applications. Application Serves are commonly deployed on web based systems since the advent and explosion of the web in the 90's, and the applications developed for this kind of platform are usually structured around a three-tier architecture: the graphical user interface, which provides the front-end for the user, the Application Server where the program logic is implemented and processed, and finally a backend database, where data is stored.[13] Application servers may or may not provide Kerberos authentication in its core components. When it does, the applications can benefit from this facility (IBM 2012, Oracle 2012).

Most of the remaining categories are generic applications, most of them changed or ported to support Kerberos using the GSS-API library. These categories can encompass all applications that use this mechanism to support Kerberos.

The work has produced enough material to make possible the identification of Kerberos usage patterns, implementation scenarios and common technical configurations to support the development of model(s) as proposed by this thesis. From the list, a selected subset of applications will be implemented to provide practical background knowledge to help in developing the security assessment.

[12] Front-end is used here to denote a user interface to an application, which may be running on the same server or in another place on the network.

[13] Source: http://encyclopedia2.thefreedictionary.com/Application+servers and http://searchsqlserver.techtarget.com/definition/application-server

3 Defining the Scope and the Methodology

In this section it is presented the models subject of study in this work. It starts with a baseline model, which represents an organization network (intranet), which should have the most generic architecture as possible. Then the derived models are introduced, which consists of a variation of the baseline with some components migrated to a Cloud. The challenge of authenticating securely over the internet is introduced and the Kerberos protocol is mapped to this scenario to show how it is possible to provide authentication for the derived models.

Figure 5 presents our baseline model. Everything inside the enterprise can be seen as a controlled environment, while everything in the outside is beyond its control, and therefore, must not be trusted. However, this assertion does not mean that an intranet is a safe place to run business without protection - it is not. According to the “2011 Cyber Security Watch Survey - How Bad Is the Insider Threat?” (CERT 2011) carried out by the Carnegie Mellon University over a population of 607 companies, 27% of all security incidents were caused by insiders, at the same time that 46% of all respondents affirm that the internal incidents had caused more damage than the outside attacks. These numbers tell us that, even though Kerberos was designed to provide, among others features, secure authentication over insecure networks (Garman 2003, p. 6), its use in the Enterprise’s Intranet should not be seen as huge gain in terms of control.

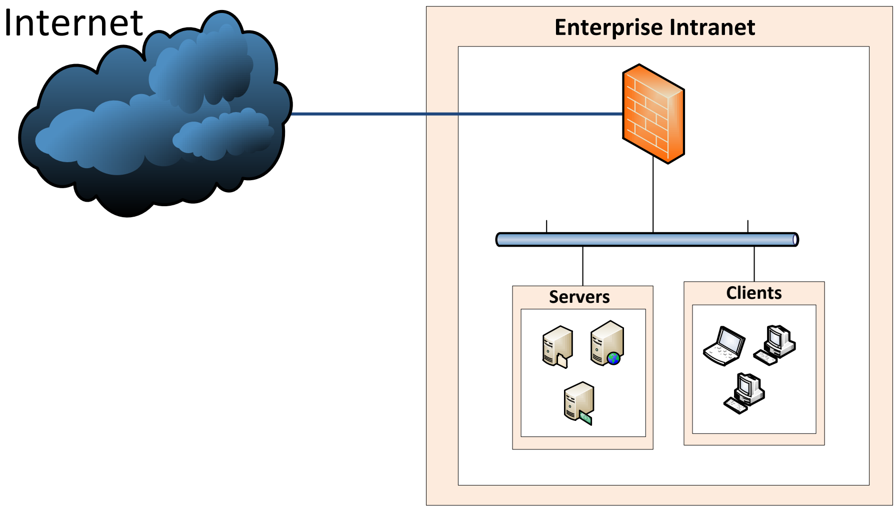


Figure 5: Intranet Model (Baseline)

In Figure 6, some services from the internal enterprise network have been extended to a Public Cloud. This model is in line with the Use Case 3.3 - Enterprise to Cloud (CCUCDG 2010, p. 23), discussed in section 0.

Almost any enterprise application can be configured to work in a Public Cloud. However, two important factors need to be considered:

- The public Cloud is not under the Enterprise's control - therefore, it can be considered an uncontrolled environment (Hiroyuki et al 2011, p.324).
- To work with the applications in the Public Cloud, it is necessary to cross a potential insecure channel: the Internet.

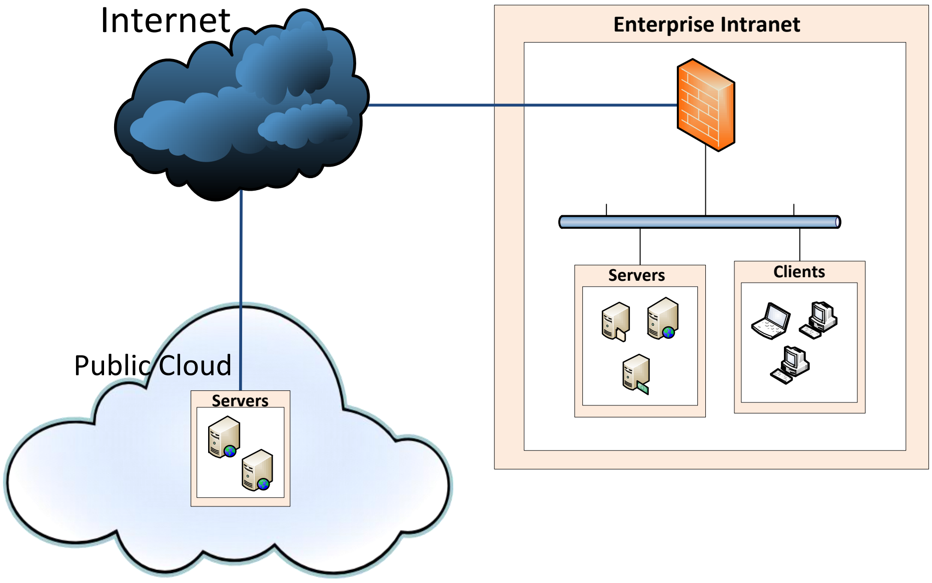


Figure 6: Enterprise to Cloud Model

Two important changes can be verified in the environment when services are migrated to the Cloud: there is a loss of control over part of the IT environment, and risky channel to transport company's values starts being used. These values may be in the form of assets when the company works with data and information, but it will always include private information such as user's credentials.

In a typical authentication scenario using Kerberos, the protocol is applied into a controlled environment, i.e. the Intranet. Proposing to use Kerberos for authentication also for services in the Cloud, it implies the protocol to work across the Internet, crossing an insecure communication medium, being open to potentially several types of attacks such as the ones described in 2.4.2.

In Figure 7 it is possible to observe the protocol working over the Internet, which is an adaptation from the schema previously present in Figure 4.

The subtle change in the level of trust in the surrounding environment is more than enough to make it unviable to apply the protocol for authenticating into services in a Public Cloud. The risk of exchanging private, important data over the Internet in the scenario above is a showstopper for most of the companies. The communication between the clients on the company's Intranet and the server in the Public Cloud can be intercepted in a number of ways, including by the man-in-the-middle attack and the eavesdropping technique, to intercept and decode authentication information, or even raw data.

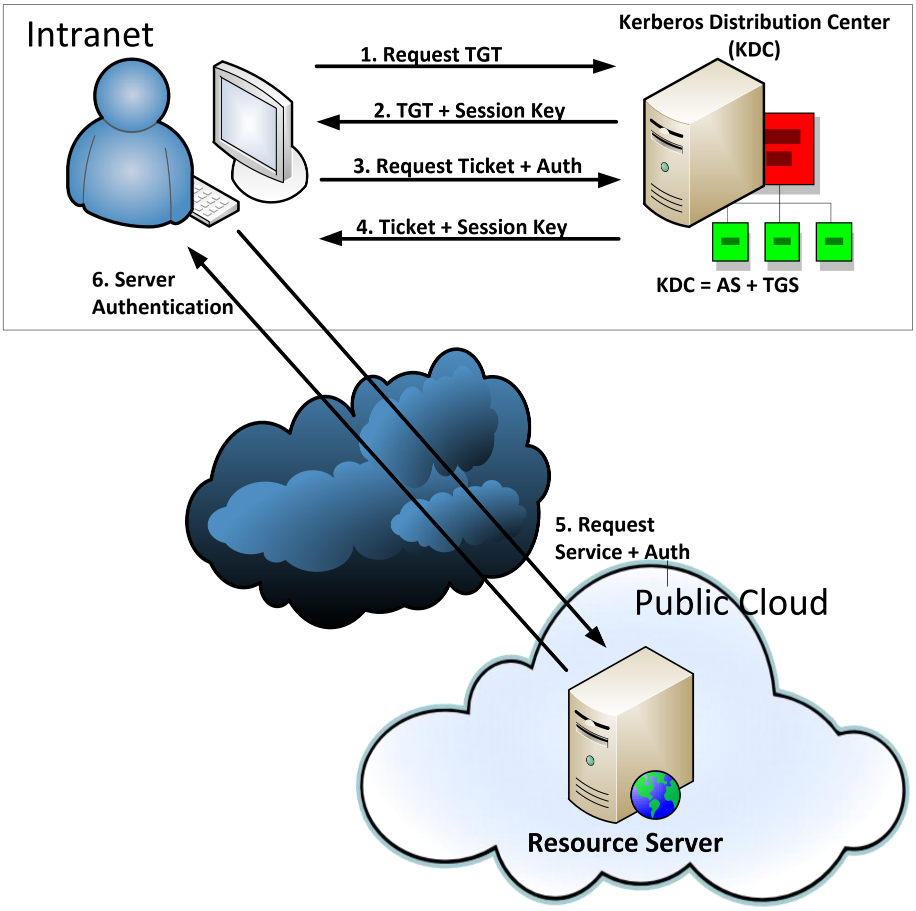


Figure 7: Kerberos Over the Internet

In order for a company to use successfully Kerberos in the Cloud as presented in Figure 7, some protection must be applied to the communication channel, to make it secure for the protocol to exchange its authentication information during the authentication process. The VPNs (Virtual Private Networks)[14] are quite appropriated in this situation, as one of its

[14] VPN is defined by (Zúquete 2010, p. 223-224) as a secure extension of a private network over an insecure (and usually public) network. The VPNs applies encryption to all data flowing through it in order to provide data integrity and confidentiality.

purposes is to allow for remote and geographically distant resources to be used as if they were locally and without disrupting the daily behavior of users (Zúquete 2010, p.228). VPNs provide the means to create an extension of a private secure network over another insecure (and usually public) network (Zúquete 2010, p. 223). Using VPNs, it is possible to create a private communication channel between the Enterprise and the Public Cloud, going through the Internet safely and protecting all the information flowing through this channel from undesired access and extend the reach of its internal network, connecting it to different networks in remote locations using a secure, encrypted tunnel[15] (Figure 8 and Figure 9).

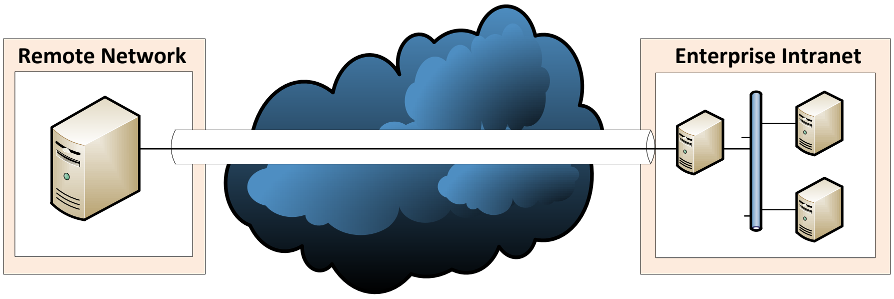


Figure 8: Point-to-Point VPN

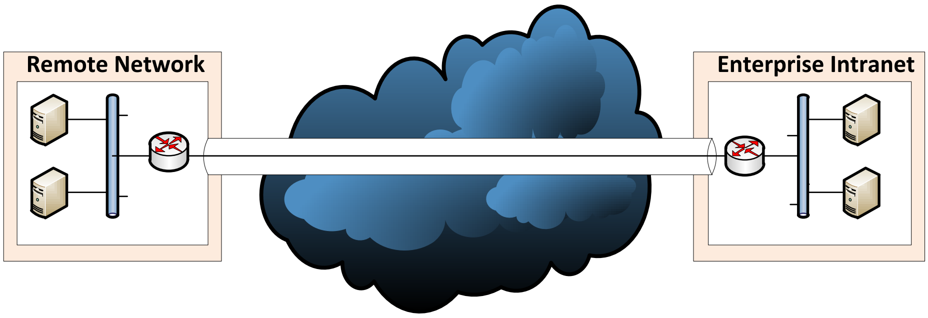


Figure 9: Lan-to-Lan VPN

A VPN can connect one computer directly to another as shown on Figure 8 or it can connect one LAN to another, thus extending the reach of the network, as for example, to connect the company headquarters to its branches. In a Lan-to-Lan VPN, the VPN client and server software are deployed in the routers, or it may have special appliances devoted exclusively to this purpose. These appliances will route all the traffic from one network to the other seamlessly to all the users in the network. A regular or point-to-point VPN (P2P VPN) will connect one resource to another in a remote location. The clients in each side of

[15] Tunnel (or secure tunnel) is defined by (Zúquete 2010, p. 229) as a mean to encapsulate several remote interactions over a VPN safely. A secure tunnel will protect the network traffic from someone who may be eavesdropping to figure out what are the interactions taking place in the communication flow.

the networks will not be aware of the remote resources, unless special configuration is implemented to satisfy business requirements.

Every type of VPN has its application, depending on the objectives desired and the available infrastructure on each side of the VPN. In this study, VPNs will be used to establish secure channels between the enterprise network and a public Cloud. This secure channel is required since a public Cloud is the most exposed implementation, being available to anyone who pays to use its resources (as it was already seen in the section 2.1). From this observation, the concept of "Cloud Exposed Surface"[16] has been developed, which will be greater in the Public Cloud implementation strategy than in the other implementation models.

3.1 Kerberos for Enterprise Authentication in the Cloud Use Cases

Using the VPN technology, the Kerberos protocol will look like what is displayed in the Figure 10, allowing the company to host its resources in a Public Cloud and access them using a secure, encrypted channel. There are several implementations of VPNs available (Zúquete 2010, p. 228-255). For our practical scenarios, it was chosen the open source solution OpenVPN (Zúquete 2010, p.253-254).

This model may seem appropriate for the enterprise, however it addresses only one aspect of the security concerns related to Cloud workloads. The communication channel is protected, but the Public Cloud is still an uncontrolled17 environment and it is necessary to deal with it since the company trusts it to host its servers and data. This change from a controlled to an uncontrolled environment may increase the attack surface to the server or even to the company, but this must be verified and will depend on the company security policies and procedures.

[16] See Figure 12: Cloud Exposed Surface - Visual Representation on page 36.

[17] From the customer's perspective.

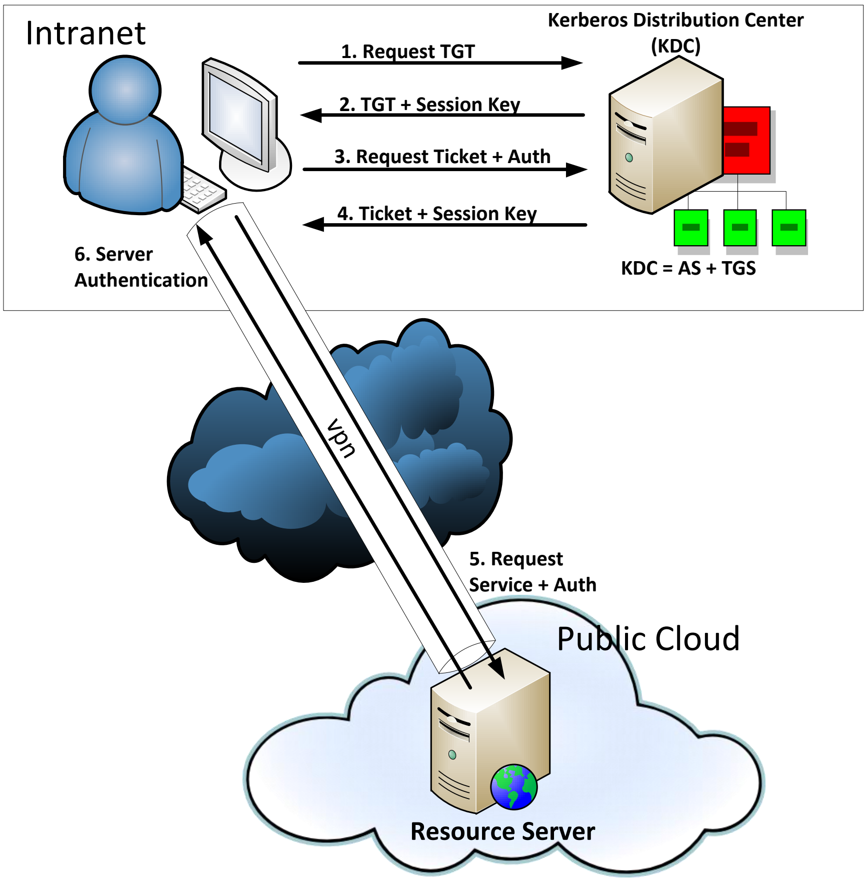


Figure 10: Enterprise Authentication in the Cloud – Kerberos Use Case 1

Another point to highlight in the scenario illustrated in Figure 10 is that it is not appropriate to provide external, protected services to employees or customers. That happens because every user consuming services in the Resource Server should have a valid Kerberos ticket in order to be authenticated and given the required access. It will not be possible for external users (i.e., users outside the enterprise Intranet) to acquire a valid ticket to the enterprise domain without adding complexity to the model presented. This scenario is covered in part by “Use Case 12: Consumer Cloud Identity Management, Single Sign-On (SSO) and Authentication” in (OASIS 2012, p.42-44), although it has a more generic approach, which includes several protocols and Identity Federation. A more similar approach to this work is found in (KITC 2010), a draft, unfinished paper by MIT that proposes different scenarios for Kerberos in the Cloud, but focuses on placing the Kerberos infrastructure itself in the Cloud. That approach diverges from the approach that will be used in this work, which is to continue using the internal Kerberos infrastructure, but move some services to the Cloud.

Using Kerberos to authenticate users to services in a Cloud, from outside the enterprise Intranet, is out of scope in this paper. However one practical scenario would be the case of employees doing home office and still having the benefits of single sign-on using Kerberos, as presented in Figure 11.

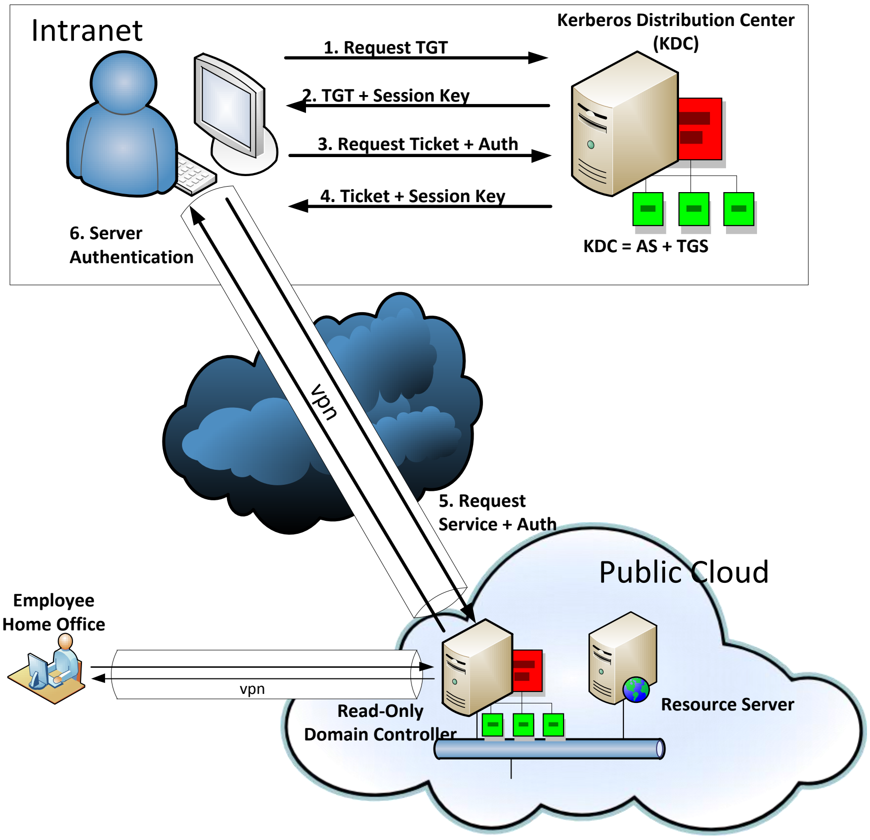


Figure 11: Enterprise Authentication in the Cloud – Kerberos Use Case 2

This scenario presents an additional increase in the attack surface depending how the solution is implemented, and must be evaluated against the level of importance and protection required by the data. In order to minimize the attack vectors, the use case "Enterprise Authentication in the Cloud – Kerberos Use Case 2" in Figure 11 can be implemented using a special deployment of an Active Directory Domain Control: Read Only Domain Control (RODC). The RODC is a feature available from Windows 2008 and newer, and was designed to provide a read only directory services database, unidirectional replication, credential caching, administrator role separation and a read-only DNS[18]. These features address the requirement for the enterprise to make it available authentication services to remote locations with poor physical security among other concerns (Microsoft 2011a).

The use case presented in Figure 11 has the following characteristics:

[18] DNS, or Domain Name System is a hierarchical schema to resolve IP Addresses to more user-friendly names, commonly used in the Internet (Tanenbaum 2003, p.616-625). The DNS is defined in the RFCs 1034 and 1035.

- The RODC server can store a subset of user’s credentials, including passwords (defined in the Domain Controller). This characteristic will allow users to authenticate against the RODC without having to contact the Domain Controller in the company’s Intranet.
- After initial replication of data, the VPN to the enterprise Intranet can be cutoff. This will isolate the RODC and the Resource Serves in the Public Cloud from the enterprise network. The RODC will still be capable of providing a set of services to its clients.
- Due to its functional characteristic of not being able to replicate data to the writeable Domain Controller, if compromised, it will not replicate any data. This feature will make impossible for malicious users to create users in the Intranet server for later exploitation.

A Read-Only Domain Controller can also play the role of an application server. This is ideal for a point-to-point VPN in the home office scenario presented in the Use Case 2, since one single server will have the capability to authenticate the clients and provide services at once, thus eliminating the requirement of an additional server in the Cloud.

3.2 The Use Cases (Models)

Looking at the graphical representation of the Cloud exposed surfaces as illustrated in Figure 12 it is possible to visualize an increased exposure surface starting with the Private Cloud implementation strategy up to the Public Cloud implementation strategy (left to right). This visual representation and its implications are backed the analysis of the Cloud implementation characteristics as defined by NIST in “The NIST Definition of Cloud Computing” (NIST 2011):

- Public Cloud is available to everyone, with its resource pools being shared with all the customers;
- Hybrid Cloud is available to everyone, but has also some private areas reserved for exclusive use by some entities who pays for this service;
- Community Cloud is closed to everyone but some groups with similar interests a group of Universities.
- Private Cloud is reserved for a single organization, and the Cloud resource pools are not shared with others entities or organizations.

What the diagram in Figure 12 does not provide is evidence of how much this additional exposure will affect security. While referring to the work of Chung Li et al (2010) and the results of theirs work, the assessment from the outside of the Cloud registered less vulnerabilities found than the same set of tests conducted from inside. These evidences the fact that a more wide accessible system may not be necessarily more unsecure, but this will depend of some factors as for example, how resilient is the Cloud infrastructure. Otherwise, the test conducted on a single tenant (client) may prove highly positive, but if the Cloud infrastructure (which is not under customer's control) is compromised, so will the customer resources.

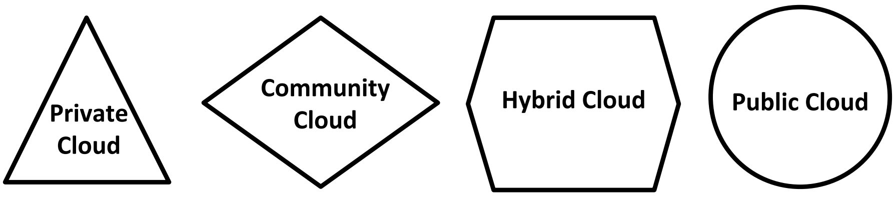


Figure 12: Cloud Exposed Surface - Visual Representation[19]

Despite the above conclusion, not all enterprise application should be migrated to the Cloud. Several factors that must be considered to select the resources to migrate and not all of them are related with security, such as the following provided by (Krutz and Vines 2010, p. 260-261):

- The criticality level of the application
- The sensitivity of the data
- Functionality over VPNs
- Performance
- Cost to move to another provider
- Bandwidth utilization

Using the above information as a decision data, it is possible to conclude that the big challenge in using Kerberos for Enterprise Authentication in the Cloud would come from the use of the Public Cloud implementation strategy, and in line with this conclusion, it was

[19] Cloud Exposed Surface - Visual Representation: The Figures are intended to represent the exposed surface by the number of sides in each geometric object. The external lines in each object represent the interface with the outside world, that its, interaction points. For example, being the private Cloud the less exposed, it is represented with only three sides, or the triangle. The Community Cloud comes next, with an increased number of sides in its geometric object – the square, and so on. The point in this representation is to highlight visually the exposed area for every one of the Cloud implementation strategies as defined by (NIST, 2011), without the compromise of being mathematically exact in the proportions represented by the figures.

decided that any case study to be assessed for security in this work would be based in the Public Cloud implementation strategy.

Regarding to the case studies analyzed, the decision about which one to choose was based on two factors:

a. The Kerberos protocol architecture.

   Independent of the deployment and the type of application, the Kerberos protocol will always follow the structure describe in 2.4.1, “How does Kerberos Works?” That is true for native applications or GSSAPI applications, which encapsulates the protocol in a more generic API.

b. The assessment of “kerberized” applications carried out and available in Annex A - “Kerberos Compatible Applications”.

   It was identified several applications that reportedly support Kerberos. Several of the applications found on Annex A targets the end-user, such as the telnet, ftp and putty applications, while others provide a framework over which other applications can be developed, such as the Apache HTTP Server and TomCat, Microsoft IIS, IBM WebSphere, etc.). These class of applications are substantially important due to its characteristics of proving internal resources that make it possible every application deployed on top of them to automatically benefit of the authentication framework available, which include Kerberos for the listed applications in Annex A - Kerberos-compatible Applications.

From factor (a), it was concluded that any “kerberized” application would satisfy the requirements of a selected model, which is, the model must be representative of a true, practical Kerberos implementation.

From factor (b), it was chosen the Microsoft IIS to represent the class of HTTP Servers and therefore, a myriad of possible applications. The HTTP servers were configured to allow the use of Kerberos tickets provided by the end-user browsers, and this way performing single sign-on using the authentication previously done in the Windows computer.

Therefore, the security assessment was carried out on the models represented in “Enterprise Authentication in the Cloud – Kerberos Use Case 1” (Figure 10) and “Enterprise Authentication in the Cloud – Kerberos Use Case 2” (Figure 11). Both models were implemented using the Public Cloud deployment strategy over an Infrastructure as a Service

(IaaS). The results were compared with the security assessment for baseline use case "Intranet Model (Baseline)" in Figure 5. This use case presents all common characteristics of the model to be analyzed, and usually deployed in the enterprises, since it is composed by the mandatory components: one centralized trusted authentication server (the Kerberos Distribution Center or KDC), one or more Kerberos clients and one or more resource servers. As a result of this architecture, a trust relationship is also present in the process of authentication, since the resource servers must be able to authenticate the clients using Kerberos tickets previously issued by the KDC.

3.3 The Security Assessment

In chapter 2, the methodologies and frameworks to access IT and systems security were investigated. Among all the sources that were found, there was not a single methodology or framework specifically defined for Cloud security assessment or evaluation. This fact presents a new challenge to overcome in this work, because now it will be necessary to come up with a method to evaluate the results of this work.

Since there is not a specific methodology or framework to assess Cloud security, a generic, comprehensive and modern methodology (OSSTMM) was chosen, as a basis for the security assessment to be conducted in this work. The OSSTMM methodology is appropriate to verify individual channels for its security, as we can read below:

> *"Since environments are significantly more complex than in years past due such things as remote operations, virtualization, Cloud computing, and other new infrastructure types, we can no longer think in simplistic tests meant only for desktops, servers, or routing equipment. Therefore, with version 3, the OSSTMM encompasses tests from all channels - Human, Physical, Wireless, Telecommunications, and Data Networks. This also makes it a perfectly suited for testing Cloud computing, virtual infrastructures, messaging middleware, mobile communication infrastructures, high-security locations, human resources, trusted computing, and any logical processes which all cover multiple channels and require a different kind of security test."* (Herzog 2010, p.11)

The OSSTMM proposes a methodology to verify and test the Operational Security (OpSec) of systems. For the Cloud, some parts of the OpSec procedures can only be assumed to be compliant with the enterprise's policies by means of terms of contracts and SLAs (Hiroyuki et al 2011, p.324) from the perspective of the customer. Larger companies can go beyond contracts and require an operational security test evaluation report from the provider, but this option may not be an option for small customers.

Following Yildiz et al (2009) as seen in “2.6 Cloud Security”, in order to assess Cloud security, all five layers should be assessed. However, there is another point of view from (Grobauer et al 2011), who proposed to identify a Delta between common IT security issues and Cloud specific security issues. This is a very interesting point of view when it is necessary to analyze Cloud security, since it makes it possible to test Cloud for its specifics security features, without having to break it down to its small components and testing all of them. Testing the individual components should be subject of the usual existing assessment methodologies. What is missing is a methodology to test Cloud specific vulnerabilities.

In order to focus on specific Cloud security issues, it was used the concepts presented by Brobauer et al (2011, p. 52), who proposes that vulnerabilities are Cloud specific when it:

- *is intrinsic to or prevalent in a core Cloud computing technology,*
- *has its root cause in one of NIST’s essential Cloud characteristics,*
- *is caused when Cloud innovations make tried-and-tested security controls difficult or impossible to implement, or*
- *is prevalent in established state-of-the-art Cloud offerings.*

Identifying, assessing and testing only a delta between a generic system and a system in the Cloud will allow the tester to focus on the relevant exposed surface, which seems very logical and this is the approach used for this current work.

Moving to the assessment methodology, the OSSTMM defines the following 7 steps for defining security test (Herzog 2010, p.33):

1. What to protect

   The purpose is to identify the Controls put in place to protect the assets, and its Limitations.
2. The engagement zone

   Where there is interaction with the assets to protect, this will be included in the engagement zone. This will include protection mechanisms, processes and other services and systems.
3. The scope

   Should include everything outside the engagement zone required by the assets in order to work or to provide their services.

4. The vectors

   The existing interactions of the asset with the environment or other internal entities.

5. The channels

   - Human
   - Physical
   - Wireless
   - Telecommunications
   - Data Networks

6. The test type[20]

   There are 6 types of tests: Blind, Double Blind, Gray Box, Double Gray Box, Tandem, and Reversal.

7. Rules of engagement

   Defines 42 operational guidelines of acceptable practices related with security assessment and penetration testing, and classified in 7 categories: sales and marketing, assessment and estimate delivery, contracts and negotiation, scope definition, test plan, test process, and reporting.

The security assessment will implement the relevant concepts from the OSSTMM, which is summarized in the process flow illustrated in Figure 13. During an OSSTMM security assessment, passive testing is combined with active testing and emanations detected from the surrounding entities, in order to derive metrics and come up with a gap analysis (which is accomplished comparing with an existing baseline) (Herzog 2010, p.41-51).

[20] Refer to (Herzog 2010, p.37) for a complete definition of all 6 test types.

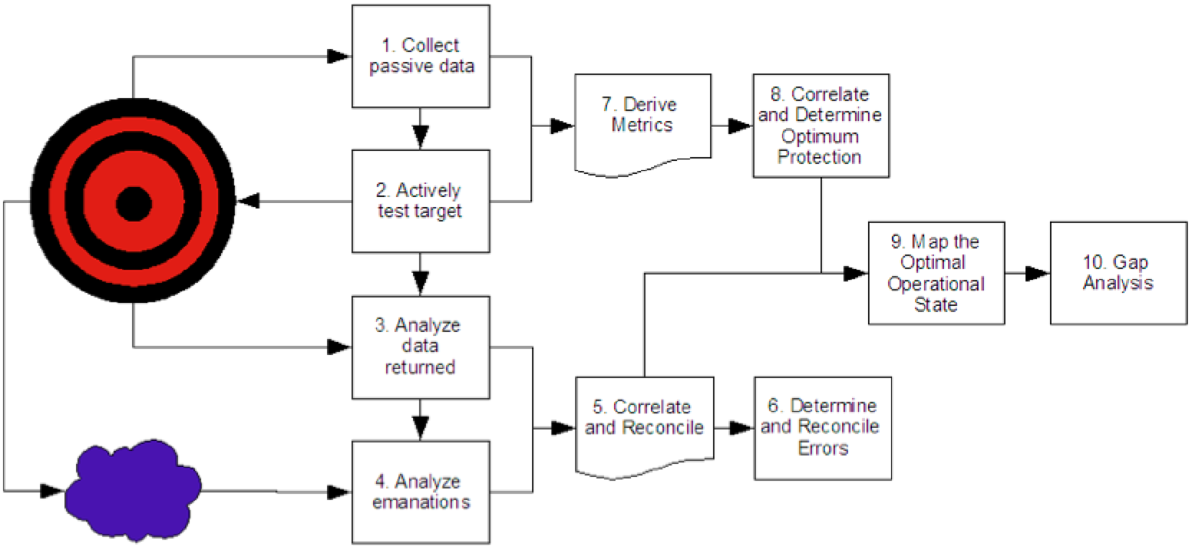

1. Collect passive data
2. Actively test target
3. Analyze data returned
4. Analyze emanations
5. Correlate and Reconcile
6. Determine and Reconcile Errors
7. Derive Metrics
8. Correlate and Determine Optimum Protection
9. Map the Optimal Operational State
10. Gap Analysis

Figure 13: OSSTMM Process Flow
(Source: Herzog 2010, p. 45)

Taking into consideration the work of Yildiz et al (2009), Brobauer et al (2011), and Herzog (2010, p.167-183) discussed above, the following components will be in the scope of the security assessment in this current work:

- The network layer;
- The Application layer, including the enterprise application and Cloud Operations Dashboard;
- Processing Servers – we make an adaptation here and will test the virtual machines hosting the services (VMs), since these VMs are under control of the customer (the enterprise in our study). The servers hosting the VMs are part of the service provider's infrastructure, and therefore, beyond the customer's possibility to test it (the host security must be covered also by SLA).

3.4 The Metrics

The Open Source Security Testing Methodology Manual version 3 (OSSTMM 3) provides a unit of comparison: the *rav*.

The *rav* takes into consideration the concepts of operations, limitations, porosity and controls to calculate the size of an attack surface for any target. At this point, it will be important to define "Attack Surface" and other related concepts.

Attack Surface	The lack of specific separations and functional controls that exist for that vector.
Attack Vector	A sub-scope of a vector created in order to approach the security testing of a complex scope in an organized manner.
Controls	Impact and loss reduction controls. The assurance that the physical and information assets as well as the channels themselves are protected from various types of invalid interactions as defined by the channel.
Limitations	This is the current state of perceived and known limits for channels, operations, and controls as verified within the audit.
Operations	Operations are the lack of security one must have to be interactive, useful, public, open, or available.
Porosity	All interactive points, operations, which are categorized as a Visibility, Access, or Trust.
Vulnerability	One classification of Limitation where a person or process can access, deny access to others, or hide itself or assets within the scope. More details and examples are available in the Limitations table in 4.2.

Table 2: rav Related Concepts

(Source: Herzog 2010, p.21-22 (a complete list definition of all related terms))

A security assessment following the OSSTMM will result in a numeric value representing the level of security of the assessed system (*rav*). When there are several targets in the scope for a security assessment, the values obtained for all individual targets can be combined to produce a final *rav*, representing the actual security for the whole system. The *rav* calculation can be simplified as (Herzog 2010, p.67):

Rav = Controls – (Porosity + Limitations).

Where:

- Porosity

  The number of visible holes in the scope, which means that only what can be detected during the tests, is accounted for the *rav*.
- Control

The controls in place to protect the targets. The OSSTMM define 10 types of controls[21], and every control in place is valued 10%.

- Limitations

  Limitations or "vulnerabilities" are derived from the porosity and the controls. The higher the porosity, higher will be the limitations. The less controls found, the higher will be the limitations.

The porosity can be determined by a set of security tests in the system, which may be comprised of several individual components. In a security test, every component in the system will be a target. There are several tools available to test systems from several attack vectors and documented in several literatures as for example by Wilhem (2010) and McClure at al (1999). To verify the models in this work, we have used the open source OpenVAS security assessment tool.

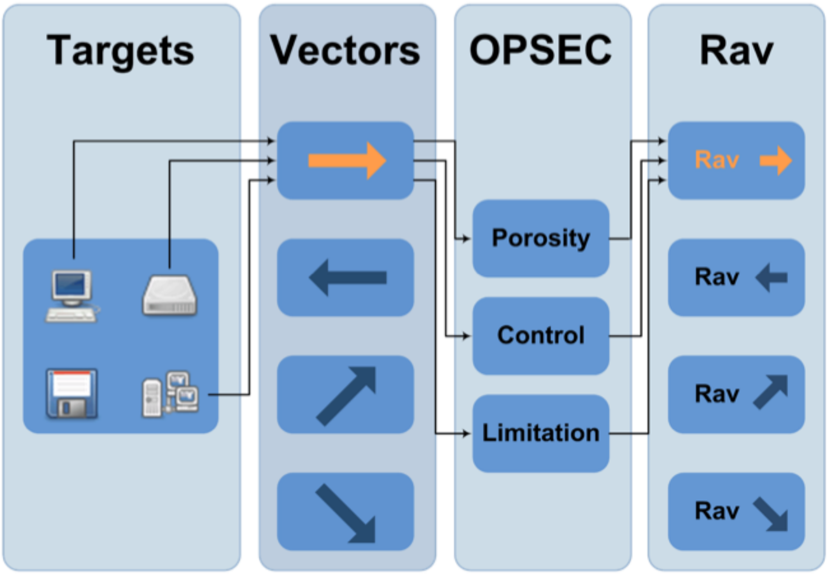


Figure 14: Making a rav from a security test
(Source: Herzog 2010, p. 67)

The controls may not be always tested for its presence, and it is a more complex subject. For example, the control number 10, the "Alarm", cannot be always tested in a Cloud environment because it depends of several factors, such as monitoring availability (be it provided by the Cloud service provider or deployed by the customer itself). In this case,

[21] Please refer to the OSSTMM V3 (Herzog 2010, p.24-25) for the list and specification of the 10 controls.

control number 10 could be valued according to contracted services, using the SLA terms of service, for instance. It could be given a value of 50% or 100%, and it should not matter or impact the final report results since this work will be looking for a delta relative to a baseline, not to the independent assessment result for every scope. Another option to deal with the security controls and supported by the OSSTMM is to assign default values to all controls and verify only the actual porosity and actual limitations for the targets (Herzog 2010, p. 67-68).

Regarding the limitations, the OSSTMM also defines it as “vulnerabilities”, which are derived from the porosity. Since the porosity is determined by security tests, the values assigned to the Limitations will be calculated based on the number of vulnerabilities found in the visible targets.

The OSSTMM is not a methodology to test Cloud specifically, but a generic methodology to test many types of IT and non-IT systems. The difficulty to standardize Cloud security assessment and evaluations is already subject of concerns in the professional sector. Several organizations have been making different contributions, and using different approaches (NIST 2010)(CSA 2009)(OWASP 2012)(USCIO 2010).

In this work, this difficulty is recognized, but it is out of scope to develop a specific Cloud security assessment framework of methodology to evaluate the results of the study conducted. Instead, the security assessment was based on the shortcut proposed in the OSSTMM methodology, which consist of taking into consideration only the Porosity and Limitations found, assigning default controls for discovered services and accepting an uncertain but perhaps small error margin (Herzog 2010, p. 67-68).

Using the *rav* metric proposed in the OSSTMM will make it possible to find a security value for the baseline relative to the scope, and later compare with the values obtained from the assessment of the Cloud model. This comparison between different scopes is supported by the methodology and defined as the concept of “Actual Security” (Herzog 2010, p.63). The Actual Security is built upon another OSSTMM concept[22], and allows for the comparison between different scopes such as the models proposed in this work for the intranet and for the Cloud. Using the *rav* metric it would be possible, for example in a physical security assessment, to affirm that Building A is 75% secure while Building B is

[22] The OSSTMM defines and allows the concept of “perfect security”, which is 100 ravs. Perfect Security is the right balance between porosity, limitations and controls, which would be 100 ravs. Perfect Security as defined by the OSSTMM means that there is a correct (or enough) number of controls applied to the system. Less than 100 ravs means lack of controls, while more than 100 ravs implies in excessive and unnecessary controls (Herzog 2010, p.21, 63, 80).

95% secure. Although the two buildings have nothing in common, the perception of vulnerability is evidently greater for Build A. Using this approach, it is possible to have objective metrics to compare the security of baseline model with the Cloud models.

The OSSTMM does not dictate which tests to run or how to apply them on the systems being assessed. The required methods to design and run a security test are supported by the design and implementation of a Virtual Lab as defined in (Wilhem 2010).

3.5 Laboratory Setup for the Use Cases

The Use Cases presented in this work were implemented using virtualized servers. The whole enterprise scenario in Baseline Model was implemented using five virtual server and two physical routers (See Annex B for the architecture). This Use Case had the compromise of making available the typical components of an organization’s network, such as a public web server (accessible from the Internet), one internal web portal, a Kerberos Distribution Center (KDC) to authenticate others services and users, and also the user’s workstation. The users should have the capability to logon into the network and be authenticated by the KDC once, and be able to access internal applications using Single Sign-On.

Cloud Use Case 1 (Annex C) and Cloud Use Case 2 (Annex D) were built on top of the Baseline model with some key changes: the public web server and the application server were moved to the Cloud. Use Case 2 also introduces the Read-Only Domain Controller, a special type of authentication server that can only be accessed for read-only operations, and therefore, very appropriate for hostile environments such as the Cloud.

The servers for the Use Case 1 and Use Case 2 were hosted in an OpenStack Cloud infrastructure with a public hostname and IP to be accessible from the Internet. This external access makes it possible for Internet users to access the organization’s public web server in all Use Cases, but also provided means for enterprise users to access and authenticate into the Read-Only Domain Controller in Use Case 2.

The choice of the virtualization infrastructure required that the virtualized environments had the actual characteristics found in an enterprise and also being capable of supporting different operating systems, running on Mac OS X and Linux, free of charge, stable and reliable. The VirtualBox open source software was chosen to implement the Baseline model with all its systems, and it was deployed under Mac OS X, while the

OpenStack Cloud IaaS solution was chosen to implement the models in the Cloud and it was deployed in a Linux environment.

OpenStack is a relative new open source solution to build private and public Clouds that had a great acceptance and involvement of reference enterprises such as Cisco, HP, IBM, Intel, Rackspace and about other two hundreds companies, plus more than 10.000 individuals around the world (www.openstack.org). OpenStack already provides the foundation for commercial Cloud services provided by Rackspace, HP, IBM among others. Such great acceptance from the industry associated with non-existent licensing fees makes it more than adequate for use in investigation projects.

The software deployed in the baseline model was the Active Directory server acting as a Kerberos Distribution Center (KDC), a domain member workstation, a domain member server and the Internet Information Services on the Windows server to act as a Kerberos service. The Linux boxes had also sshd configured to authenticate using Kerberos. These software was chosen from list in Annex A.

4 Results and Discussion

A security assessment for a complex networking system may have different results depending on the approaches and decisions taken during the planning phase. To address this issue, it was defined that the test should be based on a model that precisely represents a real, enterprise scenario without the added complexity of the large number of systems. To accomplish this objective, the use cases previously defined in this thesis were implemented in such a way that the resulting network had:

- A client workstation, who need to authenticate in a server prior to accessing network resources;
- An authentication server with a user's database, to authenticate the clients and other trusted servers in the network. This server is the Kerberos Distribution Center (KDC);
- A web application server with a trust relationship with the KDC;
- A Public web portal to provide a web presence for the enterprise over the internet;

What makes this setup different from an actual, enterprise network is the number of components deployed. While the number of components in a network may have a huge impact in the exposed attack surface, it is irrelevant for our assessment approach due to these reasons:

- The security metrics calculated by only using Kerberos inside the enterprise network (intranet) is not relevant by itself, and this fact does not change with more components added or removed from the network; the same is valid for the security metrics of Kerberos deployed in the Cloud;
- The number of devices in each use case would definitely increase the attack surface, and probably add to the overall number of vulnerabilities and limitations in the network. However, this is true no matter where the individual systems are hosted, be it in the intranet or in the Cloud;
- Despite the number of existing devices in each use case, the movement of devices between the two environments (corporate network to Cloud, or Cloud to corporate network) will not affect the security metric of that individual device,

that is, any device moved from one environment to the other will keep its individual security properties;

Given the above arguments and assumptions, it is clear that augmenting the complexity in the models by adding devices (servers, services and applications) should not impact the final metric subject of this study, since:

- At any time, the selected target would exist in one, and only one of the two different environments. Therefore, its individual security characteristic will move along with it;
- The security assessment would be executed twice, to assess the network security with the selected targets placed in each one of the two different environments.

Using this methodology, it was intended to keep the calculated security delta associated mostly with the changes in environment itself, and less with any individual target, thus making it more viable to repeat the test several times if required, since the number of moving elements is low. This methodology will also allow its application in different environments, making it possible to assess security based in a context and not on individual systems characteristics.

Using the OSSTMM and its *rav* concept to provide a tactile visualization of the different use case's security status, it was possible to measure how the enterprise overall security was affected using Kerberos to authenticate users in a public Cloud environment in relation to a baseline model. The application's usability was not affected, and the users did not even notice the changing since the setup in the Cloud does not impact the running services in the intranet. The Cloud application's take over was just a matter of changing a DNS[23] entry in the enterprise DNS server, a quick and almost unnoticed event in the network.

The following results were produced feeding the *rav* spreadsheet calculator with the outputs from the OpenVAS tool. The spreadsheet is provided by the ISECOM (OSSTMM publisher) to help in this task, and it has programmed internally all the formulas to generate the *rav* for a set of data obtained from a security test (Herzog 2010, p. 79-85).

To produce the security metrics for the systems, the OpenVAS - vulnerability assessment system was run against each one of the components of the models under analysis, one model at a time. The resulting data for each individual model was combined (Herzog

[23] The Cloud server was deployed using its own IP address, without disrupting the existing intranet services. When the servers were ready to go into production, a simple DNS change in the enterprise DNS server provided the switch from the intranet servers to the Cloud servers.

2010, p.68) and used to feed the spreadsheet calculator. All the formulas to generate the *rav* were handled, therefore, by the spreadsheet, which generated the resulting *ravs* representing the security of the systems.

Table 3 contains the final *rav* values computed for each one of the models analyzed, and the variance in the security for the Cloud models compared to the baseline model.

The numbers show that hosting the enterprise public web server and one private web application server in a public Cloud provided a loss of security, more precisely of -2,46% in the overall enterprise security. When the web application server was replaced by a Windows Read-only domain controller to provide also the role of the application server, the security variance was also negative: -2,8272%. The value in the Actual Security represents the overall enterprise security for that specific model, which was calculated considering the metrics from the internal and external assessments (for the Baseline) and also the assessment from inside the Cloud using another tenant space (for the Use Case 1 and 2).

	Baseline	Use Case 1	Use Case 2	Baseline After Migration
Actual Security (*rav*)[24]	77,5333	75,6259	75,3413	80.9317
variance (related to the Baseline *rav*)	N/A	-2,4601 %	-2,8272	4,3831

Table 3: Security metrics compared for all Models
(Source: STAR Reports produced by the security assessment - Annexes B, C and D)

The above results were obtained from the vulnerability assessment which produced the following data and are reproduced here as a summary from the Annexes B, C and D.

	Baseline	Use Case 1	Use Case 2
Visibility	101	148	159
Access	2	4	5
Trust	3	3	4

Table 4: Porosity

	Baseline	Use Case 1	Use Case 2
Vulnerabilities	13	24	24
Weaknesses	28	32	32
Concerns	53	76	86
Exposures	15	328	341
Anomalies	0	0	0

[24] The ravs in this table should be seen as a percentage (%). 100 ravs would represent a 100% secure system, which is the OSSTMM concept of Perfect Security (Perfect security was previously defined in the paper).

Table 5: Limitations

The mapping between the Security Assessment and the inputs to the rav calculator is as follows:

Item	How to get
visibility	Number of servers in the use case + number of unique open ports for all servers
Access	Interactions points between the servers and the outside world
Trust	Interactions that do not require authentication

Table 6: Description of Mapping OSSTMM x OpenVAS

The Limitations in the rav calculator were mapped directly from the OpenVAS Results as seen on the following table.

OSSTMM	OpenVAS
Vulnerability	High Severity
Weaknesses	Medium Severity
Concerns	Low Severity
7Exposures	Log
Anomalies	False Positives

Table 7: Mapping OSSTMM x OpenVAS

However, one interesting consequence of moving to services from the intranet to the Cloud is the corresponding transfer of porosity. The intranet security metrics has increased from 77,5333 *ravs* to 80,9317 *ravs* for a positive variance of 4,3831% (Annex E). This change may be as much more relevant when the services migrated to the Cloud are considered of low importance, since this move will provide a tradeoff between risk associated with low importance data versus risk associated will high importance data. The low importance data will be migrated to a less secure environment, while high importance data is kept in an even more secure environment (since some targets were transferred, taking along with them the associated porosity).

The gain in terms of security for the enterprise intranet is a factor that may be surprising at first, but logical when closely analyzed. Looking at the attack vectors for the Baseline model (Annex B, Figure 1) it is possible to count 7 internal attack channels and 2 external attack channels for only 7 targets. These vectors and channels combined produced about 101 holes and 309 total limitations in the surface (Annex B, p. 1). Considering that every visible target contributes to increase the porosity of the surface is very logical that moving the target out of the surface will decrease its number of holes and limitations. And removing only low risk targets from the surface contributes in two ways to a better security:

- Less exposed targets in that environment that could be compromised in order to gain privileges and later compromise more important targets;
- Automatically increase the environment security since the attack surface is lower.

These concepts are illustrated in Figure 15 and Figure 16. An attacker would try to compromise every target he can enumerate, even those targets that do not hold any important assets. The purpose is to gain access that can eventually be used to escalate privileges, access other targets and ultimately, the desired resources. In the simple example in Figure 15 the attacker tries to compromise all the servers in the enterprise network, which is composed of two non-strategic servers holding basic information (which may be even public), but which has also two other very important servers to the organization (strategic servers). These two strategic servers could be the Kerberos Distribution Center (KDC, Windows Domain Controller), which has a database of all users in the network, but could be also a corporate database with financial information. The point here is that critical and non-critical systems are equally exposed. Once any of the targets are compromised, it can be used as an attack vector to the other targets as illustrated in Figure 16. Some reasons to protect Kerberos servers can be found in (Garman 2003, p. 101-109).

The Kerberos protocol provides a better user experience by providing application's single sign-on for users already authenticated in a KDC. As it was presented previously in this work (section 2.4), these features are provided by means of an encrypted ticket that is stored in the user's workstation after his initial logon on the KDC. A Kerberos encrypted token has a limited lifetime, which is configured in the KDC and is usually of about 8 to 24 hours. This lifetime has the objective of making it unviable for an attacker to indefinitely use any stolen ticket, since after expiration, a new ticket will only be issued by the KDC after the user provides his password. However, when a server machine is compromised, all communication from client to that server can be decrypted since the attacker had access to the server tickets stored locally (Garman 2003, p. 10). If this compromised server is the "Non-Strategic server 1" in Figure 16, the attacker will be able to launch internal attacks in the enterprise intranet.

The Cloud Use Case 1 analyzed in this work had these benefits confirmed as it was already presented above. When two servers were moved to the Public Cloud, the internal security metric has increased by 4,3831%, with the additional benefits of an enhanced security as illustrated by Figure 17[25].

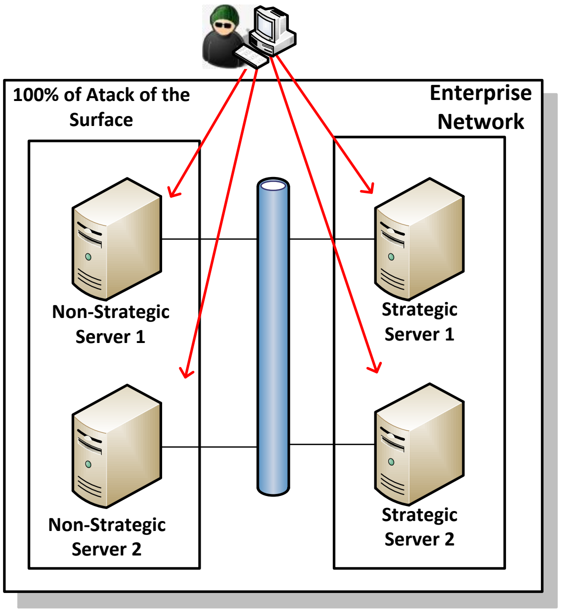


Figure 15: Exploring Attack Surfaces

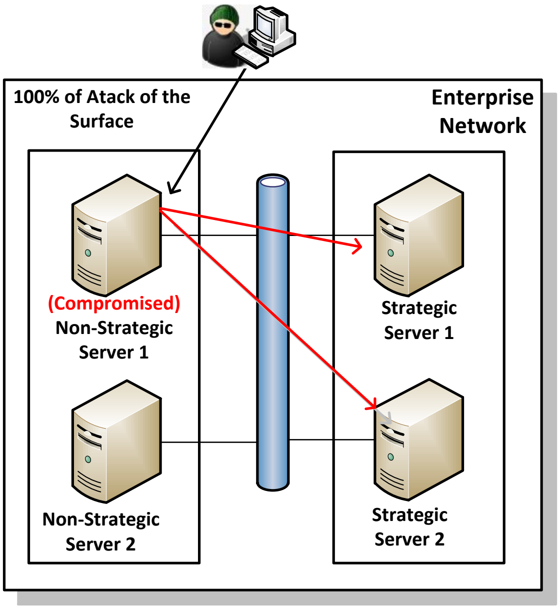


Figure 16: Exploring Internal Attack Surfaces

Although the overall enterprise network security had decreased by 2.4601%, the internal network security has improved by transferring some no-strategic services to a public Cloud. By hardening the traffic flow from the external servers to the internal network, a compromised server in the Cloud would not present a higher treat to the intranet resources as it would do if the same server were inside the enterprise network.

After studying the baseline model, and its counter-part Cloud Use Case 1, it was analyzed how the Cloud model could be expanded and improved.

[25] Farm out is used here to express the migration of those resources to an infrastructure outside the enterprise network – the Cloud in this work's context.

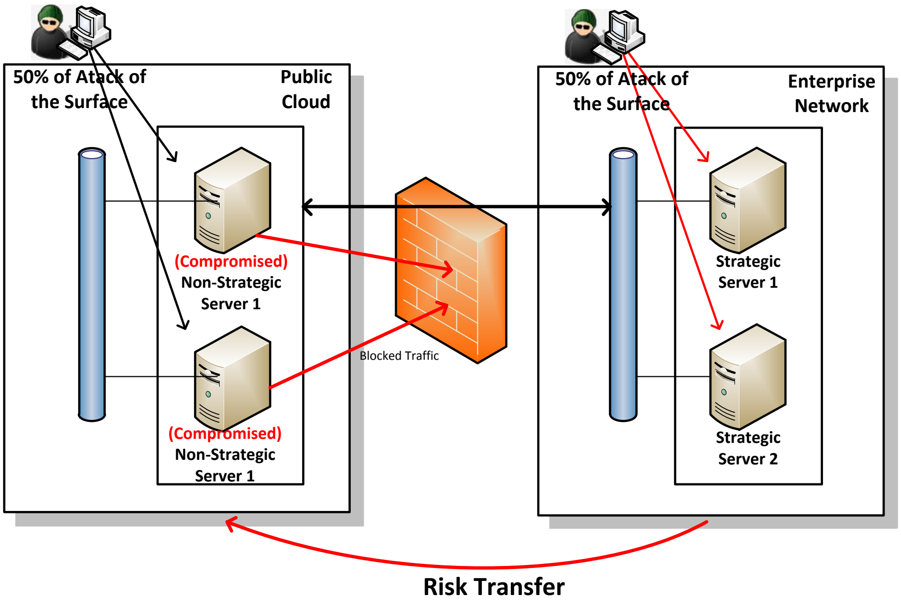


Figure 17: Reducing Porosity by Farming Out Resources

Using a VPN in the Use Case 1, it was possible to deploy a trusted service in a public Cloud environment, and still allowing intranet users to benefit from the single sign-on feature. In that scenario, security was improved in the internal network at the cost of a small decrease in the overall security. Since it was not assigned different weights to each server, the non-strategic and strategic resources had the same impact in the final *rav*, and this is one reason the overall metric has decreased. Another reason is the introduction of new components in the Use Case 1 that did not exist in the Base Model:

- The Cloud Management Dashboard;
- The Cloud default router.

The Cloud Dashboard is a typical component in public Clouds. It is used by the tenants to manage their virtual servers, and must be accessible from the Internet. This component is a web application designed to allow the tenant administrators to perform several actions with within their Cloud space, such as launching virtual servers (also known as instances), view the instance console and logon into the instance, assign a public IP Address to the instances, and so on. The Dashboard must authenticate the users and allow access only to the authorized Cloud space for each tenant.

The second component added to Use Case 1 was the default router. This component provides the tenant's instances with connectivity to the outside world (Internet), which is required in order to allow the enterprise web portal to be available to its customers as well as to its own employees using the VPN server to access resources in the Resource server. All services installed in this host and its corresponding open ports have definitely contributed to the porosity of the Cloud surface.

To improve the metrics and provide a better tradeoff between risk and benefits, it was introduced the Use Case 2 (section 3.1). In this scenario, the enterprise have the option to deploy a remote read-only authentication server that allow them to provide roaming authentication and the same Kerberos functionality to its employees accessing the application server from abroad as well as from the intranet. This scenario can be switched from an enterprise internal use only to an external use only (accessible from the Internet), or for both types of use. The read-only authentication server performs a function of a Kerberos Distribution Center with a read-only database of users allowed to login into that server, and will not accept any write operation. The user's database replicated to this KDC may also be a limited set of users from the main KDC in a way that only the required user's credentials are available in the Cloud, and consequently minimizing these data exposure in an environment with a lower degree of control.

The Use Case 2 can have the VPN connection with the enterprise switched off after synchronizing the user's credential with the read-only domain controller (private application server), and it will still be capable of authenticating users that connect to it. The roaming users in this scenario will have a VPN client to connect directly with the application server, and still benefit of Kerberos single sign-on and other authentication services hosted locally in the Cloud. Although the web portal can be openly accessible from the Internet, to access the private services running in the read-only authentication server an employee must have its workstation connected to the enterprise network, or have a VPN and corresponding authentication VPN key to be able to access it from the Internet.

The read-only authentication server has been implemented in our Use Case 2 using a Windows 2008 Read-Only Domain Controller, and has allowed the extension of the Use Case 1, which has been designed to match the exact existing functions of the Baseline model, and add new features to make it possible for the enterprise to expand its internal service portfolio, while keeping all the usability characteristics fond in the original model.

5 Conclusions and Future Work

Kerberos is an authentication protocol that provides the means to authenticate users and resources over an unsecure network (Garman 2003, p. 6) with an already long history of being a “de facto” standard authentication protocol for TCP/IP networks (De Clercq 2004, p. 133). Due to its wide adoption (Foley 2010) several applications have already Kerberos support integrated in its core (Annex A), which facilitates the implementation since it does not require any major changes in the software source code. Since Kerberos is so well integrated into the IT systems in the organizations, and these organizations are moving its resources to the Cloud, it makes sense that Kerberos should be there as well.

Once the organization has its resources hosted in the Cloud, its security will be affected in some way. Decision makers must know what are the new security challenges. They often look into numbers and other very objective facts to take decisions. Besides financial numbers, technical viability will also be considered, and the security of the assets is mandatory and must be assured. The problem here is that security can be a subjective matter, depending on the approach applied to measure it.

In this work, it was presented scenarios for Cloud usage and its challenges and the necessity of an evaluation or assessment methodology to facilitate decisions in favor of its adoption. It was made clear that VPNs are required for intranet / Cloud interoperability, especially when using Kerberos for single sign-on authentication in order to protect data traffic over the channels. Given the arguments to go for the Cloud, it has to be verified about viability concerning several factors, including security. A resource can only be migrated to a Cloud if it will still comply with the organization’s security standards and policies, and therefore, it needed to be tested in the source environment to establish a baseline and metrics that can be compared with the destination environment. Having a baseline is important to establish a point of reference.

The OSSTMM is a security testing methodology that focuses on the operations of the systems, and its interactions points - interfaces with the external world. The OSSTMM defines operations as the lack of security a system must have to become useful (Herzog 2010, p. 31), and presents a methodology and the tools to measure it assessing the limitations (which are classified by the consequences of its actions), controls (to reduce impact and loss) and porosity (interactive points) (OSSTMM 2010, p. 21-22).

In this work, the security assessment was performed using the short cut proposed by the OSSTMM, which consists of counting the porosity and limitations identified by vulnerability scanner software and assigning default controls for discovered services. This method presents a small error margin, but is supported by the methodology as a way to achieve quick comparisons between different systems security (OSSTMM 2010, p. 68).

Using a software vulnerability scanner it was possible to identify the weaknesses in the Use Cases proposed for the Cloud, calculate the rav for each model and compare with the baseline model to assess how security was impacted. The Use Cases were designed to be generic, containing solutions that use Kerberos for single sign-on by means of supported and documented configurations and without the requirement to change application code or programming.

The numbers obtained and presented on section 0 are a good indicator that Cloud is technically viable for using Kerberos for single sign-on authentication by organizations. Although we understand that more Use Cases security assessments may be required to support a generic and wide accepted method such as the proposed in this work, we also understand that the Use Cases analyzed are generic and are using wide spread software and protocols, thus being very good representatives of actual and diverse solutions.

In line with the above argument, a good improvement for this work would be to identify more Use Cases to assess and apply the method on different Cloud providers – a huge challenge if commercial Cloud providers are approached. Besides that, the use of the full OSSTMM methodology can be applied, therefore, requiring the identification of all controls implemented in each Use Case with the benefit of reducing error margin and providing a more comprehensive view of the Cloud security operations.

The method to assess the systems security can also be improved by using several tools, and the results correlated and combined to have a more complete set of metrics. This aspect would benefit much from tools that can analyze Cloud virtualization solutions, such as shared memory and storage, disk wiping techniques and processes, virtual networking and tenant isolation, among others. These aspects are intrinsically related with virtualization, and therefore, influence directly or indirectly the Cloud security.

The subject of this work involved several different technologies, being clearly a multi-disciple work that required research in several IT-related fields such as authentication, operating systems, protocols and Cloud computing. This multidisciplinary characteristic of the investigation provides opportunities to publish academic research papers in some of these fields, which the author intends to pursue in the future. Indeed, during the development of this thesis one paper was submitted and accepted for an international conference about Information Systems and Security. The paper “Enterprise to Cloud Security Assessment – A Method Using OSSTMM 3.0

Concepts” describes the method used to validate the models in this master thesis and was presented at “5th. International Conference on Knowledge Management and Information Sharing – KMIS2013”, in Vilamoura, Algarve, published in the conference proceedings.

Bibliographic References

Foley, Mary Jo (2010), “Behind the IDC data: Windows still No. 1 in server operating systems”, (Online). Available at: http://www.zdnet.com/blog/microsoft/behind-the-idc-data-windows-still-no-1-in-server-operating-systems/5408

De Clercq, Jan (2004), Windows Server 2003 Security Infrastructures, MA, Elsevier.

OASIS (2005), “Security Assertion Markup Language (SAML) v2.0”, (Online).
Available at: http://www.oasis-open.org/standards#samlv2.0, (Downloaded in 19/02/2012).

IETF (2010), Hammer-Lahav , E. (2010), “RFC5849 - The OAuth 1.0 Protocol”, Internet Engineering Task Force (IETF), Request for Comments: 5849, April 2010, ISSN: 2070-1721., (Online).
Available at: https://tools.ietf.org/html/rfc5849

OpenID (2012), “What Is OpenID”, (Online).
Available at: http://openid.net/get-an-openid/what-is-openid

Yildiz, Mehmet et al (2009), “A Layered Security Approach for Cloud Computing Infrastructure”, 2009 10th International Symposium on Pervasive Systems Algorithms, and Networks, IEEE 978-0-7695-3908-9/09, p.763-767.

Garman, Jason (2003), Kerberos The Definitive Guide, CA, O’Reilly.

NIST (2011), “The NIST Definition of Cloud Computing”, National Institute of Standards and Technology – U.S Department of Commerce, NIST Special Publication 800-145 (Online).
Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Cloud Computing Use Cases Group (2010), “Cloud Computing Use Cases Version 4.0” (Online). Available at: http://cloudusecases.org

OASIS (2006), “Service Provisioning Markup Language (SPML) v2.0”, (Online).
Available at: http://www.oasis-open.org/standards#spmlv2.0

Daniels, Jeff (2011), Assured Identity for the Cloud, Dissertation for the Degree of Doctor in Philosophy, Indiana State University, Terre Haute, Indiana.

Casola, Valentina et al (2010), “Identity Federation in Cloud Computing", Sixth International Conference on Information Assurance and Security, Aug. 2010, (Online).
Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5604074

Neuman, Clifford et al (2005), “RFC4121 - The Kerberos Network Authentication Service (V5)”, Internet Engineering Task Force (IETF), Request for Comments: 4121, July 2005, (Online). Available at: http://www.ietf.org/rfc/rfc4120.txt

Needham, Roger M. and Michael D. Schroeder (1978), “Using Encryption for Authentication in Large Networks of Computers”, Communications of the ACM, August 1978 Volume 21 Number 12, Xerox Palo Alto Research Center.

Denning, Dorothy E. and Giovanni Maria Sacco (1981), “Timestamps in Key Distribution Protocols”, Communications of the ACM, August 1981 Volume 24 Number 8, Purdue University.

Tsay, Joe-Kai (2008), Formal Analysis of the Kerberos Authentication Protocol, Dissertation for the Degree of Doctor in Mathematics, Pennsylvania , University of Pennsylvania.

Bella, Giampaolo and Elvinia Riccobene (1997), “Formal Analysis of the Kerberos Authentication System”, Journal of Universal Computer Science, vol. 3, no. 12 (1997), pp.1337-1381.

Butler, Frederick et al (2006), “Formal analysis of Kerberos 5”, Theoretical Computer Science 367 (2006), pp.57–87.

Butler, Frederick et al (2004), “A Formal Analysis of Some Properties of Kerberos 5 Using MSR”, Department of Computer & Information Science Technical Reports (CIS), University of Pennsylvania, 2004

Backes, M. et al (2006), “Cryptographically Sound Security Proofs for Basic and Public-Key Kerberos”, D. Gollmann, J. Meier, and A. Sabelfeld (Eds.): ESORICS 2006, LNCS 4189, pp.362–383.

Pashalidis, Andreas and Chris J. Mitchell (2003), “A Taxonomy of Single Sign-On Systems”, in R. Safavi-Naini and J. Seberry (Eds.): ACISP 2003, LNCS 2727, pp. 249–264, University of London, Egham, Surrey, United Kingdom.

Jensen, Meiko et al (2009), “On Technical Security Issues in Cloud Computing”, 2009 IEEE International Conference on Cloud Computing, pp. 109-116.

Huan-Chung-li et al (2010), “Analysis on Cloud-Based Security Vulnerability Assessment “, IEEE International Conference on E-Business Engineering, 978-0-7695-4227-0/10, p. 490-494.

Coelho, Paulo (2007), Security Certification for Organizations: A Framework to Manage Information Security, Dissertation for the Degree of Master in Management of Information Systems, Lisboa, ISCTE.

NIST (2010), “Special Publication 800-53 - A Guide for Assessing the Security Controls in Federal Information Systems and Organizations Building Effective Security Assessment Plans, Revision 1, June 2010”, (Online). Available at: http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

Alberts, Christopher J. and Audrey J. Dorofee (2001), “OCTAVE Method Implementation Guide Version 2.0, Volume 1: Introduction”, Carnegie Mellon University, (Online). Available at: http://www.cert.org/octave/octavemethod.html

Caralli, Richard A. et al (2007b), “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process”, TECHNICAL REPORT CMU/SEI-2007-TR-012 ESC-TR-2007-012, Carnegie Mellon, (Online). Available at: http://www.cert.org/archive/pdf/07tr012.pdf

Herzog, Pete (2010), “OSSTMM 3 – The Open Source Security Testing Methodology Manual – Contemporary Security Test and Analysis”, Institute for Security and Open Methodologies (ISECOM), (Online). Available at: http://www.isecom.org/mirror/OSSTMM.3.pdf

Herzog, Pete (2011), “Analyzing the Biggest Bank Robbery in History: Lessons in OSSTMM Analysis”, Online Banking Magazine, 2/2011, (Onine). Available at: http://hakin9.org/analyzing-the-biggest-bank-robbery-in-history-lessons-in-osstmm-analysis/

Rathore, Balwant et al (2006), “Information Systems Security Assessment Framework (ISSAF)”, Draft v0.2.1, 2006, OISSG, (Online). Available at: http://www.oissg.org/issaf

CSA (2009), “Security Guidance for Critical Areas of Focus in Cloud Computing 2.1”, Cloud Security Alliance, (Online). Available at: www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

U.S. Chief Information Officer (2010), “Proposed Security Assessment and Authorization for U.S. Government Cloud Computing”, (Online). Available at: http://educationnewyork.com/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf

CERT (2011), “2011 CyberSecurityWatch Survey - How Bad Is the Insider Threat?”, Carnegie Mellon University, (Online). Available at: http://www.cert.org/archive/pdf/CyberSecuritySurvey2011Data.pdf

Hiroyuki, Sato et al (2011), “Building a Security Aware Cloud by Extending Internal Control to Cloud”, 2011 Tenth International Symposium on Autonomous Decentralized Systems, IEEE 978-0-7695-4349-9/11, p. 323-326.

Zúquete, André (2010), Segurança em Redes Informáticas – 3ª Ed. Act. E Aum., Lisboa, FCA Editora de Informática.

OASIS (2012), “Identity in the Cloud Use CasesVersion1.0, Committee Note 01, 08 May 2012”, (Online). Available at:http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/cn01/IDCloud-usecases-v1.0-cn01.html

MIT (2010), “Kerberos In The Cloud - Use Case Scenarios” (Online).
Available at: https://www.oasis-open.org/committees/download.php/38245/Kerberos-Cloud-use-cases-11june2010.pdf

Microsoft (2011a), “AD DS: Read-Only Domain Controllers”, (Online). Available at: http://technet.microsoft.com/en-us/library/cc732801(v=ws.10).aspx

Krutz, Ronald L. and Vines, Russel D. (2010), Cloud Security: A Comphrehensive Guide to Secure Cloud Computing, Indianápolis, Wiley Publishing.

Bernd Grobauer, Tobias Walloschek, Elmar Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security & Privacy, vol. 9, no. 2, pp. 50-57, March-April 2011, doi:10.1109/MSP.2010.115, (Online). Available at: http://www.computer.org/csdl/mags/sp/2011/02/msp2011020050-abs.html

Wilhelm, Thomas (2010), Professional Penetration Testing, Burlington, Elsevier Inc.

MacClure, Stuart et al (1999), Hacking Exposed: Network Security Secrets and Solutions, California, Oxborne.

Microsoft (2012a),“Using Kerberos Integrated Authentication to Connect to SQL Server”, (Online). Available at: http://msdn.microsoft.com/en-us/library/gg558122.aspx

Microsoft (2012b), “Guidelines for Deploying Windows Server Active Directory on Windows Azure Virtual Machines”, (Online). Available at: http://msdn.microsoft.com/en-us/library/windowsazure/jj156090.aspx

Microsoft (2012c), “Create a Virtual Network for Cross-Premises Connectivity”, (Online). Available at: https://www.windowsazure.com/en-us/manage/services/networking/cross-premises-connectivity

Microsoft (2012d), “Install a Replica Active Directory Domain Controller in Windows Azure Virtual Networks”, (Online). Available at: https://www.windowsazure.com/en-us/manage/services/networking/replica-domain-controller

Microsoft (2013a) “Configure Windows Authentication (IIS 7), (Online). Available at: http://technet.microsoft.com/en-us/library/cc754628

Microsoft (2013b), “How to use Kerberos authentication in SQL Server”, (Online). Available at: http://support.microsoft.com/kb/319723

Caralli, Richard A. et al (2007), “The OCTAVE Allegro Guidebook, v1.0”, Carnegie Mellon, (Online). Available at: http://www.cert.org/octave/allegro.html

OWASP (2012), “Cloud Top 10 Security Risks”, (Online).
Available at: https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project

Linn, J. (2000), “Generic Security Service Application Program Interface Version 2, Update 1”, Internet Engineering Task Force (IETF), Request for Comments: 2743, January 2000, (Online). Available at: http://tools.ietf.org/html/rfc2743

faqs.org (2000), “Kerberos FAQ, v2.0 Section -5.2. What is GSSAPI?”, (Online). Available at: http://www.faqs.org/faqs/kerberos-faq/general/section-84.html

Cloud Security Alliance (2009), “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”, (Online). Available at: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

IBM (2012), “Kerberos (KRB5) authentication mechanism support for security“, (Online). Available at: http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.doc%2Finfo%2Fae%2Fae%2Fcsec_kerb_auth_explain.html

Oracle (2012), “How To Configure Browser-based SSO with Kerberos/SPNEGO and Oracle WebLogic Server”, (Online). Available at: http://www.oracle.com/technetwork/articles/idm/weblogic-sso-kerberos-1619890.html

Wilson, Piers (2011), “Positive perspectives on cloud security”, Information Security Technical Report 16(2011), Elsevier, pp. 97-101.

Tanenbaum, Andrew S. (2003), Rede de Computadores, Rio de Janeiro, Elsevier.

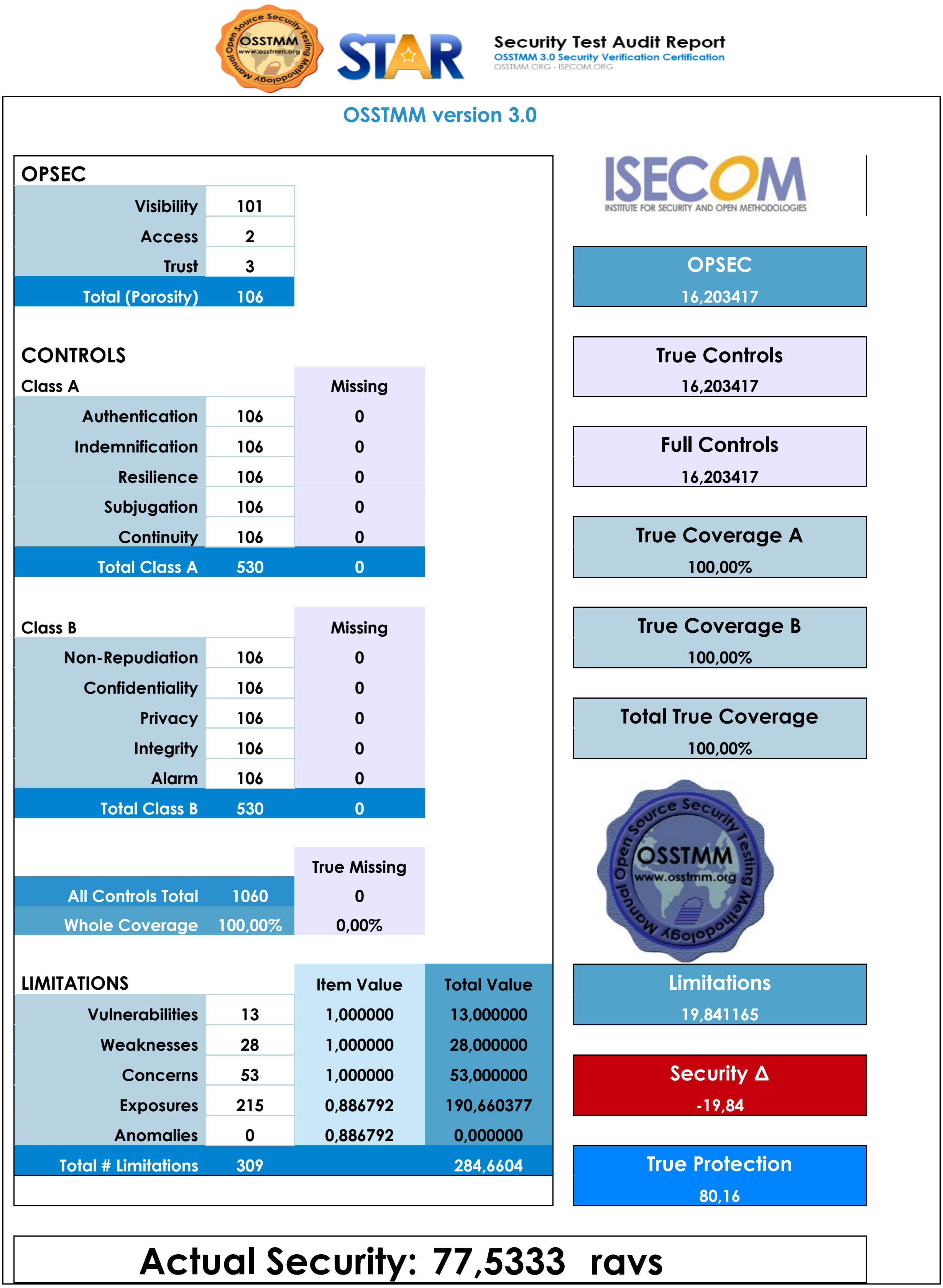
Annex A – Kerberos-compatible Applications

Category	Name	References
Operating System and Platforms	IBM AIX (operating system)	http://pic.dhe.ibm.com/infocenter/aix/v7r1/index.jsp?topic=%2Fcom.ibm.aix.security%2Fdoc%2Fsecurity%2Fkerberos_install_config_krb5.htm
	Unisys Clearpath (mainframe system	http://public.support.unisys.com/aseries/docs/clearpath-mcp-12.1/pdf/88078878-005.pdf and http://www.unisys.com/unisys/inc/pdf/misc/MCP13.1Webinar.pdf
	iSeries (OS/400, mini supercomputer)	http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=%2Frzamz%2Frzamzenablesso.htm
	Linux	http://www.centos.org/docs/5/html/Deployment_Guide-en-US/ch-kerberos.html
	Mac OS X	http://support.apple.com/kb/TA20987 and http://web.mit.edu/macdev/www/osx-kerberos-extras.html
	Windows	http://technet.microsoft.com/en-us/library/cc753173(v=ws.10).aspx
	IBM z/OS (mainframe system)	http://publibz.boulder.ibm.com/epubs/pdf/euvb3a20.pdf and http://publib.boulder.ibm.com/infocenter/zos/v1r11/index.jsp?topic=/com.ibm.zos.r11.euvfa00/euvb3a7005.htm and http://www.vm.ibm.com/devpages/spera/zJJune08.pdf
HTTP / Web Server	Apache HTTP Server	http://acksyn.org/?p=460 and http://hc.apache.org/httpcomponents-client-ga/tutorial/html/authentication.html and http://wiki.centos.org/HowTos/HttpKerberosAuth and http://support.microsoft.com/kb/555092
	Microsoft IIS HTTP Server	http://support.microsoft.com/kb/326089 and http://technet.microsoft.com/en-us/library/cc754628(v=ws.10).aspx and http://support.microsoft.com/kb/215383

Java/Web Application Server	Glassfish Geronimo JBoss IBM WebSphere Application Server Oracle WebLogic SAP NetWeaver	http://metro.java.net/2.0/guide/_Configuring_Kerberos_for_Glassfish_and_Tomcat.html https://cwiki.apache.org/GMOxDOC21/configuring-kerberos-realm.html http://support.sas.com/resources/thirdpartysupport/v92m2/appservers/IWAJBoss.pdf https://docs.jboss.org/author/display/GTNPORTAL35/SPNEGO http://www.redbooks.ibm.com/abstracts/sg247771.html and http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=%2Fcom.ibm.websphere.express.doc%2Finfo%2Fexp%2Fae%2Fcsec_kerb_auth_explain.html http://www.oracle.com/technetwork/articles/idm/weblogic-sso-kerberos-1619890.html http://help.sap.com/saphelp_nw70ehp1/helpdata/en/43/4bd58c6c5e5f34e10000000a1553f6/content.htm and http://help.sap.com/saphelp_nwce10/helpdata/en/43/847c65725e7104e10000000a1553f7/content.htm and http://scn.sap.com/community/netweaver-sso/blog/2012/08/17/how-to-configure-sap-netweaver-single-sign-on-for-sap-gui-for-windows-with-kerberos-integration http://tomcat.apache.org/tomcat-7.0-doc/windows-auth-howto.html and http://jaaslounge.sourceforge.net/howto/SSO_Tomcat_Howto.pdf
Databse Systems	DB2 MS SQL Server Oracle	http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp?topic=%2Fcom.ibm.db2.luw.admin.sec.doc%2Fdoc%2Fc0011990.html http://technet.microsoft.com/en-us/library/cc280744(v=sql.105).aspx and http://msdn.microsoft.com/en-us/library/cc280745(v=sql.105) http://docs.oracle.com/cd/A97630_01/network.920/a96573/asokerb.htm

TCPIP Applications	ftp on Mainframe (z/OS)	http://publib.boulder.ibm.com/infocenter/zos/v1r11/index.jsp?topic=/com.ibm.zos.r11.halz002/cftpker.htm
	ssh	http://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch11_04.htm and http://www.openbsd.org/cgi-bin/man.cgi?query=sshd_config&sektion=5 and http://www.openssh.com/features.html
	Putty	http://tig.csail.mit.edu/wiki/TIG/InstallingKerberosForWindows#Using_Kerberos_with_SSH and http://rc.quest.com/topics/putty/
	MobaXterm	http://mobaxterm.mobatek.net/
	WinSCP	http://winscp.net/eng/docs/ui_login_authentication#attempt_gssapi_authentication and http://winscp.net/eng/docs/ssh
	Basic TCPIP tools (telnet, ftp, rlogin, rsh, rcp, ksu)	http://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-user/Kerberos-V5-Applications.html#Kerberos-V5-Applications
Content Management, Portals and Web	DRUPAL	http://drupal.org/project/kerberos_authentication
	PHP	http://sammoffatt.com.au/jauthtools/Kerberos/Configuring_Apache_To_Authenticate_PHP_Documents and http://php.net/manual/en/book.kadm5.php
	Sharepoint	http://www.microsoft.com/en-us/download/details.aspx?id=23176
Generic Applications	CUPS Printing Service	http://www.cups.org/documentation.php/kerberos.html
	IBM Tivoli Access Management	http://www.ibm.com/developerworks/tivoli/library/t-tamwkj/

Annex B – STAR Report - Baseline Model



STAR

Security Test Audit Report

OSSTMM 3.0 Security Verification Certification

OSSTMM.ORG - ISECOM.ORG

OSSTMM version 3.0

OPSEC		
Visibility	101	
Access	2	
Trust	3	
Total (Porosity)	106	

CONTROLS

Class A		Missing
Authentication	106	0
Indemnification	106	0
Resilience	106	0
Subjugation	106	0
Continuity	106	0
Total Class A	530	0

Class B		Missing
Non-Repudiation	106	0
Confidentiality	106	0
Privacy	106	0
Integrity	106	0
Alarm	106	0
Total Class B	530	0

		True Missing
All Controls Total	1060	0
Whole Coverage	100,00%	0,00%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	13	1,000000	13,000000
Weaknesses	28	1,000000	28,000000
Concerns	53	1,000000	53,000000
Exposures	215	0,886792	190,660377
Anomalies	0	0,886792	0,000000
Total # Limitations	309		284,6604

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC
16,203417

True Controls
16,203417

Full Controls
16,203417

True Coverage A
100,00%

True Coverage B
100,00%

Total True Coverage
100,00%

Limitations
19,841165

Security Δ
-19,84

True Protection
80,16

Actual Security: 77,5333 ravs

Attack Vectors – Baseline Model

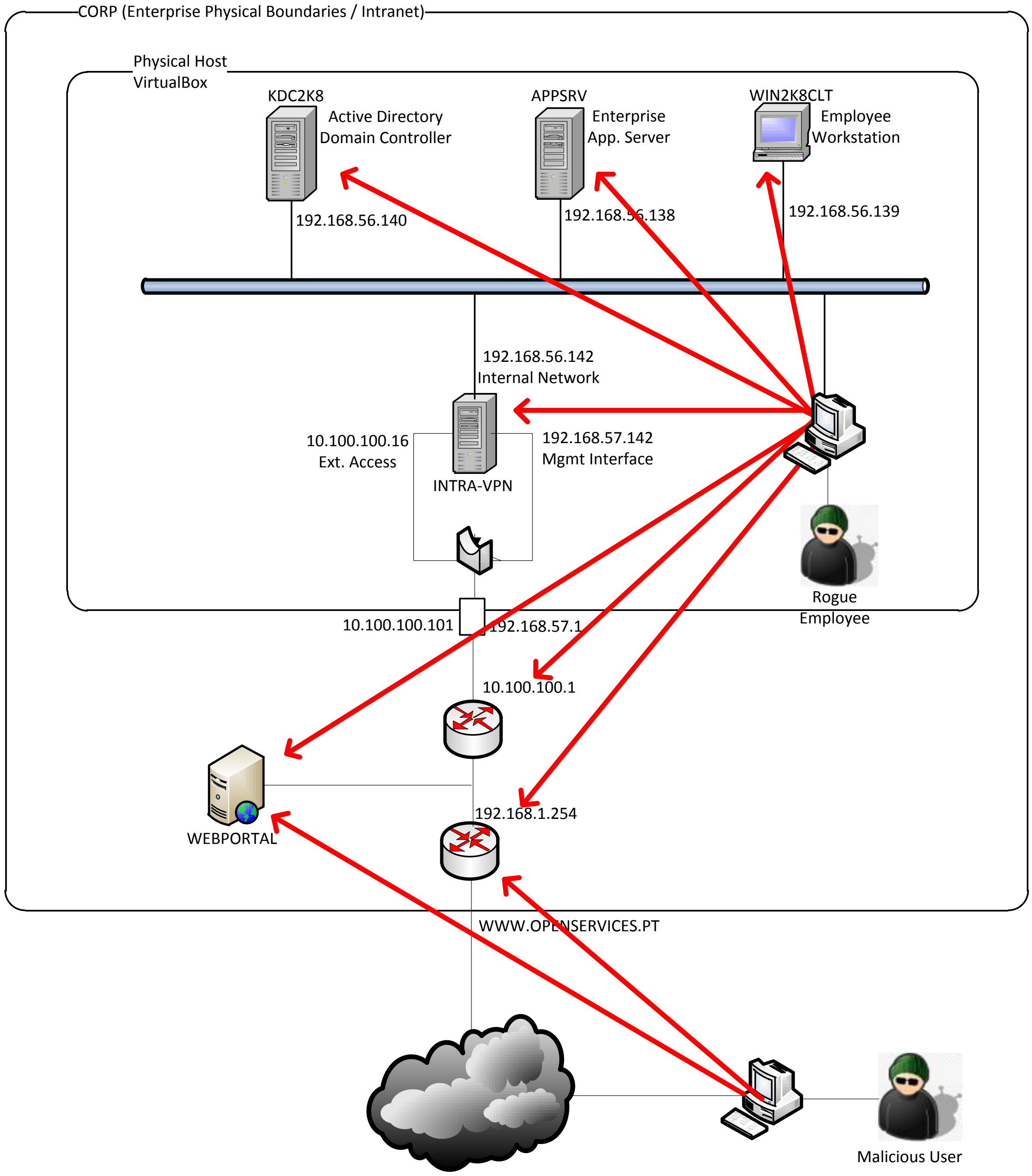


Figure 18: The Architecture and Attack Vectors

Legend:

→ Attack Vector

A. Induction Phase

Module		Findings
A.1	Posture Review	External web server is the only exposed service to the public; No services is provided for roaming employees;
A.2	Logistics	The intranet servers run in VirtualBox instances. The virtual instances communicate with each other using the “internal network” feature of the VirtualBox. The internal network communicates with the outside world via a router (linux), wich has three interfaces: internal network / bridged network / management network. To access any server in this network, one must go through the management interface (accessible only from the Host) or via the bridged interface (see Figure 1).
A.3	Active Detection Verification	Concerns to the verification of filtered ports, audit logs and event console for monitoring intrusion.

B. Interaction Phase

Module		Findings
B.4	Visibility Audit	All servers in the scope count for the visibility. Each open TCP/UDP port for each server also count as a value. The total number of servers plus the sum of all open ports for all servers is the final value assigned to visibility.
B.5	Access Verification	Every controlled access to a resources is taken into account, including domain authentication and the appsrv.corp.intranet authentication.
B.6	Trust Verification	Access to resources without requiring authentication was accounted: public webportal access, appsrv root web page, Kerberos trust between appsrv and the KDC.
B.7	Control Verification	It was assigned default controls for all interaction points and visibility points.

C. Inquest Phase

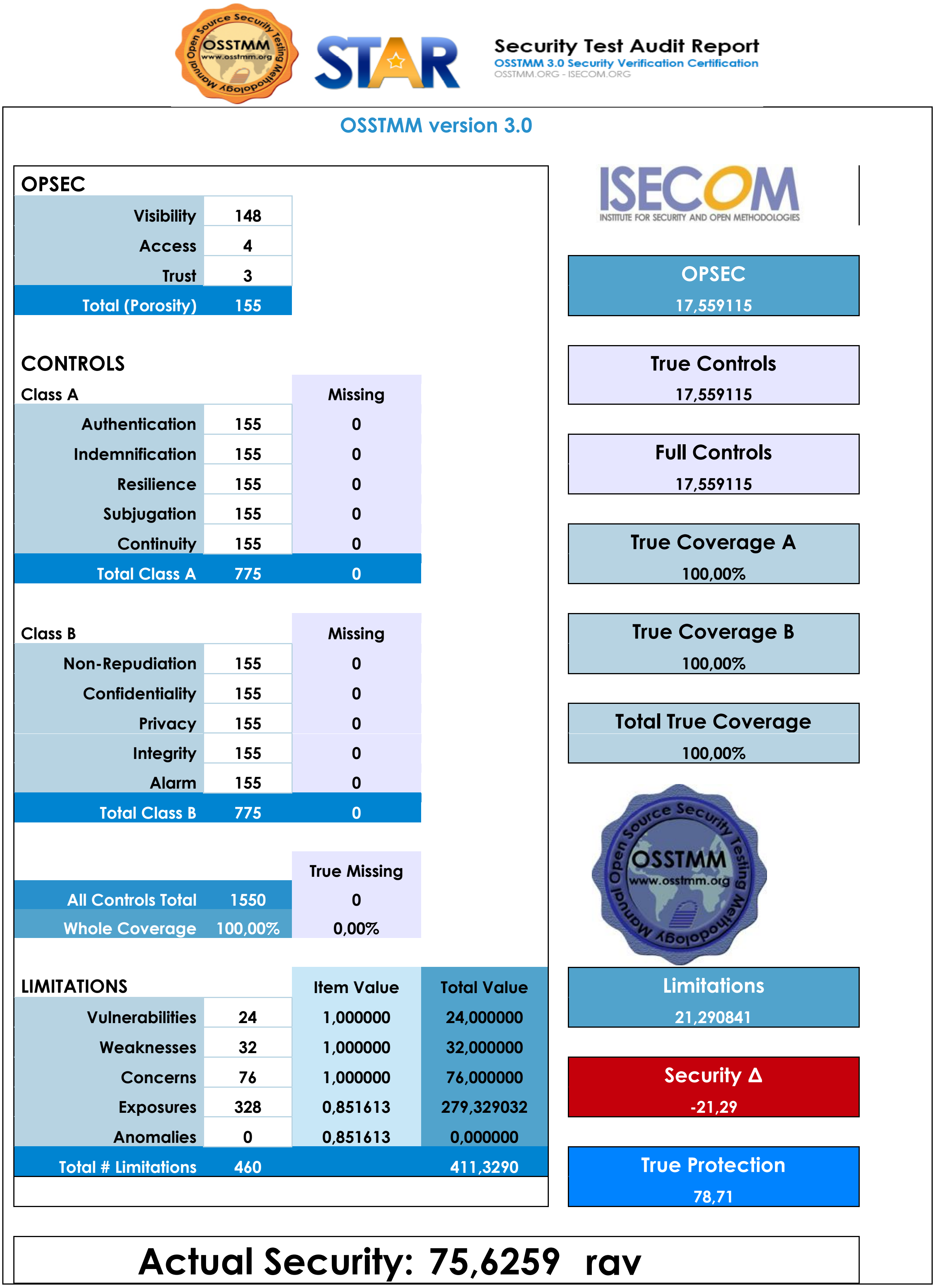
Module		Findings
C.8	Process Verification	Does not appy.
C.9	Configuration Verification / Training Verification	Does not apply.
C.10	Property Validation	Does not apply.
C.11	Segregation Review	Does not apply.
C.12	Exposure Review	Does not apply.
C.13	Competitive Intelligence Scouting	Does not apply.

D. Intervention Phase

Module		Findings
D.14	Quarantine Verification	Does not apply.
D.15	Privilege Audit	Does no apply.
D.16	Survivability	Does not apply.

	Validation / Service Continuity	
D.17	Alert and Log Review / End Survey	It was assigned default values for these controls.

Annex C – STAR Report: Cloud Use Case 1



Security Test Audit Report

OSSTMM 3.0 Security Verification Certification

OSSTMM.ORG - ISECOM.ORG

OSSTMM version 3.0

OPSEC	
Visibility	148
Access	4
Trust	3
Total (Porosity)	155

CONTROLS

Class A		Missing
Authentication	155	0
Indemnification	155	0
Resilience	155	0
Subjugation	155	0
Continuity	155	0
Total Class A	775	0

Class B		Missing
Non-Repudiation	155	0
Confidentiality	155	0
Privacy	155	0
Integrity	155	0
Alarm	155	0
Total Class B	775	0

		True Missing
All Controls Total	1550	0
Whole Coverage	100,00%	0,00%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	24	1,000000	24,000000
Weaknesses	32	1,000000	32,000000
Concerns	76	1,000000	76,000000
Exposures	328	0,851613	279,329032
Anomalies	0	0,851613	0,000000
Total # Limitations	460		411,3290

ISECOM

INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC	17,559115
True Controls	17,559115
Full Controls	17,559115
True Coverage A	100,00%
True Coverage B	100,00%
Total True Coverage	100,00%
Limitations	21,290841
Security Δ	-21,29
True Protection	78,71

Actual Security: 75,6259 rav

Attack Vectors – Cloud Use Case 1

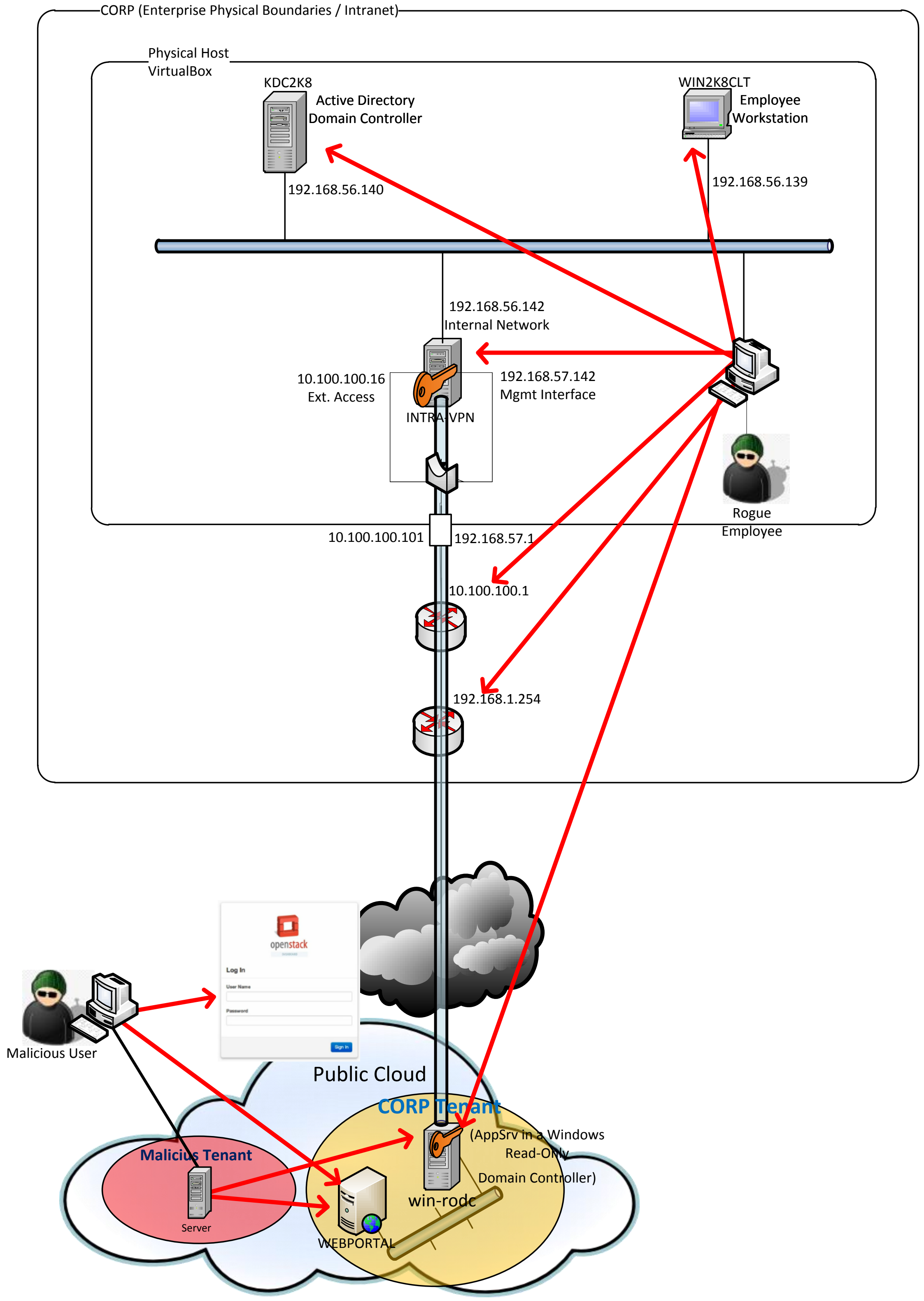


Figure 19: The Architecture and Attack Vectors

Legend:

→ Attack Vector

A. Induction Phase

Module		Findings
A.1	Posture Review	External web server is the only exposed service to the public; No services is provided for roaming employees;
A.2	Logistics	The intranet servers run in VirtualBox instances. The virtual instances communicate with each other using the “internal network” feature of the VirtualBox. The internal network communicates with the outside world via a router (linux), wich has three interfaces: internal network / bridged network / management network. To access any server in this network, one must go through the management interface (accessible only from the Host) or via the bridged interface (see Figure 1).
A.3	Active Detection Verification	Concerns to the verification of filtered ports, audit logs and event console for monitoring intrusion, which was verified using the OpenVAS security assessment tool.

B. Interaction Phase

Module		Findings
B.4	Visibility Audit	All servers in the scope count for the visibility. Each open TCP/UDP port for each server also count as a value. The total number of servers plus the sum of all open ports for all servers is the final value assigned to visibility.
B.5	Access Verification	Every controlled access to a resources is taken into account, including domain authentication, private application server authentication, Cloud management dashboard authentication, VPN authentication.
B.6	Trust Verification	Access to resources without requiring authentication was accounted: public webportal access, private application server root web page, Kerberos trust between application server and the KDC.
B.7	Control Verification	It was assigned default controls for all interaction points and visibility points (OSSTMM p. 67-68).

C. Inquest Phase

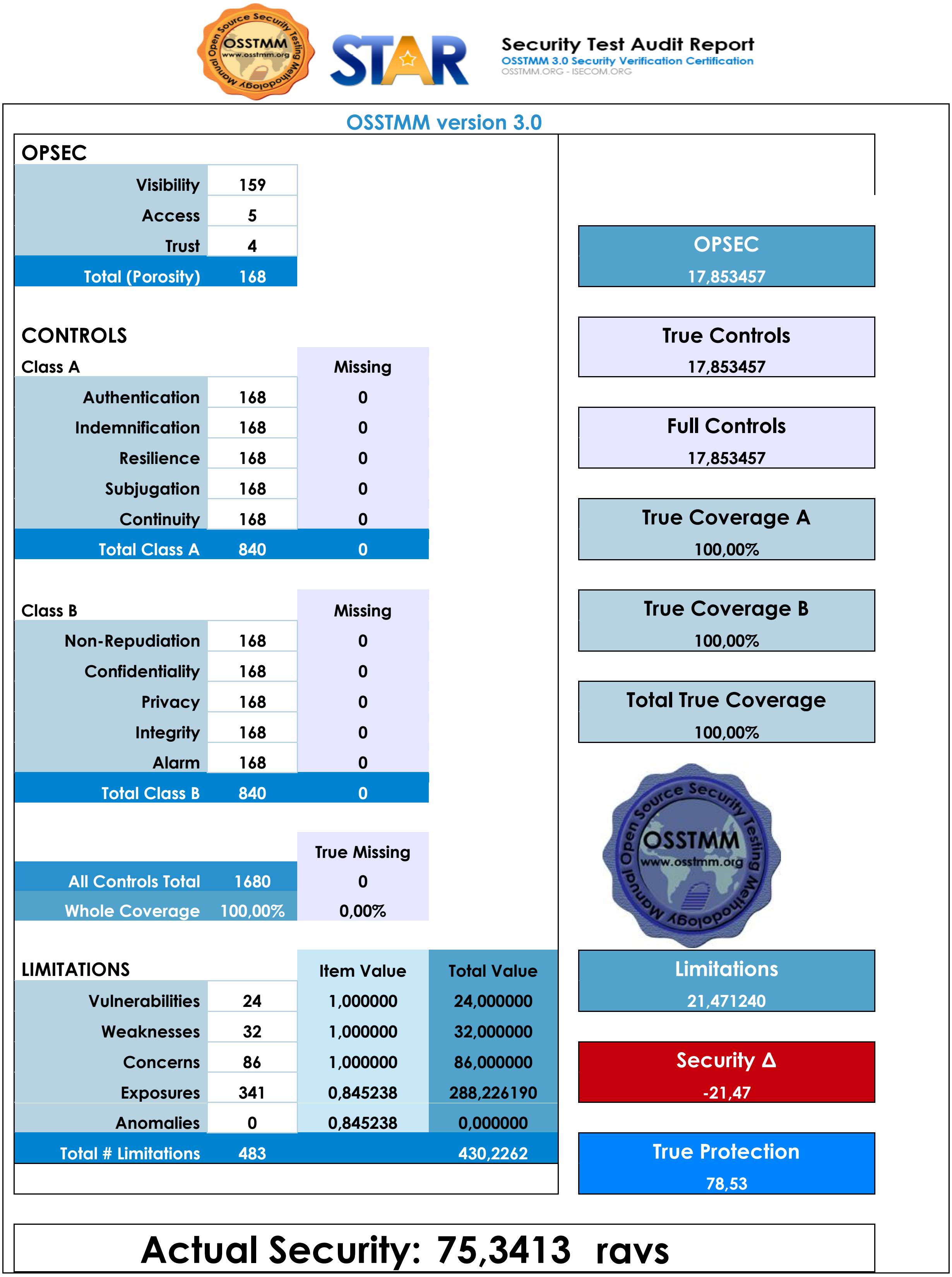
Module		Findings
C.8	Process Verification	Does not appy.
C.9	Configuration Verification / Training Verification	Does not apply.
C.10	Property Validation	Does not apply.
C.11	Segregation Review	Does not apply.
C.12	Exposure Review	Does not apply.
C.13	Competitive Intelligence Scouting	Does not apply.

D. Intervention Phase

Module		Findings
D.14	Quarantine	Does not apply.

	Verification	
D.15	Privilege Audit	Does no apply.
D.16	Survivability Validation / Service Continuity	Does not apply.
D.17	Alert and Log Review / End Survey	It was assigned default values for these controls (OSSTMM p. 67-68).

Annex D - STAR Report: Cloud Use Case 2



Security Test Audit Report
OSSTMM 3.0 Security Verification Certification
OSSTMM.ORG - ISECOM.ORG

OSSTMM version 3.0

OPSEC

Visibility	159
Access	5
Trust	4
Total (Porosity)	168

CONTROLS

Class A		Missing
Authentication	168	0
Indemnification	168	0
Resilience	168	0
Subjugation	168	0
Continuity	168	0
Total Class A	840	0

Class B		Missing
Non-Repudiation	168	0
Confidentiality	168	0
Privacy	168	0
Integrity	168	0
Alarm	168	0
Total Class B	840	0

		True Missing
All Controls Total	1680	0
Whole Coverage	100,00%	0,00%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	24	1,000000	24,000000
Weaknesses	32	1,000000	32,000000
Concerns	86	1,000000	86,000000
Exposures	341	0,845238	288,226190
Anomalies	0	0,845238	0,000000
Total # Limitations	483		430,2262

OPSEC	17,853457
True Controls	17,853457
Full Controls	17,853457
True Coverage A	100,00%
True Coverage B	100,00%
Total True Coverage	100,00%
Limitations	21,471240
Security Δ	-21,47
True Protection	78,53

Actual Security: 75,3413 ravs

Attack Vectors – Cloud Use Case 2

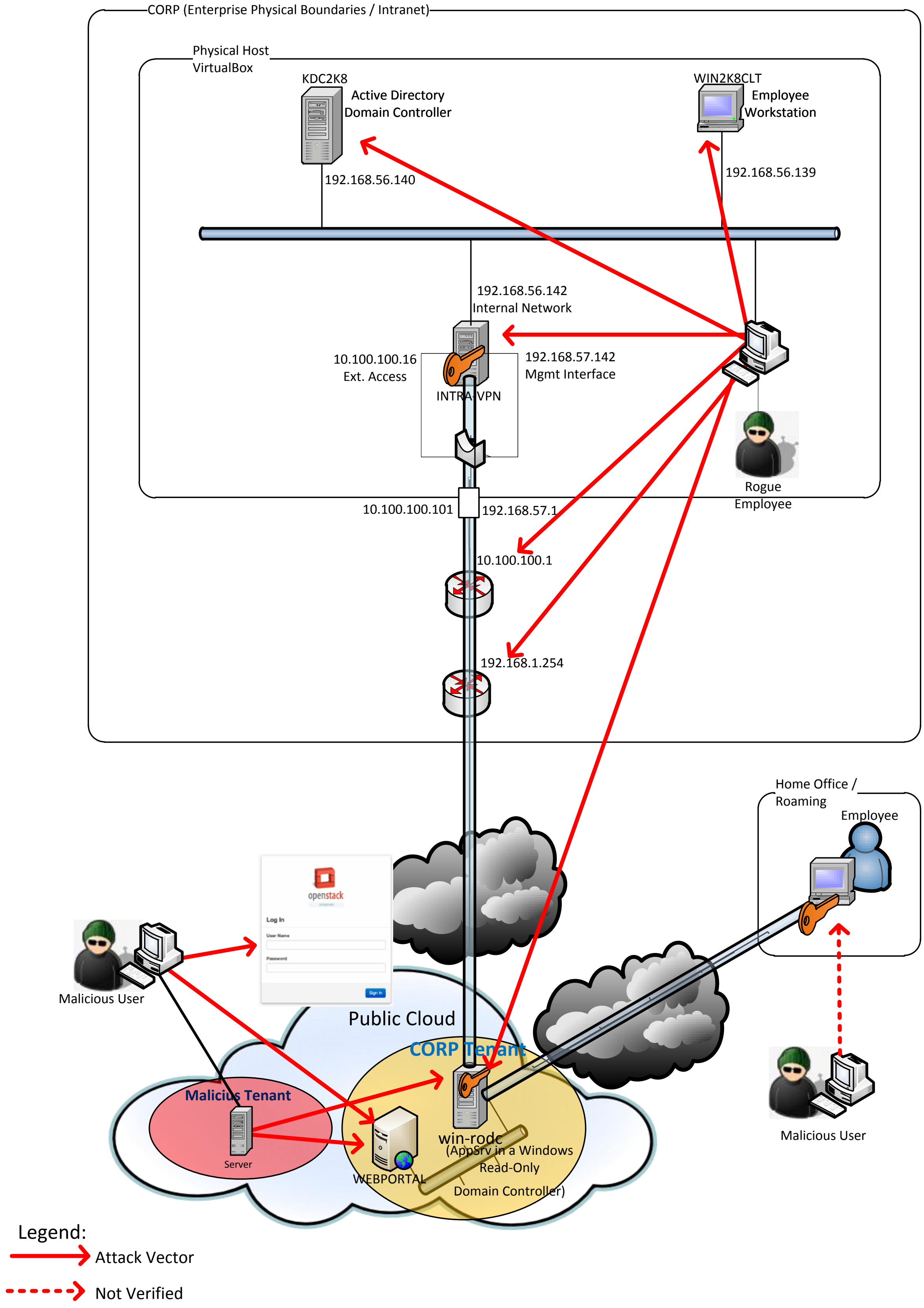


Figure 20: The Architecture and Attack Vectors

A. Induction Phase

Module		Findings
A.1	Posture Review	The webportal server hosts the enterprise public web server, which is openly accessible from the internet; A roaming service is available for employees, who can connect to the private appsrvcloud application server hosted in the Cloud, and running in the read-only domain controller. Employees connect to the appsrvcloud server using a VPN client; no other direct connection is available to the appsrvcloud other than using the VPN. There is no direct routing from the public web server in the Cloud to the enterprise intranet:
A.2	Logistics	The intranet servers run in VirtualBox instances. The virtual instances communicate with each other using the “internal network” feature of the VirtualBox. The internal network communicates with the outside world via a router (linux), wich has three interfaces: internal network / bridged network / management network. To access any server in this network, one must go through the management interface (accessible only from the Host) or via the bridged interface (see Figure 1).
A.3	Active Detection Verification	Concerns to the verification of filtered ports, audit logs and event console for monitoring intrusion, which was verified using the OpenVAS security assessment tool.

B. Interaction Phase

Module		Findings
B.4	Visibility Audit	All servers in the scope count for the visibility. Each open TCP/UDP port for each server also count as a value. The total number of servers plus the sum of all open ports for all servers is the final value assigned to visibility.
B.5	Access Verification	Every controlled access to a resources is taken into account, including domain authentication, private application server authentication, Cloud management dashboard authentication, VPN authentication.
B.6	Trust Verification	Access to resources without requiring authentication was accounted: public webportal access, private application server root web page, Kerberos trust between the application server, read-only domain controller and the KDC,
B.7	Control Verification	It was assigned default controls for all interaction points and visibility points (OSSTMM p. 67-68).

C. Inquest Phase

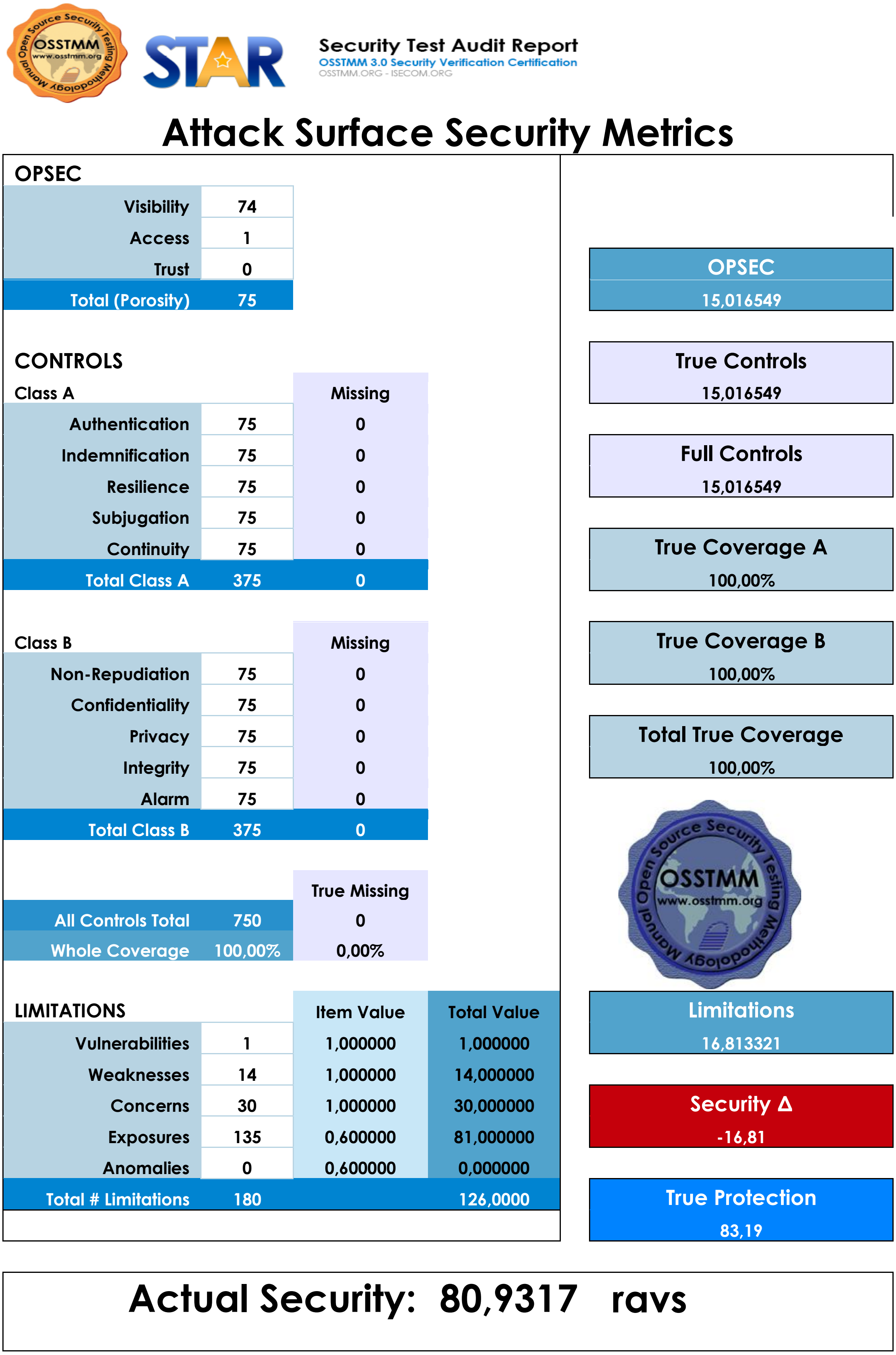
Module		Findings
C.8	Process Verification	Does not appy.
C.9	Configuration Verification / Training Verification	Does not apply.
C.10	Property Validation	Does not apply.

C.11	Segregation Review	Does not apply.
C.12	Exposure Review	Does not apply.
C.13	Competitive Intelligence Scouting	Does not apply.

D. Intervention Phase

Module		Findings
D.14	Quarantine Verification	Does not apply.
D.15	Privilege Audit	Does no apply.
D.16	Survivability Validation / Service Continuity	Does not apply.
D.17	Alert and Log Review / End Survey	It was assigned default values for these controls (OSSTMM p. 67-68).

Annex E - STAR Report: Baseline Model After Migration



Security Test Audit Report

OSSTMM 3.0 Security Verification Certification

OSSTMM.ORG - ISECOM.ORG

Attack Surface Security Metrics

OPSEC

Visibility	74
Access	1
Trust	0
Total (Porosity)	75

CONTROLS

Class A		Missing
Authentication	75	0
Indemnification	75	0
Resilience	75	0
Subjugation	75	0
Continuity	75	0
Total Class A	375	0

Class B		Missing
Non-Repudiation	75	0
Confidentiality	75	0
Privacy	75	0
Integrity	75	0
Alarm	75	0
Total Class B	375	0

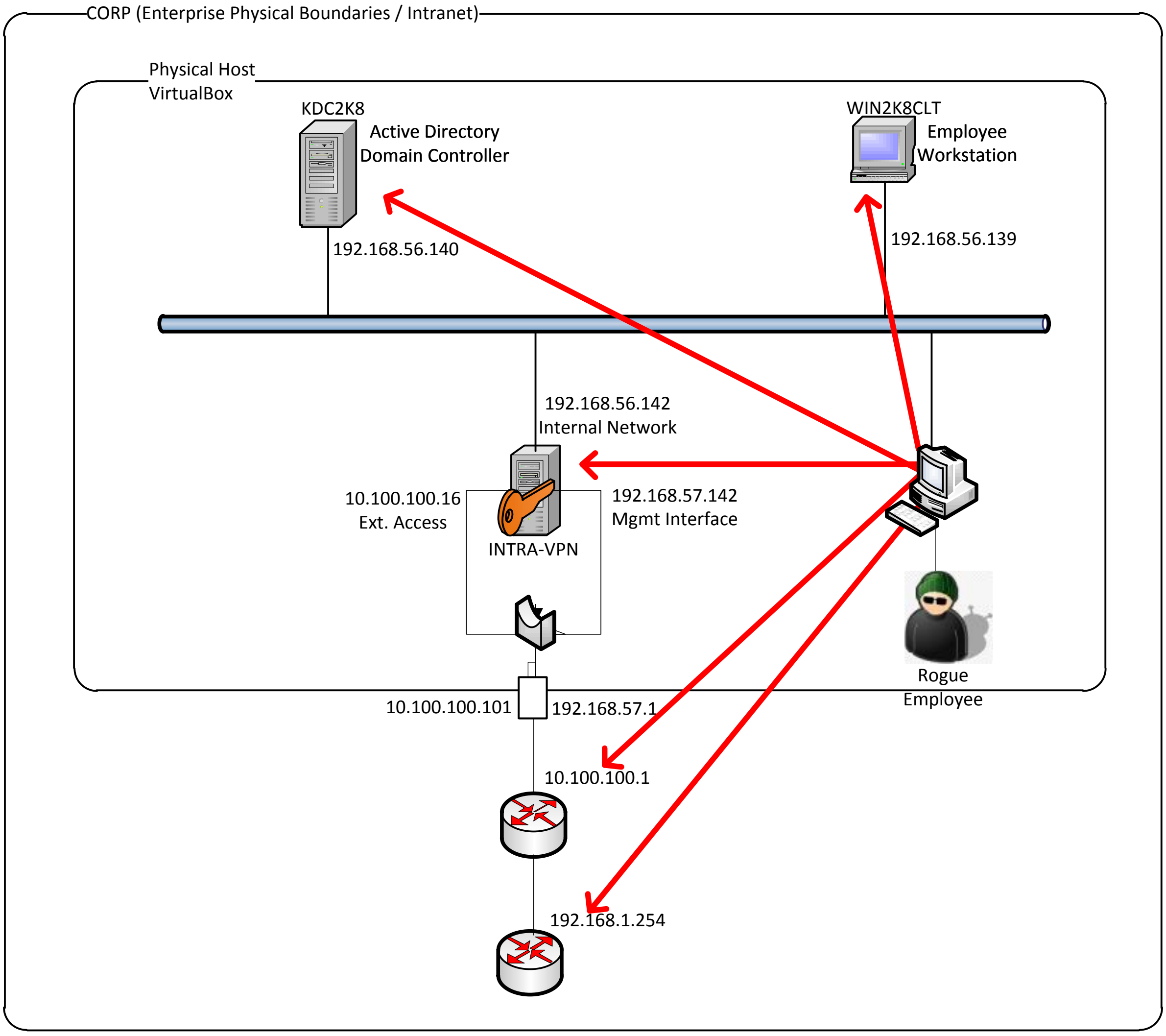
		True Missing
All Controls Total	750	0
Whole Coverage	100,00%	0,00%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	1	1,000000	1,000000
Weaknesses	14	1,000000	14,000000
Concerns	30	1,000000	30,000000
Exposures	135	0,600000	81,000000
Anomalies	0	0,600000	0,000000
Total # Limitations	180		126,0000

OPSEC	15,016549
True Controls	15,016549
Full Controls	15,016549
True Coverage A	100,00%
True Coverage B	100,00%
Total True Coverage	100,00%
Limitations	16,813321
Security Δ	-16,81
True Protection	83,19

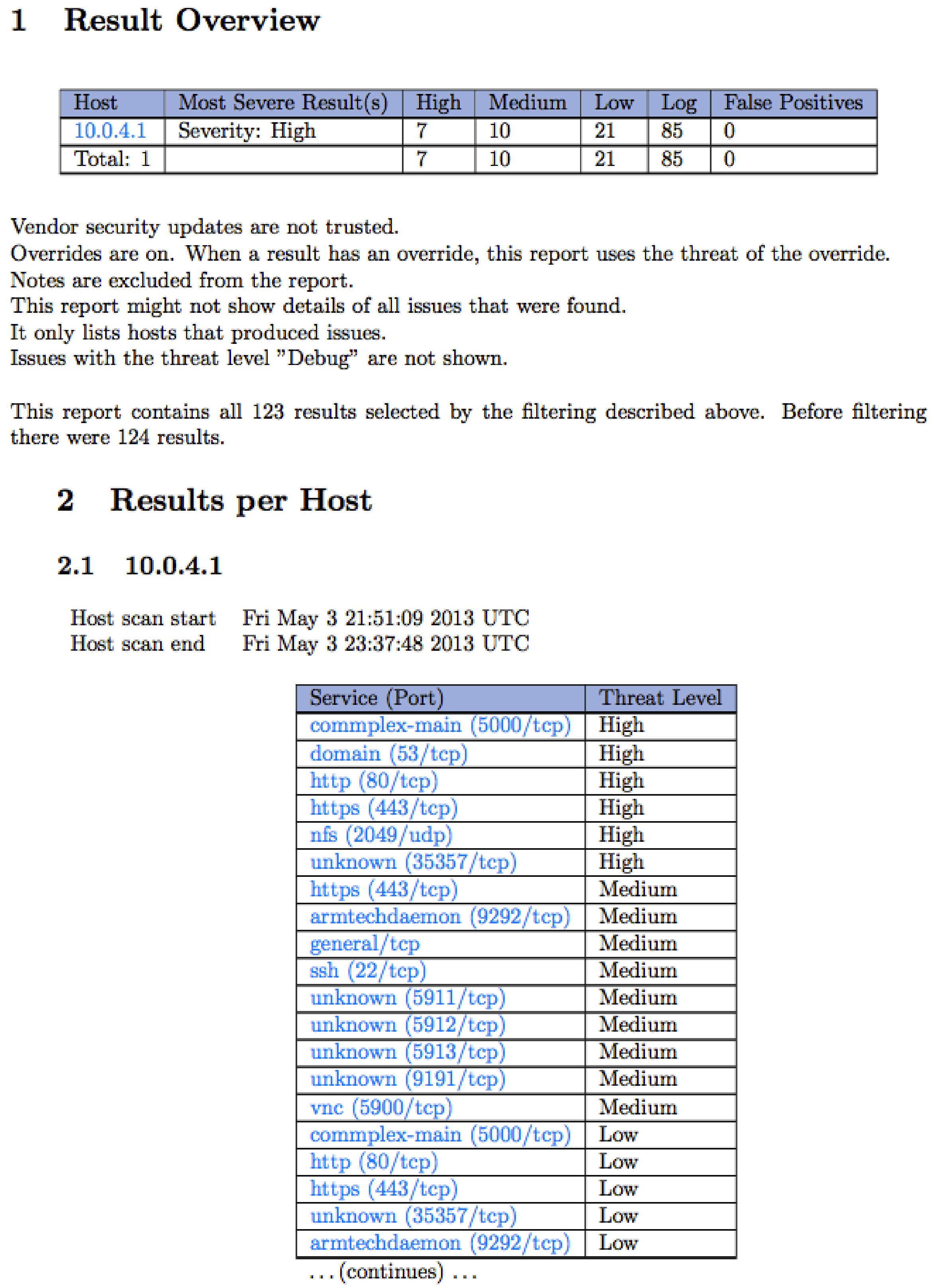
Actual Security: 80,9317 ravs

Attack Vectors – Base Line model After Migration



Annex F – OpenVAS Assessment Reports

E1 - 10.0.4.1 - Default router for the tenant in the Cloud



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
10.0.4.1	Severity: High	7	10	21	85	0
Total: 1		7	10	21	85	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are excluded from the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 123 results selected by the filtering described above. Before filtering there were 124 results.

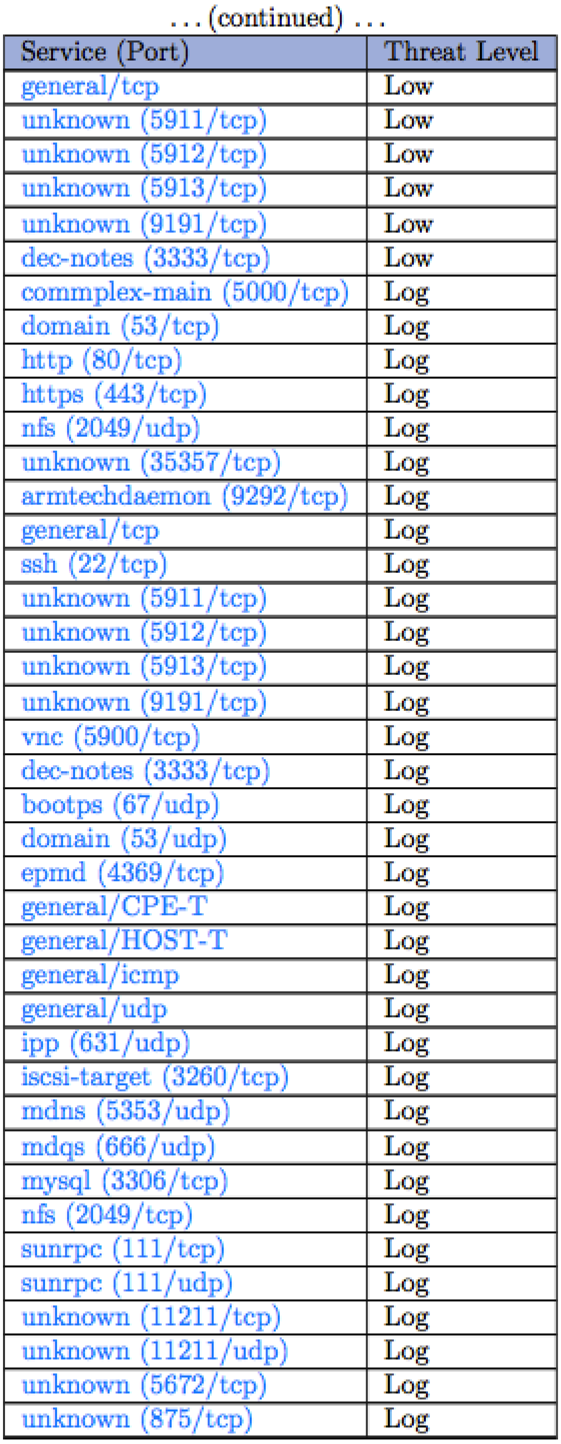
2 Results per Host

2.1 10.0.4.1

Host scan start	Fri May 3 21:51:09 2013 UTC
Host scan end	Fri May 3 23:37:48 2013 UTC

Service (Port)	Threat Level
commplex-main (5000/tcp)	High
domain (53/tcp)	High
http (80/tcp)	High
https (443/tcp)	High
nfs (2049/udp)	High
unknown (35357/tcp)	High
https (443/tcp)	Medium
armtechdaemon (9292/tcp)	Medium
general/tcp	Medium
ssh (22/tcp)	Medium
unknown (5911/tcp)	Medium
unknown (5912/tcp)	Medium
unknown (5913/tcp)	Medium
unknown (9191/tcp)	Medium
vnc (5900/tcp)	Medium
commplex-main (5000/tcp)	Low
http (80/tcp)	Low
https (443/tcp)	Low
unknown (35357/tcp)	Low
armtechdaemon (9292/tcp)	Low

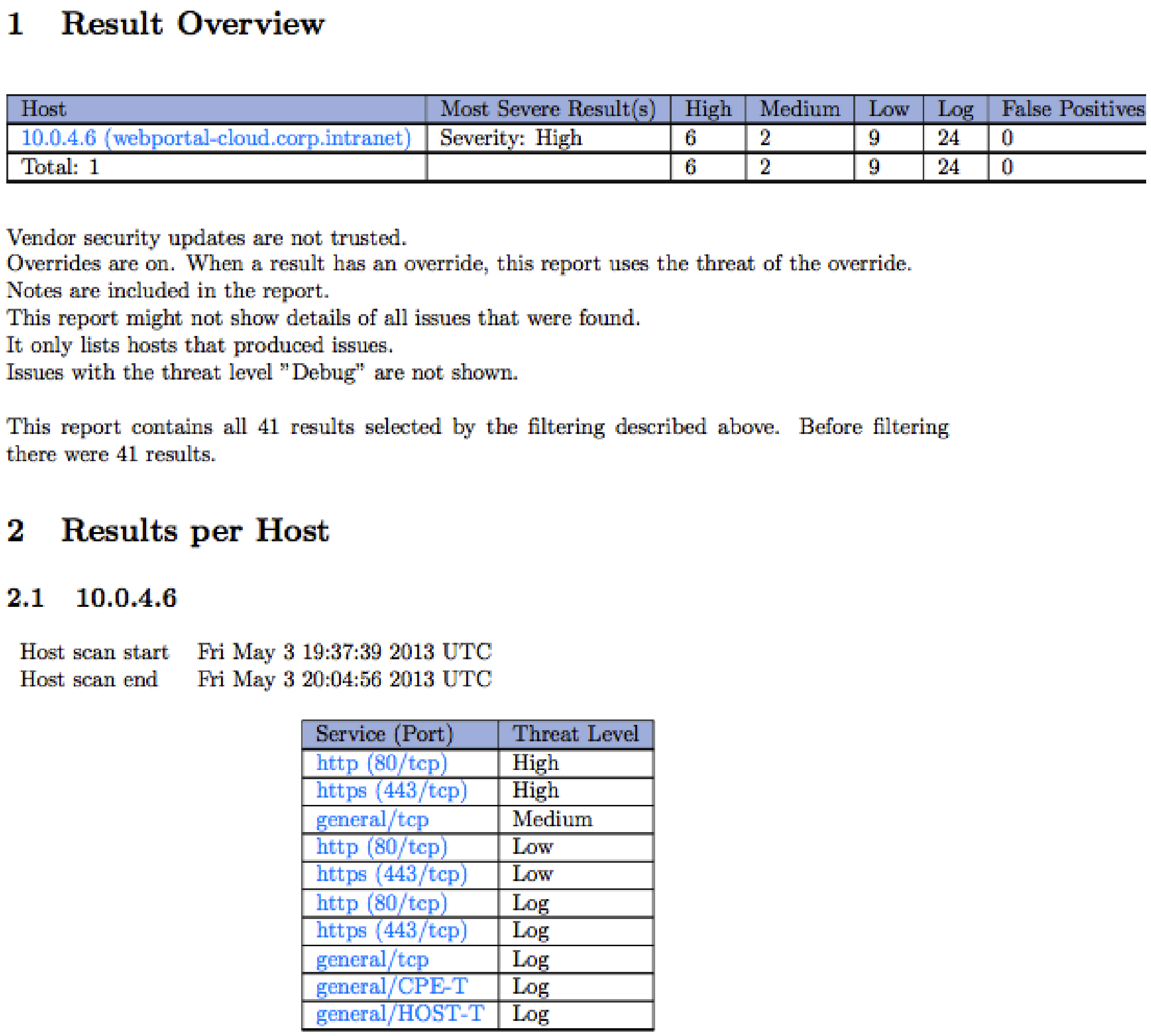
. . . (continues) . . .



. . . (continued) . . .

Service (Port)	Threat Level
general/tcp	Low
unknown (5911/tcp)	Low
unknown (5912/tcp)	Low
unknown (5913/tcp)	Low
unknown (9191/tcp)	Low
dec-notes (3333/tcp)	Low
commplex-main (5000/tcp)	Log
domain (53/tcp)	Log
http (80/tcp)	Log
https (443/tcp)	Log
nfs (2049/udp)	Log
unknown (35357/tcp)	Log
armtechdaemon (9292/tcp)	Log
general/tcp	Log
ssh (22/tcp)	Log
unknown (5911/tcp)	Log
unknown (5912/tcp)	Log
unknown (5913/tcp)	Log
unknown (9191/tcp)	Log
vnc (5900/tcp)	Log
dec-notes (3333/tcp)	Log
bootps (67/udp)	Log
domain (53/udp)	Log
epmd (4369/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log
general/udp	Log
ipp (631/udp)	Log
iscsi-target (3260/tcp)	Log
mdns (5353/udp)	Log
mdqs (666/udp)	Log
mysql (3306/tcp)	Log
nfs (2049/tcp)	Log
sunrpc (111/tcp)	Log
sunrpc (111/udp)	Log
unknown (11211/tcp)	Log
unknown (11211/udp)	Log
unknown (5672/tcp)	Log
unknown (875/tcp)	Log

E2 - 10.0.4.6 - Corp WebPortal in the Cloud, tested from malicious tenant



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
10.0.4.6 (webportal-cloud.corp.intranet)	Severity: High	6	2	9	24	0
Total: 1		6	2	9	24	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 41 results selected by the filtering described above. Before filtering there were 41 results.

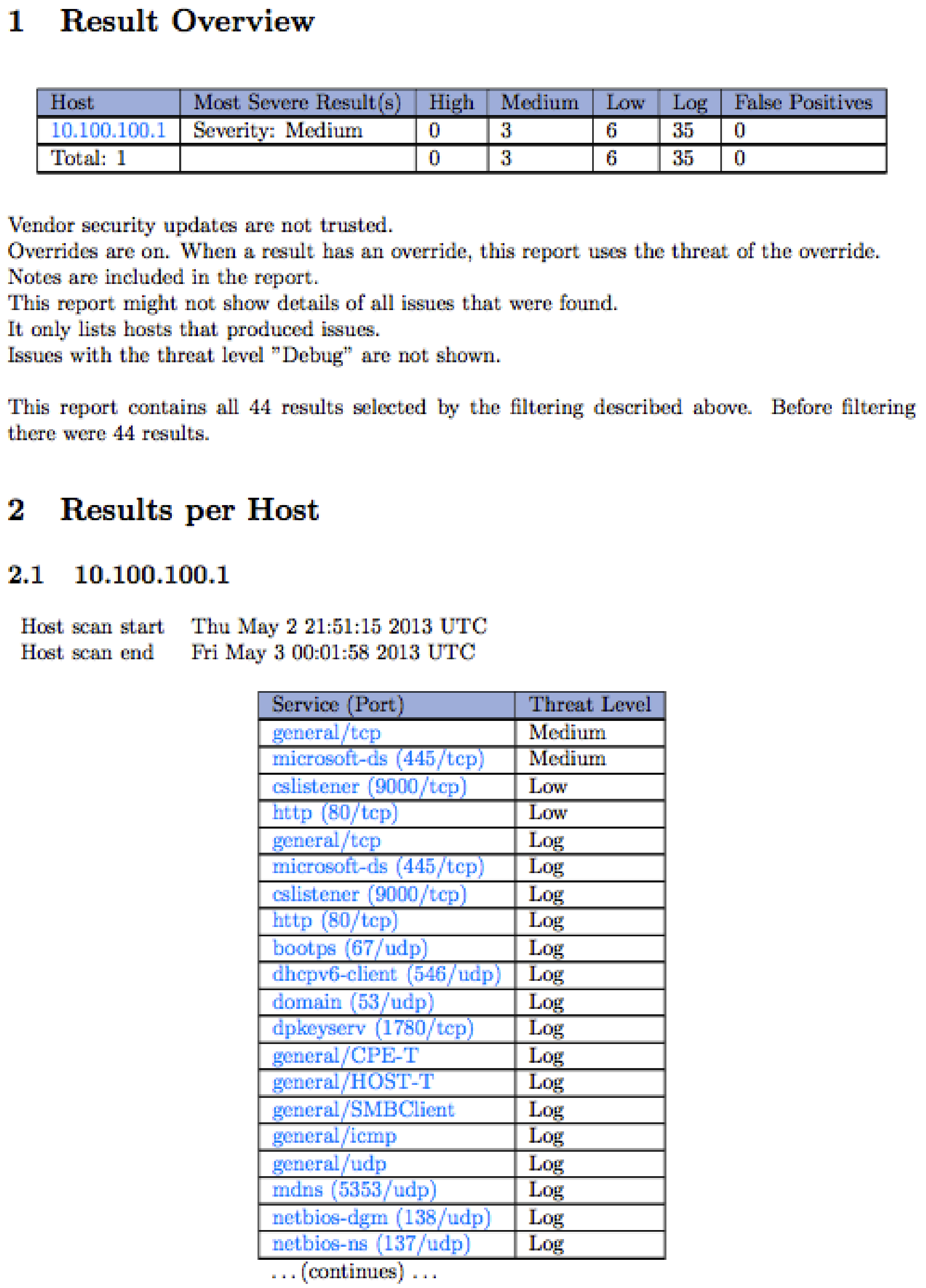
2 Results per Host

2.1 10.0.4.6

Host scan start Fri May 3 19:37:39 2013 UTC
Host scan end Fri May 3 20:04:56 2013 UTC

Service (Port)	Threat Level
http (80/tcp)	High
https (443/tcp)	High
general/tcp	Medium
http (80/tcp)	Low
https (443/tcp)	Low
http (80/tcp)	Log
https (443/tcp)	Log
general/tcp	Log
general/CPE-T	Log
general/HOST-T	Log

E3 - 10.100.100.1 – Corp internal DMZ router, tested from the Intranet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
10.100.100.1	Severity: Medium	0	3	6	35	0
Total: 1		0	3	6	35	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 44 results selected by the filtering described above. Before filtering there were 44 results.

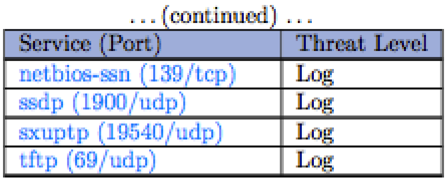
2 Results per Host

2.1 10.100.100.1

Host scan start	Thu May 2 21:51:15 2013 UTC
Host scan end	Fri May 3 00:01:58 2013 UTC

Service (Port)	Threat Level
general/tcp	Medium
microsoft-ds (445/tcp)	Medium
cslistener (9000/tcp)	Low
http (80/tcp)	Low
general/tcp	Log
microsoft-ds (445/tcp)	Log
cslistener (9000/tcp)	Log
http (80/tcp)	Log
bootps (67/udp)	Log
dhcpv6-client (546/udp)	Log
domain (53/udp)	Log
dpkeyserv (1780/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/SMBClient	Log
general/icmp	Log
general/udp	Log
mdns (5353/udp)	Log
netbios-dgm (138/udp)	Log
netbios-ns (137/udp)	Log

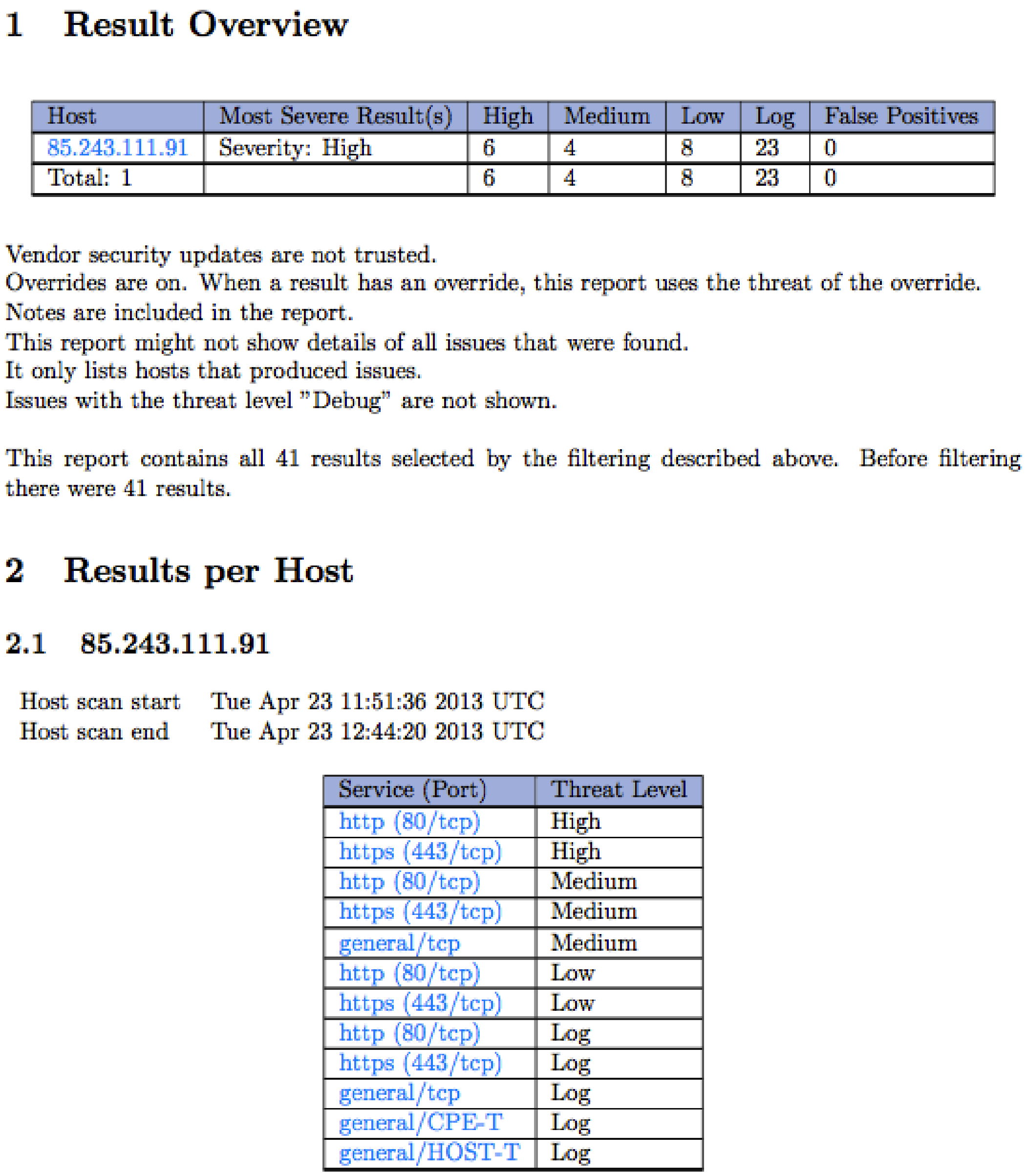
. . . (continues) . . .



. . . (continued) . . .

Service (Port)	Threat Level
netbios-ssn (139/tcp)	Log
ssdp (1900/udp)	Log
sxuptp (19540/udp)	Log
tftp (69/udp)	Log

E4 - 85.243.111.91 - Corp WebPortal in the Intranet, tested from the Internet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
85.243.111.91	Severity: High	6	4	8	23	0
Total: 1		6	4	8	23	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 41 results selected by the filtering described above. Before filtering there were 41 results.

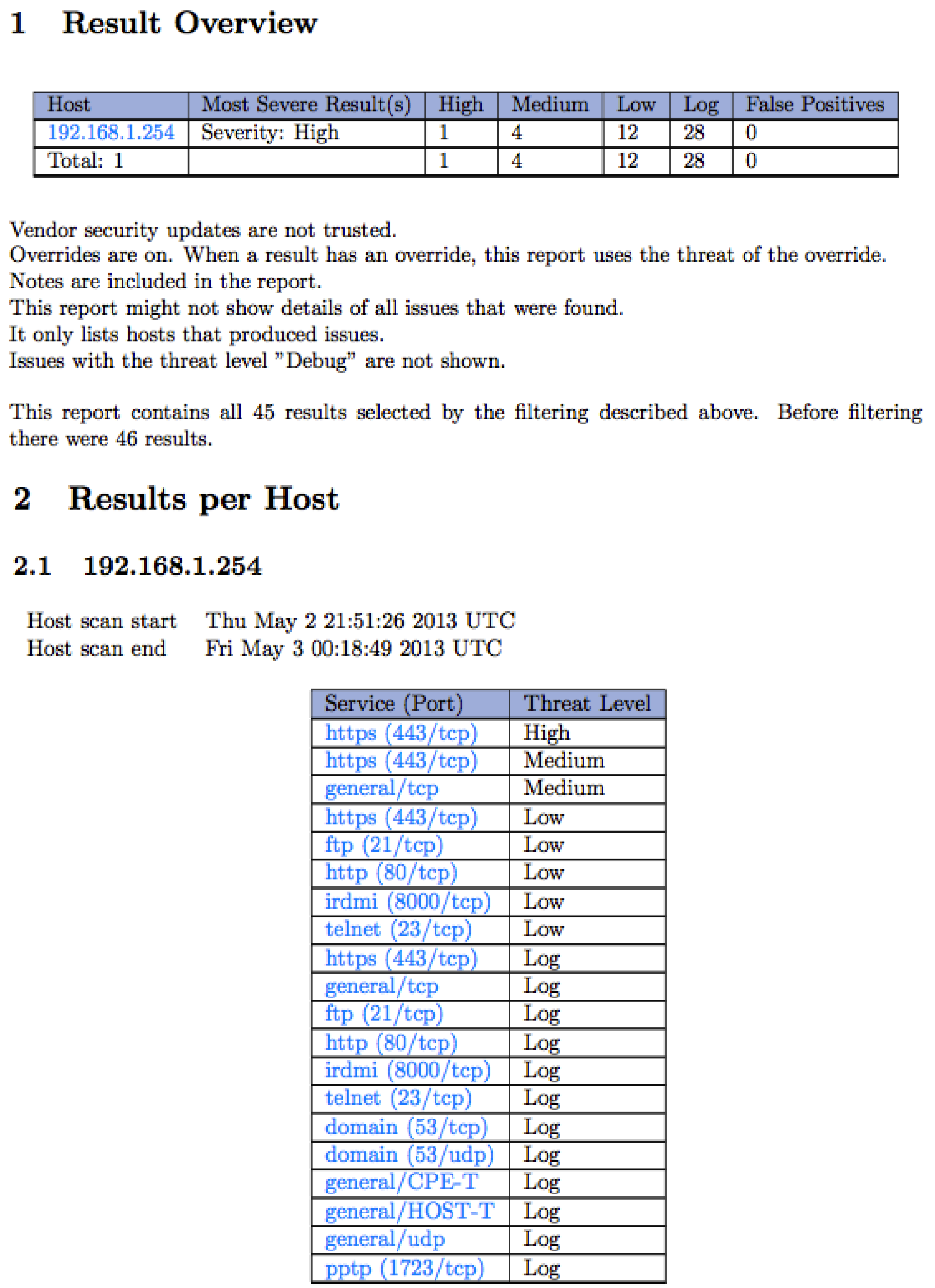
2 Results per Host

2.1 85.243.111.91

Host scan start	Tue Apr 23 11:51:36 2013 UTC
Host scan end	Tue Apr 23 12:44:20 2013 UTC

Service (Port)	Threat Level
http (80/tcp)	High
https (443/tcp)	High
http (80/tcp)	Medium
https (443/tcp)	Medium
general/tcp	Medium
http (80/tcp)	Low
https (443/tcp)	Low
http (80/tcp)	Log
https (443/tcp)	Log
general/tcp	Log
general/CPE-T	Log
general/HOST-T	Log

E5 - 192.168.1.254 – Corp External DMZ router, tested from the Intranet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.1.254	Severity: High	1	4	12	28	0
Total: 1		1	4	12	28	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 45 results selected by the filtering described above. Before filtering there were 46 results.

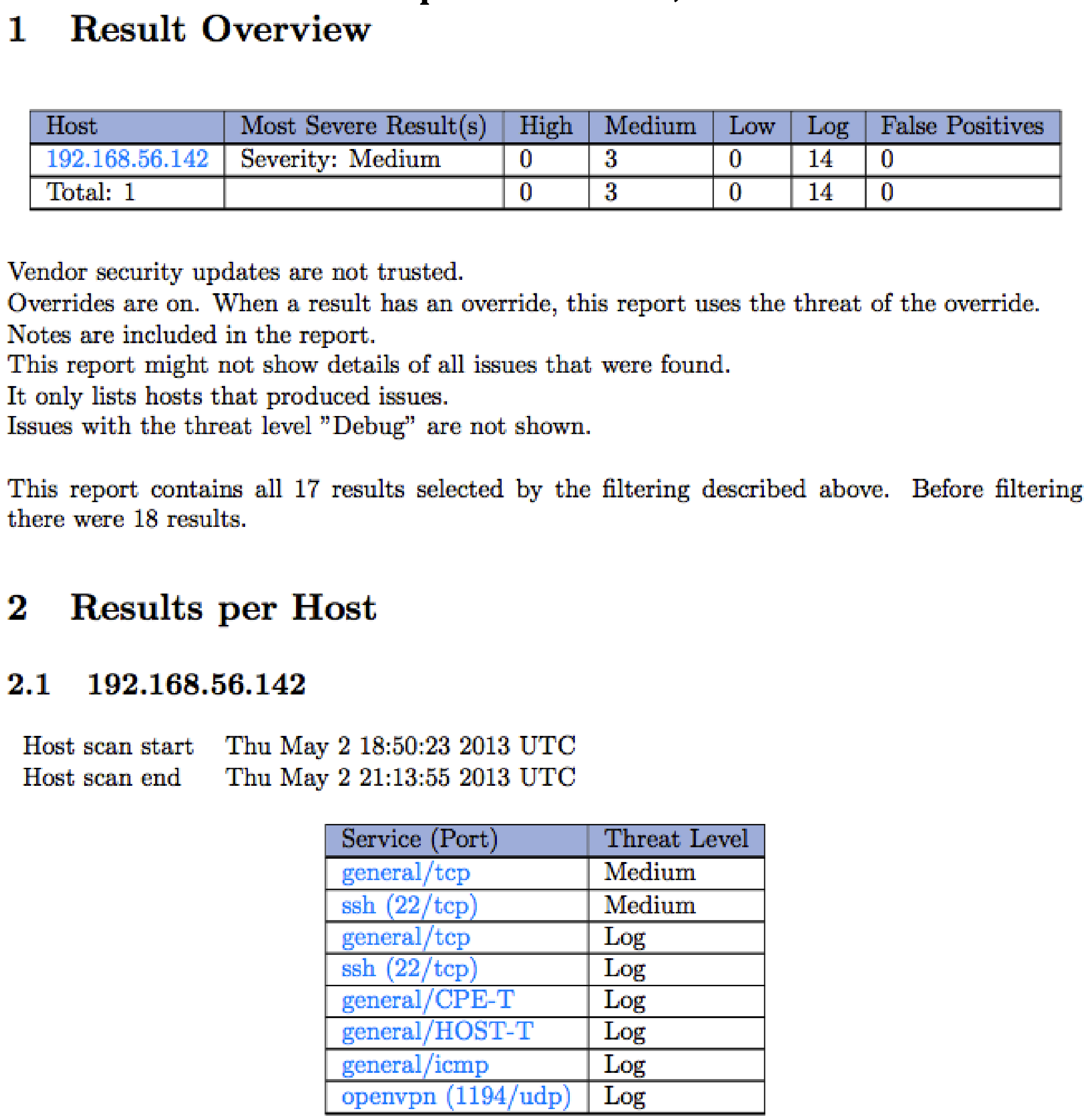
2 Results per Host

2.1 192.168.1.254

Host scan start	Thu May 2 21:51:26 2013 UTC
Host scan end	Fri May 3 00:18:49 2013 UTC

Service (Port)	Threat Level
https (443/tcp)	High
https (443/tcp)	Medium
general/tcp	Medium
https (443/tcp)	Low
ftp (21/tcp)	Low
http (80/tcp)	Low
irdmi (8000/tcp)	Low
telnet (23/tcp)	Low
https (443/tcp)	Log
general/tcp	Log
ftp (21/tcp)	Log
http (80/tcp)	Log
irdmi (8000/tcp)	Log
telnet (23/tcp)	Log
domain (53/tcp)	Log
domain (53/udp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/udp	Log
pptp (1723/tcp)	Log

E6 - 192.168.56.142 – Corp default router, tested from the Intranet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.56.142	Severity: Medium	0	3	0	14	0
Total: 1		0	3	0	14	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 17 results selected by the filtering described above. Before filtering there were 18 results.

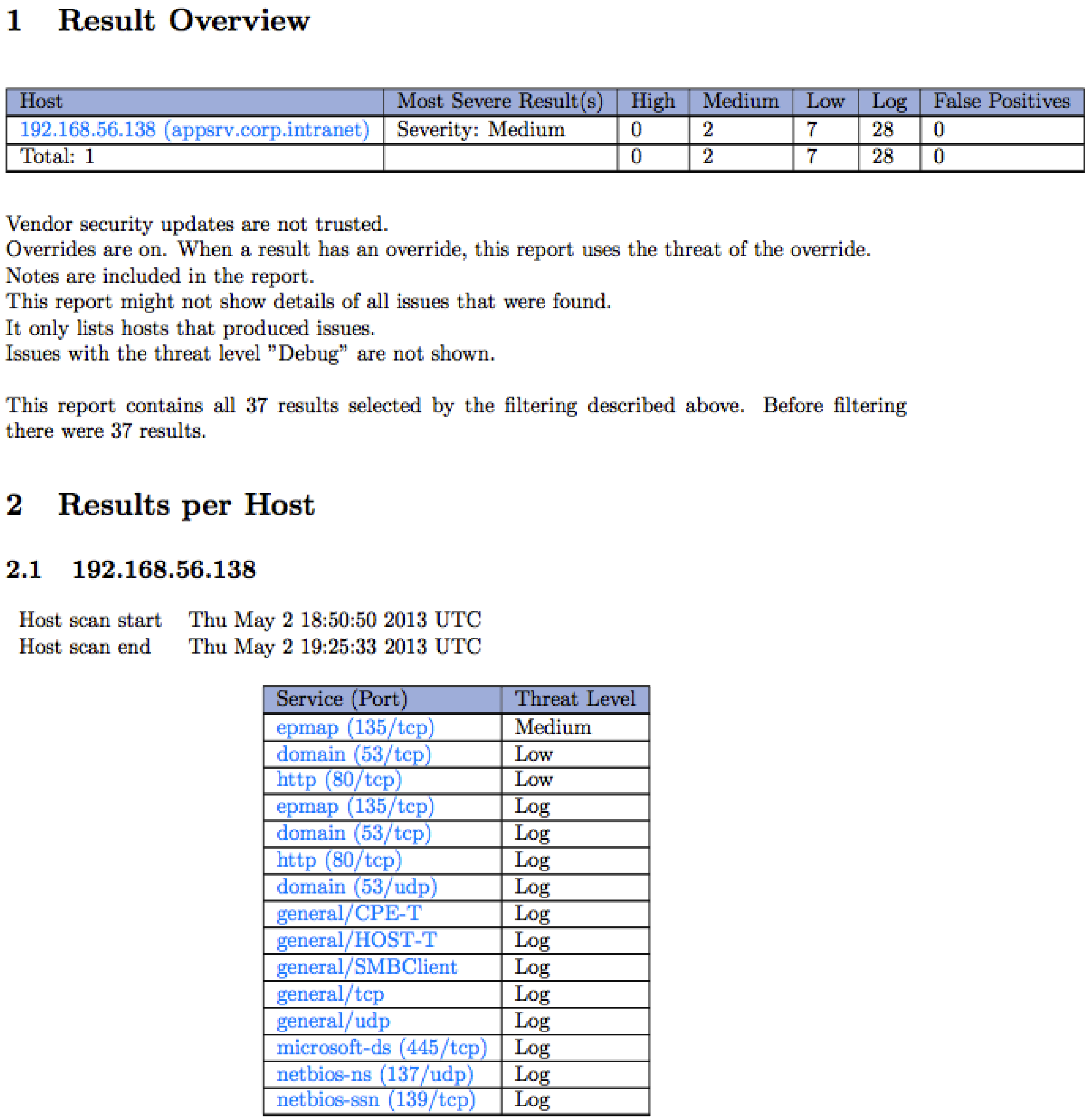
2 Results per Host

2.1 192.168.56.142

Host scan start	Thu May 2 18:50:23 2013 UTC
Host scan end	Thu May 2 21:13:55 2013 UTC

Service (Port)	Threat Level
general/tcp	Medium
ssh (22/tcp)	Medium
general/tcp	Log
ssh (22/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log
openvpn (1194/udp)	Log

E7 - Appsrv.corp.intranet - Application Server in the Intranet tested from the Intranet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.56.138 (appsrv.corp.intranet)	Severity: Medium	0	2	7	28	0
Total: 1		0	2	7	28	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 37 results selected by the filtering described above. Before filtering there were 37 results.

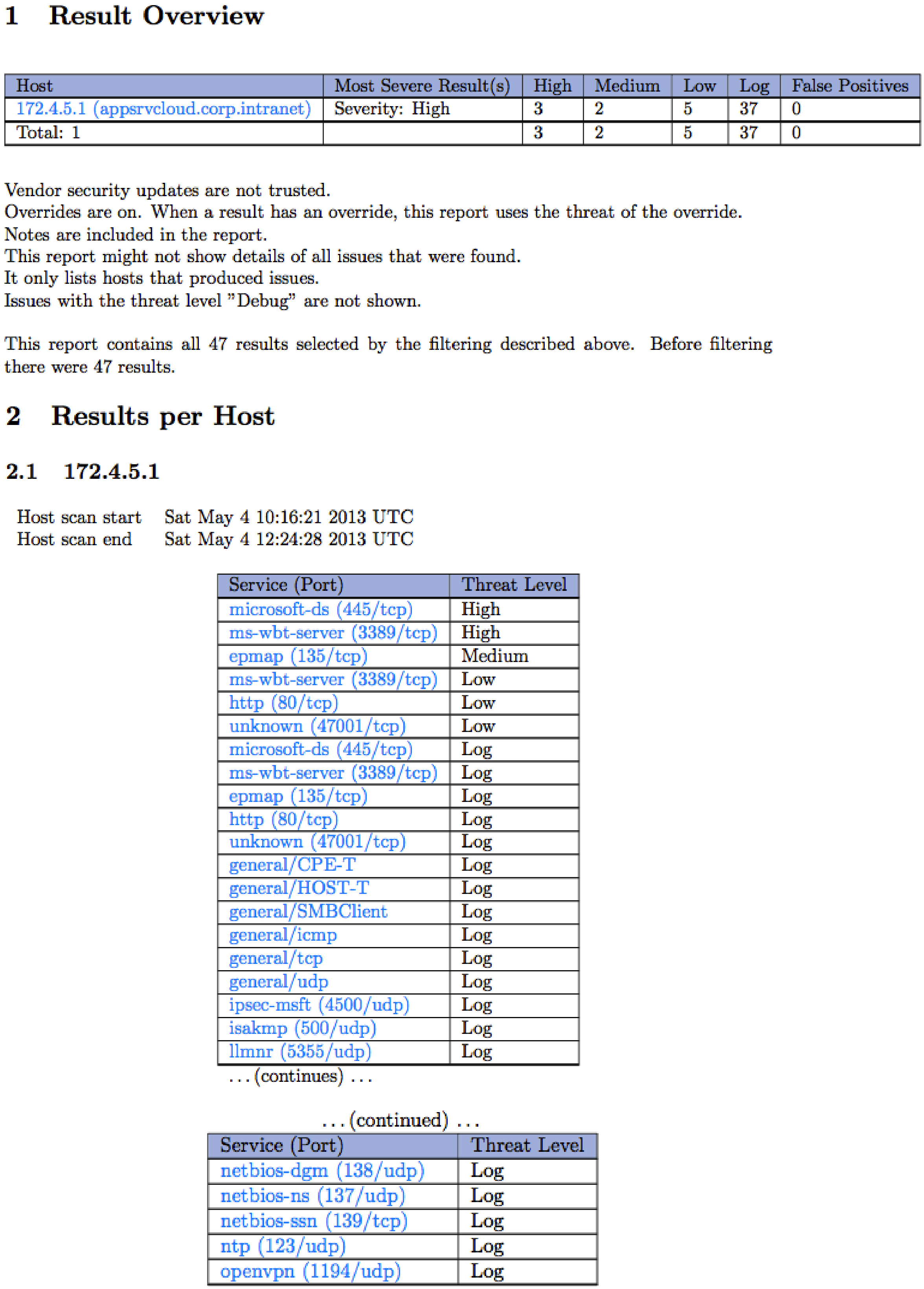
2 Results per Host

2.1 192.168.56.138

Host scan start	Thu May 2 18:50:50 2013 UTC
Host scan end	Thu May 2 19:25:33 2013 UTC

Service (Port)	Threat Level
epmap (135/tcp)	Medium
domain (53/tcp)	Low
http (80/tcp)	Low
epmap (135/tcp)	Log
domain (53/tcp)	Log
http (80/tcp)	Log
domain (53/udp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/SMBClient	Log
general/tcp	Log
general/udp	Log
microsoft-ds (445/tcp)	Log
netbios-ns (137/udp)	Log
netbios-ssn (139/tcp)	Log

E8 - Appsrvcloud.corp.intranet - Application Server in the Cloud, tested from the Intranet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
172.4.5.1 (appsrvcloud.corp.intranet)	Severity: High	3	2	5	37	0
Total: 1		3	2	5	37	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 47 results selected by the filtering described above. Before filtering there were 47 results.

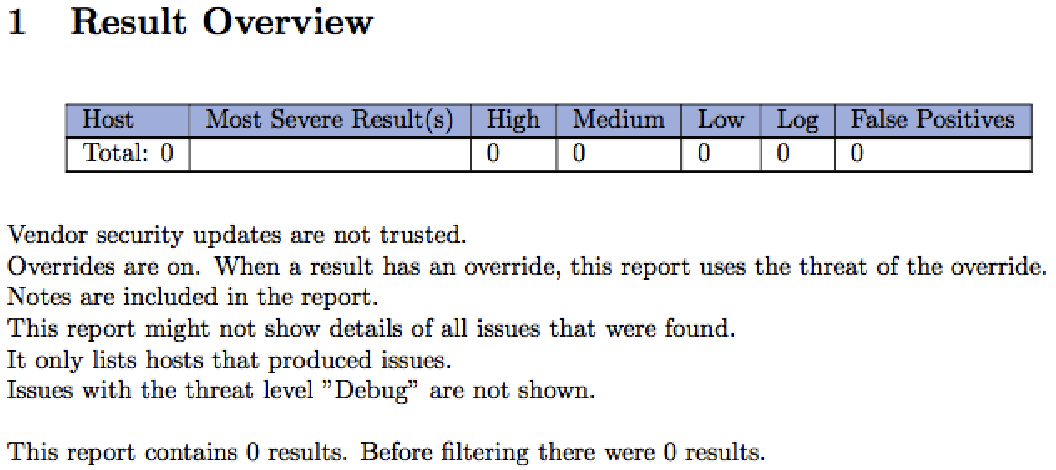
2 Results per Host

2.1 172.4.5.1

Host scan start Sat May 4 10:16:21 2013 UTC
Host scan end Sat May 4 12:24:28 2013 UTC

Service (Port)	Threat Level
microsoft-ds (445/tcp)	High
ms-wbt-server (3389/tcp)	High
epmap (135/tcp)	Medium
ms-wbt-server (3389/tcp)	Low
http (80/tcp)	Low
unknown (47001/tcp)	Low
microsoft-ds (445/tcp)	Log
ms-wbt-server (3389/tcp)	Log
epmap (135/tcp)	Log
http (80/tcp)	Log
unknown (47001/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/SMBClient	Log
general/icmp	Log
general/tcp	Log
general/udp	Log
ipsec-msft (4500/udp)	Log
isakmp (500/udp)	Log
llmnr (5355/udp)	Log
netbios-dgm (138/udp)	Log
netbios-ns (137/udp)	Log
netbios-ssn (139/tcp)	Log
ntp (123/udp)	Log
openvpn (1194/udp)	Log

E9 - Appsrvcloud.corp.intranet – Corp AppServer Server in the Cloud, tested from a Malicious Cloud tenant



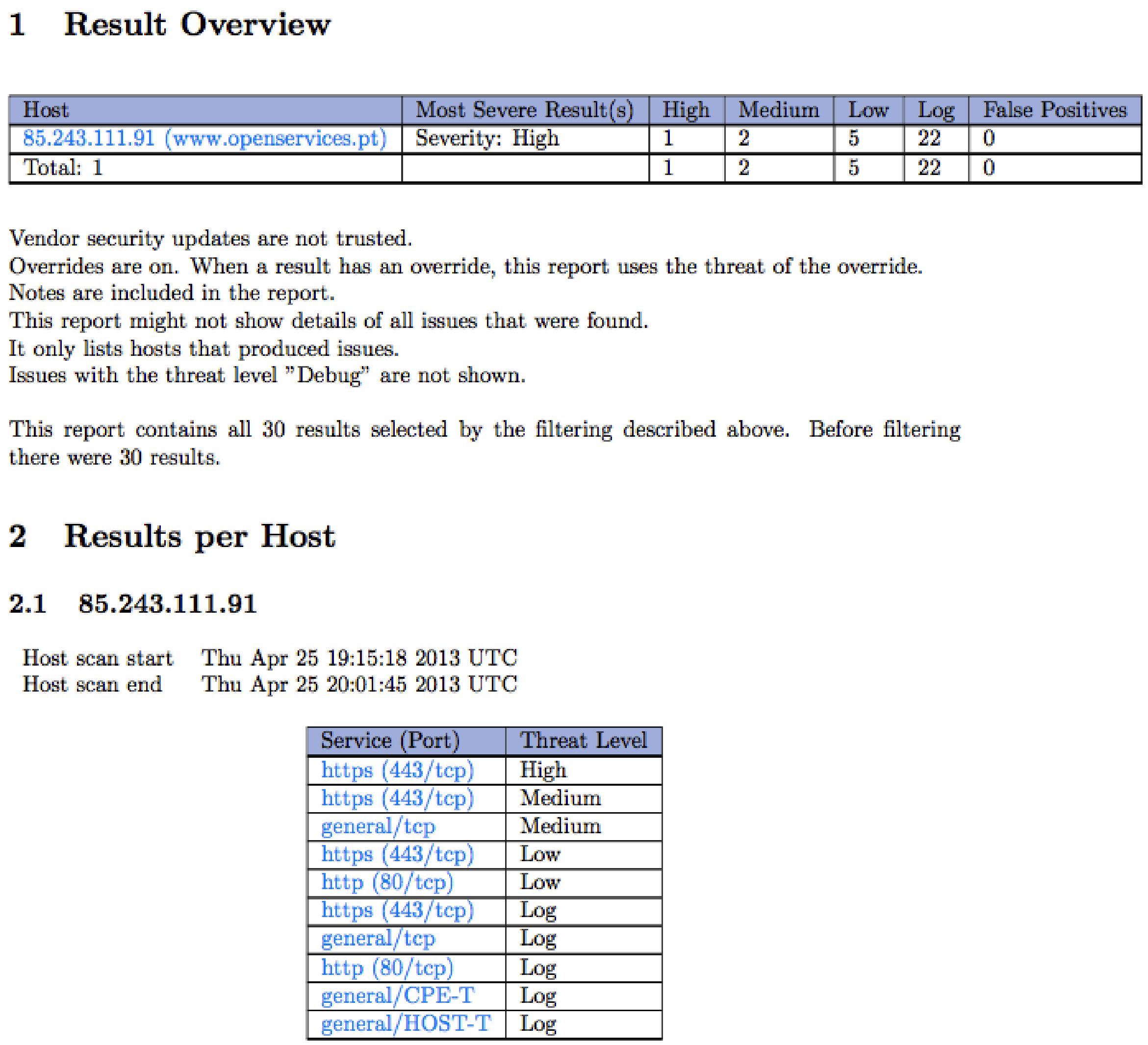
1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
Total: 0		0	0	0	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains 0 results. Before filtering there were 0 results.

E10 - Cloud0.dyndns-web.com/dashboard – Cloud Dashboard tested from the Internet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
85.243.111.91 (www.openservices.pt)	Severity: High	1	2	5	22	0
Total: 1		1	2	5	22	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 30 results selected by the filtering described above. Before filtering there were 30 results.

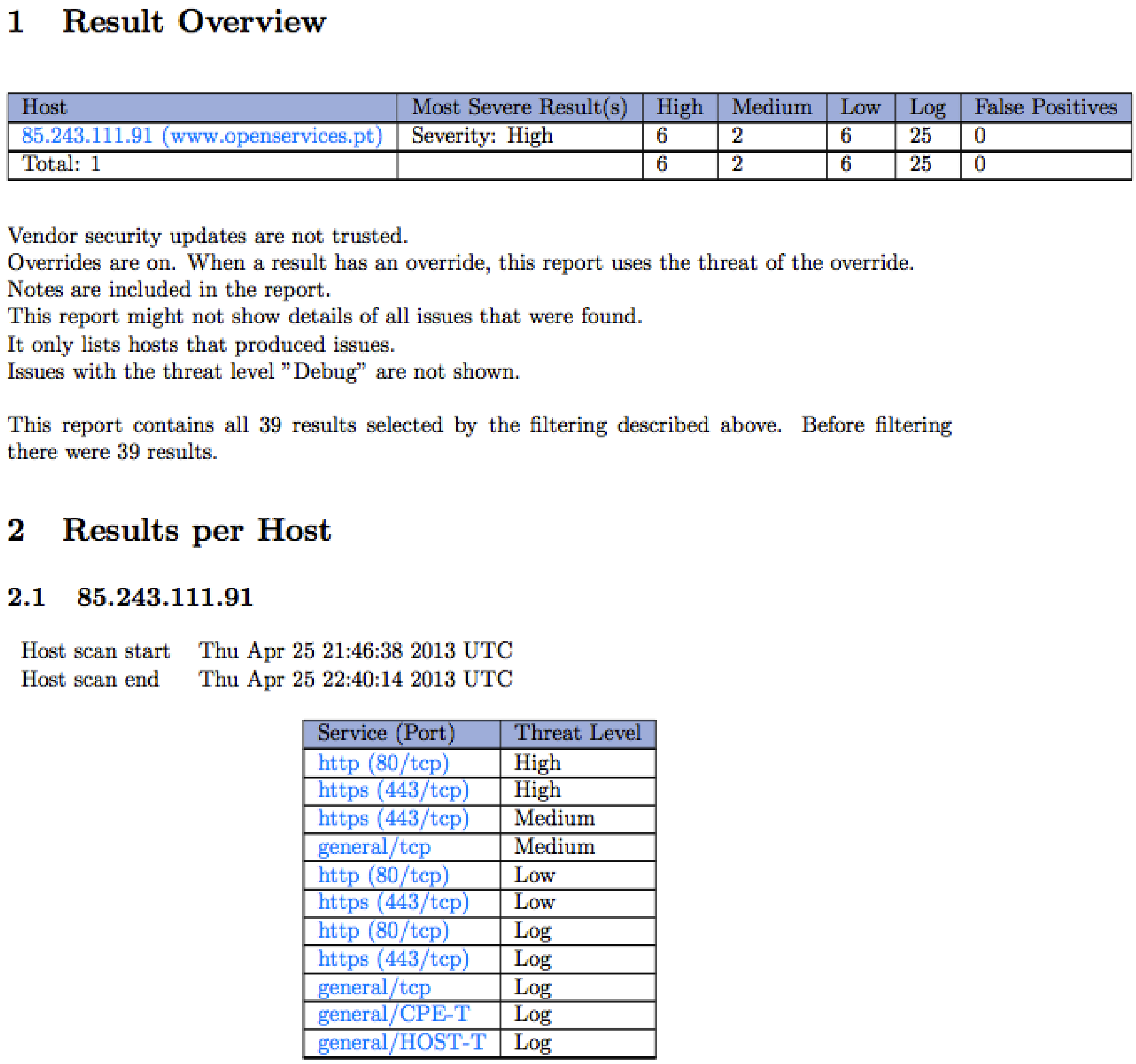
2 Results per Host

2.1 85.243.111.91

Host scan start	Thu Apr 25 19:15:18 2013 UTC
Host scan end	Thu Apr 25 20:01:45 2013 UTC

Service (Port)	Threat Level
https (443/tcp)	High
https (443/tcp)	Medium
general/tcp	Medium
https (443/tcp)	Low
http (80/tcp)	Low
https (443/tcp)	Log
general/tcp	Log
http (80/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log

E11 - Cloud0.dyndns-web.com/Corp - Corp Public WebPortal tested from the Internet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
85.243.111.91 (www.openservices.pt)	Severity: High	6	2	6	25	0
Total: 1		6	2	6	25	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 39 results selected by the filtering described above. Before filtering there were 39 results.

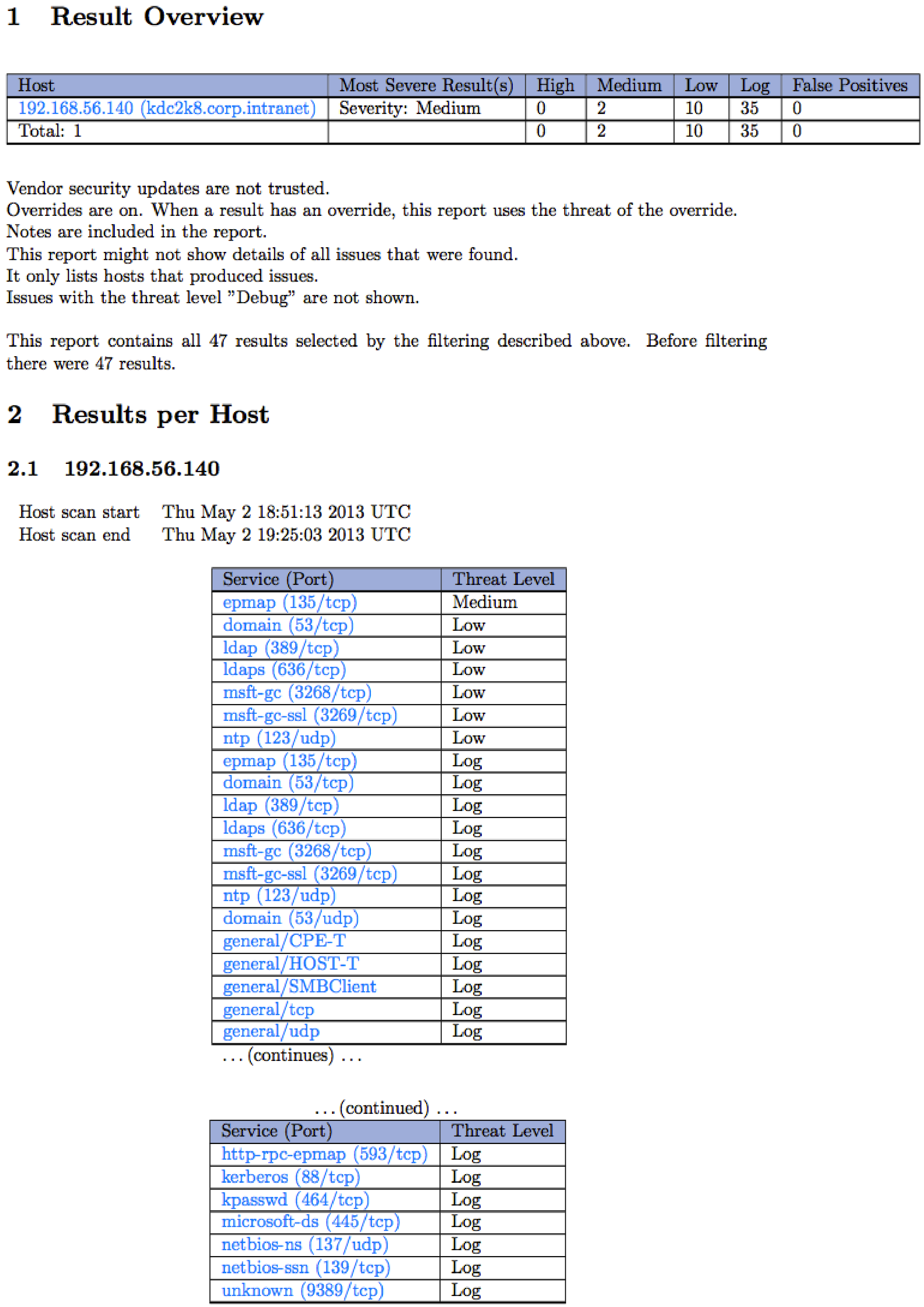
2 Results per Host

2.1 85.243.111.91

Host scan start	Thu Apr 25 21:46:38 2013 UTC
Host scan end	Thu Apr 25 22:40:14 2013 UTC

Service (Port)	Threat Level
http (80/tcp)	High
https (443/tcp)	High
https (443/tcp)	Medium
general/tcp	Medium
http (80/tcp)	Low
https (443/tcp)	Low
http (80/tcp)	Log
https (443/tcp)	Log
general/tcp	Log
general/CPE-T	Log
general/HOST-T	Log

E12 - Kdc2k8.corp.intranet – Corp Kerberos Distribution Center tested from the Intranet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.56.140 (kdc2k8.corp.intranet)	Severity: Medium	0	2	10	35	0
Total: 1		0	2	10	35	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 47 results selected by the filtering described above. Before filtering there were 47 results.

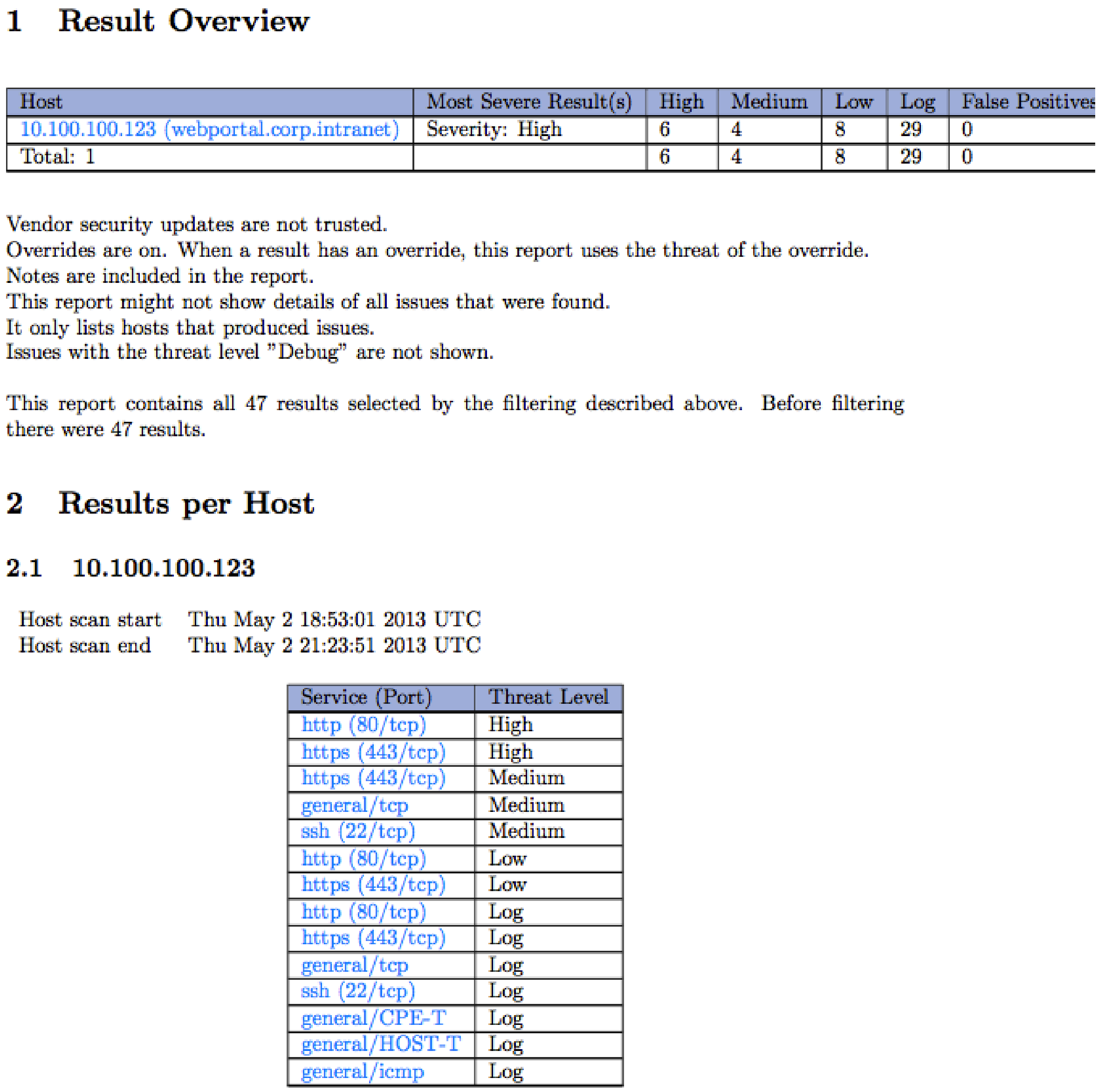
2 Results per Host

2.1 192.168.56.140

Host scan start	Thu May 2 18:51:13 2013 UTC
Host scan end	Thu May 2 19:25:03 2013 UTC

Service (Port)	Threat Level
epmap (135/tcp)	Medium
domain (53/tcp)	Low
ldap (389/tcp)	Low
ldaps (636/tcp)	Low
msft-gc (3268/tcp)	Low
msft-gc-ssl (3269/tcp)	Low
ntp (123/udp)	Low
epmap (135/tcp)	Log
domain (53/tcp)	Log
ldap (389/tcp)	Log
ldaps (636/tcp)	Log
msft-gc (3268/tcp)	Log
msft-gc-ssl (3269/tcp)	Log
ntp (123/udp)	Log
domain (53/udp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/SMBClient	Log
general/tcp	Log
general/udp	Log
http-rpc-epmap (593/tcp)	Log
kerberos (88/tcp)	Log
kpasswd (464/tcp)	Log
microsoft-ds (445/tcp)	Log
netbios-ns (137/udp)	Log
netbios-ssn (139/tcp)	Log
unknown (9389/tcp)	Log

E13 - 10.100.100.123 – Corp Public WebPortal in the Corp Network tested from the Intranet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
10.100.100.123 (webportal.corp.intranet)	Severity: High	6	4	8	29	0
Total: 1		6	4	8	29	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 47 results selected by the filtering described above. Before filtering there were 47 results.

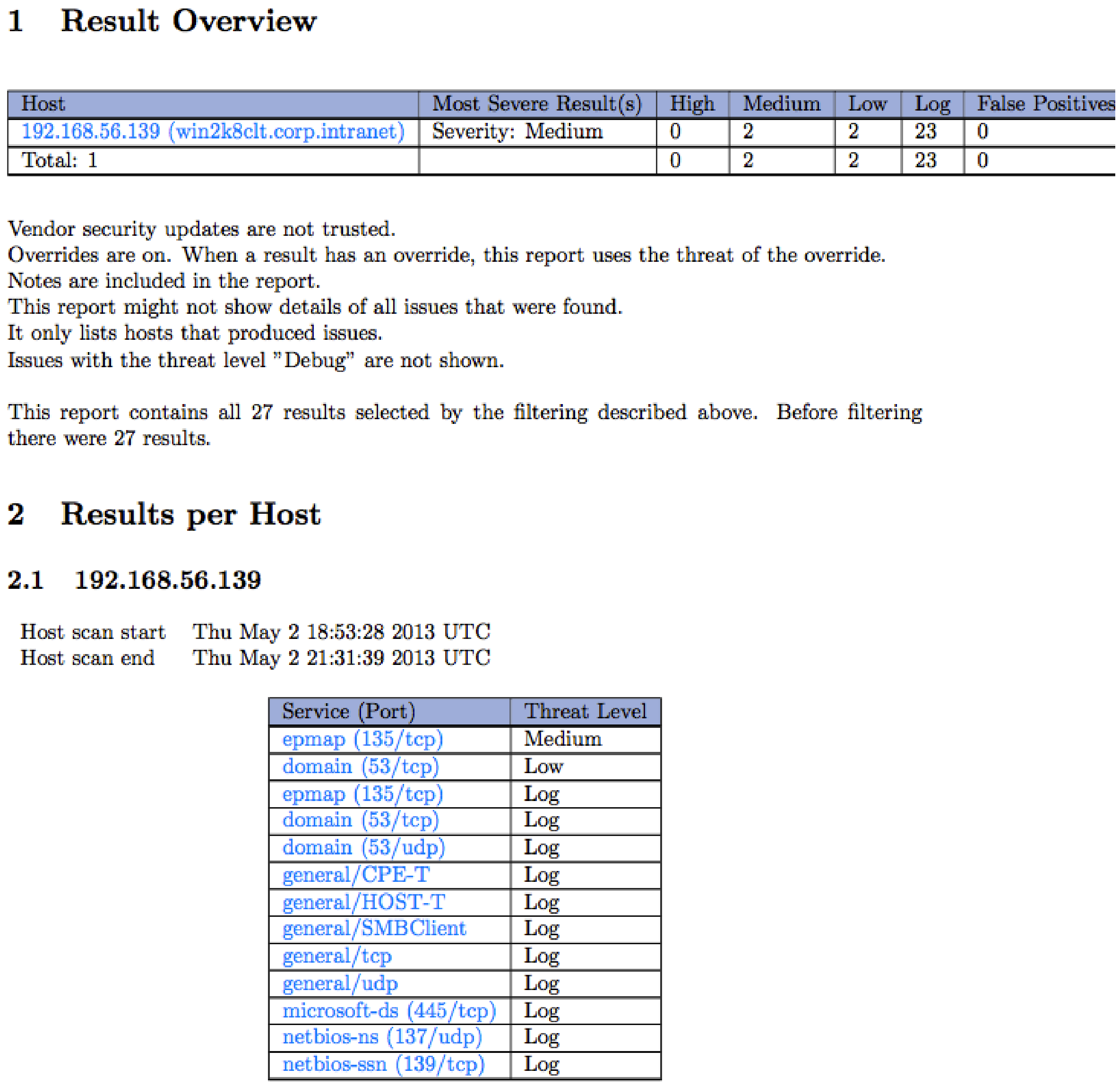
2 Results per Host

2.1 10.100.100.123

Host scan start	Thu May 2 18:53:01 2013 UTC
Host scan end	Thu May 2 21:23:51 2013 UTC

Service (Port)	Threat Level
http (80/tcp)	High
https (443/tcp)	High
https (443/tcp)	Medium
general/tcp	Medium
ssh (22/tcp)	Medium
http (80/tcp)	Low
https (443/tcp)	Low
http (80/tcp)	Log
https (443/tcp)	Log
general/tcp	Log
ssh (22/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log

E14 - Win2k8clt.corp.intranet – Corp User's workstation tested from the Intranet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.56.139 (win2k8clt.corp.intranet)	Severity: Medium	0	2	2	23	0
Total: 1		0	2	2	23	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 27 results selected by the filtering described above. Before filtering there were 27 results.

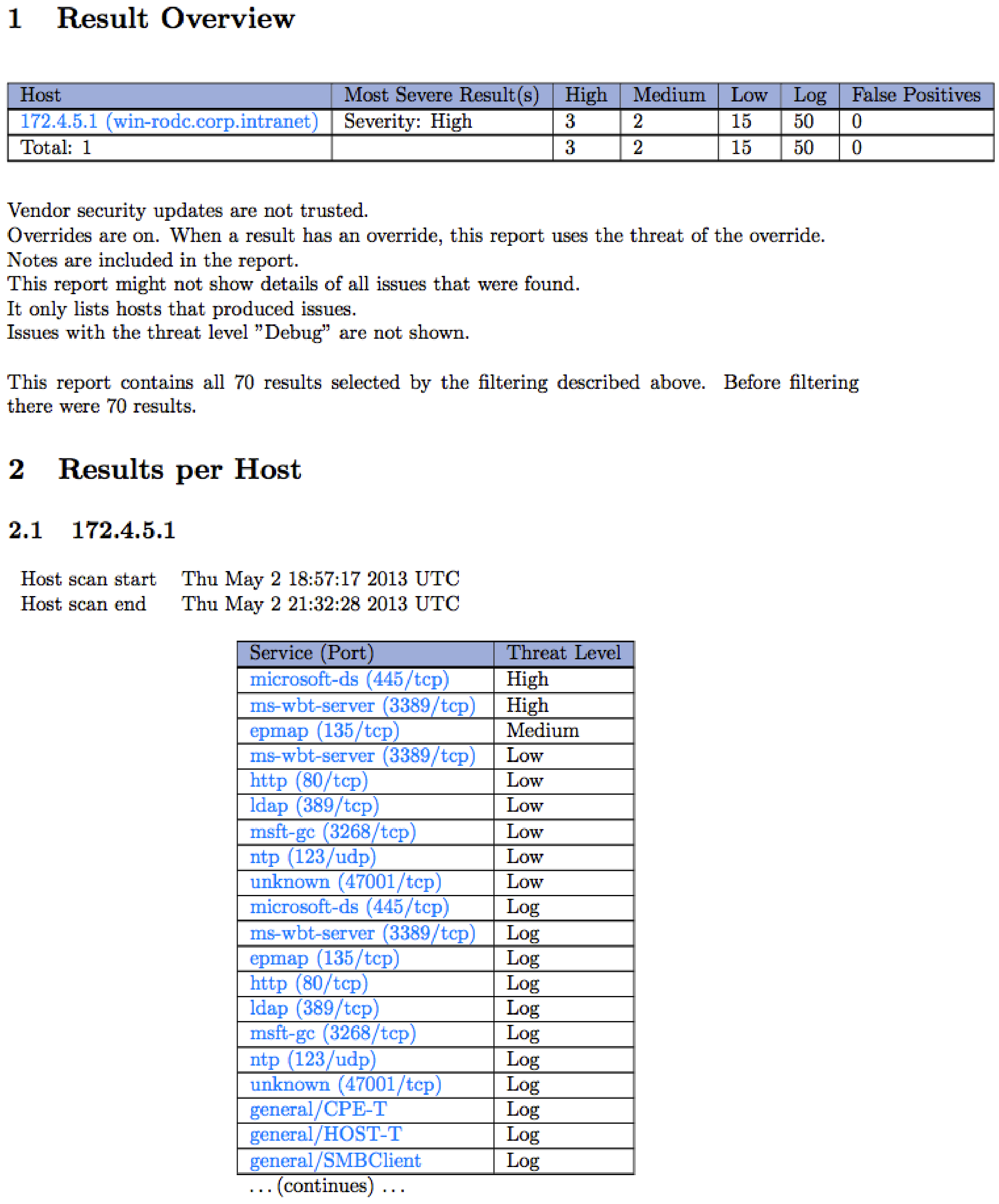
2 Results per Host

2.1 192.168.56.139

Host scan start	Thu May 2 18:53:28 2013 UTC
Host scan end	Thu May 2 21:31:39 2013 UTC

Service (Port)	Threat Level
epmap (135/tcp)	Medium
domain (53/tcp)	Low
epmap (135/tcp)	Log
domain (53/tcp)	Log
domain (53/udp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/SMBClient	Log
general/tcp	Log
general/udp	Log
microsoft-ds (445/tcp)	Log
netbios-ns (137/udp)	Log
netbios-ssn (139/tcp)	Log

E15 - win-rodc.corp.intranet – Read-Only Domain Controller in the Cloud tested from the Intranet



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
172.4.5.1 (win-rodc.corp.intranet)	Severity: High	3	2	15	50	0
Total: 1		3	2	15	50	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 70 results selected by the filtering described above. Before filtering there were 70 results.

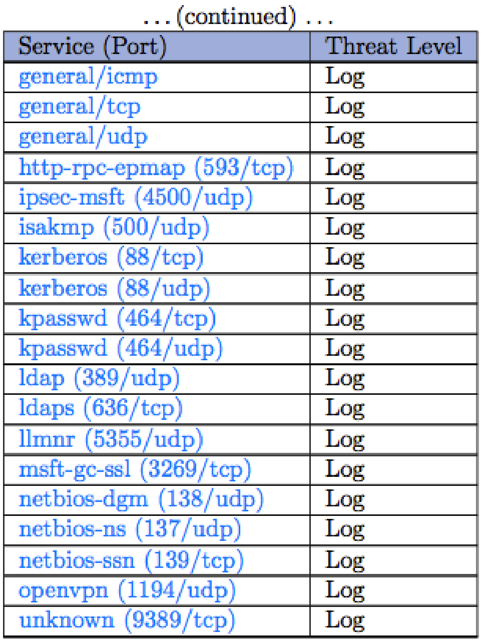
2 Results per Host

2.1 172.4.5.1

Host scan start Thu May 2 18:57:17 2013 UTC
Host scan end Thu May 2 21:32:28 2013 UTC

Service (Port)	Threat Level
microsoft-ds (445/tcp)	High
ms-wbt-server (3389/tcp)	High
epmap (135/tcp)	Medium
ms-wbt-server (3389/tcp)	Low
http (80/tcp)	Low
ldap (389/tcp)	Low
msft-gc (3268/tcp)	Low
ntp (123/udp)	Low
unknown (47001/tcp)	Low
microsoft-ds (445/tcp)	Log
ms-wbt-server (3389/tcp)	Log
epmap (135/tcp)	Log
http (80/tcp)	Log
ldap (389/tcp)	Log
msft-gc (3268/tcp)	Log
ntp (123/udp)	Log
unknown (47001/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/SMBClient	Log

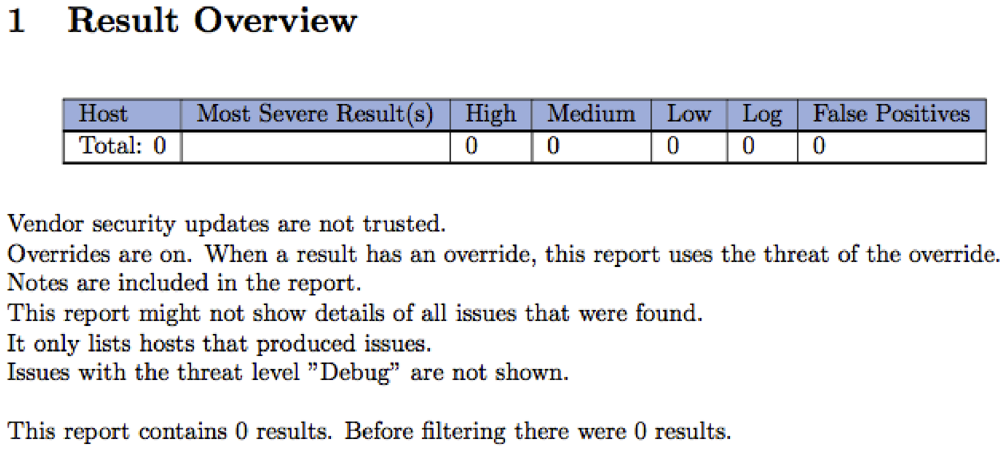
. . . (continues) . . .



. . . (continued) . . .

Service (Port)	Threat Level
general/icmp	Log
general/tcp	Log
general/udp	Log
http-rpc-epmap (593/tcp)	Log
ipsec-msft (4500/udp)	Log
isakmp (500/udp)	Log
kerberos (88/tcp)	Log
kerberos (88/udp)	Log
kpasswd (464/tcp)	Log
kpasswd (464/udp)	Log
ldap (389/udp)	Log
ldaps (636/tcp)	Log
llmnr (5355/udp)	Log
msft-gc-ssl (3269/tcp)	Log
netbios-dgm (138/udp)	Log
netbios-ns (137/udp)	Log
netbios-ssn (139/tcp)	Log
openvpn (1194/udp)	Log
unknown (9389/tcp)	Log

E16 - win-rodc.corp.intranet – Read-Only Domain Controller in the Cloud tested from a Malicious Cloud tenant



1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
Total: 0		0	0	0	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains 0 results. Before filtering there were 0 results.