2section*.1

Vulnerability Scanning with OpenVAS

Laboratory Report in EDA263/DAT641 Computer Security

Robert Grzelka - 911009C759

Group 68

Version no: 1

March 6, 2018

Contents

1 Introduction 1

2 Description of OpenVAS Setup 3

2.1 Port Scanning 5

2.2 Fingerprinting 6

2.2.1 Service Fingerprinting 6

2.2.2 Remote Host Fingerprinting 7

2.3 Vulnerability Scanning 7

3 Results 10

3.1 Port Scanning 10

3.1.1 Port 0 11

3.1.2 IMAP/IMAPS (143, 993) and POP3/POP3S (110, 995) 11

3.1.3 HTTP (80, 8080) 11

3.1.4 Microsoft-DS (445) and NetBIOS (139) 13

3.1.5 SSH on port 22 14

3.2 Fingerprinting Services 16

3.2.1 Host "Rome.Secnet" OS 17

3.2.2 Ports 80/8080, Apache Tomcat, Apache HTTP 18

3.2.3 Ports 445, Samba 19

3.2.4 Port 22, OpenSSH 20

3.2.5 Ports 143, 110, 993, 995, POP3, IMAP, POP3S, IMAPS 21

3.3 Vulnerability Scan 22

4 Discussion 25

5 Conclusion 27

6 Comments 28

6.1 Check if all the requirements from the template have been covered. 28

6.2 Is the report written in a clear voice? Is it easy to follow? 28

6.3 Introduction: 28

6.3.1 Is the purpose of the report clear? 28

6.3.2 Is it clear what is contained in this report? 28

6.4 Description of OpenVAS setup 28

6.4.1 Does the report explain the different components of the vulnerability assessment system used? 28

6.4.2 Does the report describe the scans that are performed (their configuration) and also a motivation for choosing them (what is their aim)? 28

6.4.3 Is it possible to repeat the scans (for result validation) based on the information presented here? . . . 28
6.5 Presentation of results . . . 28
6.5.1 Does the report contain results (most important ones) for each of the scans performed? . . . 28
6.5.2 Is there enough information describing the results in the report? . 29
6.6 Discussion of results . . . 29
6.6.1 Does the report contain a detailed discussion of most of the results obtained (at least for the most important ones)? . . . 29
6.6.2 Are the suggestions and decisions properly motivated? . . . 29
6.6.3 Are the initial recommendations updated (with the help of new results and findings)? . . . 29
6.7 Conclusions . . . 29
6.7.1 Are the main findings of the report highlighted? . . . 29
6.7.2 Do the authors present a strategy (a short list of actions) that can be followed to better secure the system? . . . 29
6.8 References . . . 29
6.8.1 Are the external sources used in the report properly referred to? . 29
6.9 General . . . 29
6.9.1 Are the figures and tables properly used and referred to? . . . 29
6.9.2 Grammar/structure of paper? . . . 29
6.9.3 Spelling errors (we hope all authors will use a spell checker before submitting the report, but please also comment if that is the case)? 30

References 31

A Report from OpenVAS Vulnerability Scanning 33

List of Tables

1 Information about open ports . . . 10
2 Service fingerprint . . . 16
3 Vulnerability scan fingerprint . . . 17
4 Summary of vulnerability scan recommendations . . . 26

List of Figures

1 The network setup . . . 3
2 Port Scanners NVT . . . 5
3 General NVT . . . 6
4 Vulnerability scan with OS NVT selected for host OS . . . 8

1 Introduction

Every kind of web bussiness need to be bulletproof from network attacks so that customers would receive services without any issues. Simply putting it, system need to have availability, integrity and confidentiality so it can work properly and give services. But here starts the hard part. Between TravelBiscuitAB and its customers lays open network with bad guys waiting in the dark. If system is not specially prepared then probably by default it will have vulnerabilities that will help intruders get inside system, do malicious stuff, and then scenario similar to described next will happen. We have normal day, everything seems fine, we go on lunch and when come back, our screens show the same picture of ransomware: pay or begone. Other scenarios are possible too, specially more silent ones, that no one could notice until too late: leak of sensitive data, falsifications, man in the middle attacks, etc...

If TravelBiscuitAB will notice issues of network security after something bad happens it is usually to late, will make you lose a lot of money, trust, face and customers. TravelBiscuitAB need to protect itself from potential attacks. Best way is security by prevention, that is why this default configurations or mistakes, sometimes even dummy and trivial (as they may seem) things have to be removed or fixed. Servers have to be set with security in mind.

Having broad experience and variety of tools we will first scan your system and then show how defenseless it is. It will make you scared. Then we will fix it. This is out job. Make your system waterproof from any leaks. We will not let other humans break into your system and eat your cake.

This report contains details of scan over the one of hosts of TravelBiscuitAB. Reasons to produce this report are:

1. analyze the current security level;
2. find vulnerabilities over network ports services;
3. recommend means of fixing this threats and give advice;
4. make host system more confident, integrated and raise its availability.

We will perform scan in depth over open ports, used services and security vulnerabilities of one of TravelBiscuitAB hosts. For this purpose introduced will be OpenVAS software. This software has very powerful scanning capabilities that will tell us state of system.

Still, OpenVAS its only a tool. Without understanding of its results and broad experience about existing services and typical vulnerabilities, this tool will be rendered as useless. Typical layman, after using OpenVAS would just tell you that that and this is vulnerable, so you have to update services and your system. Usually that is not enough. That kind of report is simply useless.

Together with our knowledge and experiences, we will base our guidelines on OpenVAS how to make TravelBiscuitAB secure. This will include guidelines for: opened ports, security of services on this ports, dealing with existing issues of this services, and system of host.

For us, after years of system securing tasks, simple look on results of OpenVAS scanner will let us know TravelBiscuitAB host system better than TravelBiscuitAB itself.

Opened ports will make your host naked in our eyes. Used services of TravelBiscuitAB host will let us know its system and find how to penetrate it. Fixing it require much more effort than simple scan, necessary are steps to rise security based on this scan. Such steps include maintenance of ports, services and system with proper configuration and selection of services. And that is sole purpose of this report.

Each opened port and service will be decomposed and described from security point of view. Additional means and alternatives will be described. In case of configuration with security issues, proper ones will be given. Host system will be evaluated as a whole and necessary steps for it will be issued. Set of proposed guidelines will be prepared especially for this system, to keep its effectiveness and performance with rise of security performance. In effect, anyone who would try to attack your system, will discover that its impossible, with effort not worth gains. Attackers will turn around and look for weaker preys.

Report content is structured in following way:

1. Introduction where we include a description of rest of the paper, briefly mention used tool OpenVAS, areas of host scans, purpose of report and effects.

2. Vulnerability scanning setup for utility OpenVAS with description of its functionality and pointed out steps taken to perform used scans. Different areas of scan depths will be described: open ports, services fingerprints, and host vulnerabilities. This will show overview of setup of which results will be included in next section and further explained there.

3. Results of scans with settings from previous section. After looking at settings of OpenVAS, one may move to corresponding subsection in this part. Findings will be displayed and described.

4. Discussion of displayed findings is meant to lay summary of found issues in vulnerabilities of system and services, comments on used services and ports.

5. Conclusions of host security and steps required for its upgrade by changes to be done with ports, services and system of host.

2 Description of OpenVAS Setup

This security task was made with help of Open Vulnerability Assessment System (OpenVAS or OVAS). With goal to perform Network Vulnerability Tests (NVTs) using multiple services and tools of OVAS. This system is being keep as one interface and allows user to perform deep vulnerability scan [1].

OpenVAS is a pack composed of different services and tools that are a good solution for vulnerability scanning and management. OpenVAS is supported by daily updated NVTs (Network Vulnerability Tests) numbering as of now over 50000. OpenVAS is free and under GNU General Public License (GNU GPL). User may use it by 3 different interfaces with same backend services: web-browser, a desktop-application or a CLI [1].

Any found vulnerabilities by OpenVAS come together with specific descriptions and references pointing to more details. Scans are repeatable, tasked and cached so further scans of one host depends on previous scans of this host. OpenVAS offers threat alerts function, if one was found during scan, user will be notified.
Network scans that were performed have a logical layout shown in Figure 1. Among 3 hosts in network, our selected test target was "rome.secnet". OpenVAS scanners are executed from server "theoden.ce.chalmers.se" between our client machine and target "rome.secnet".

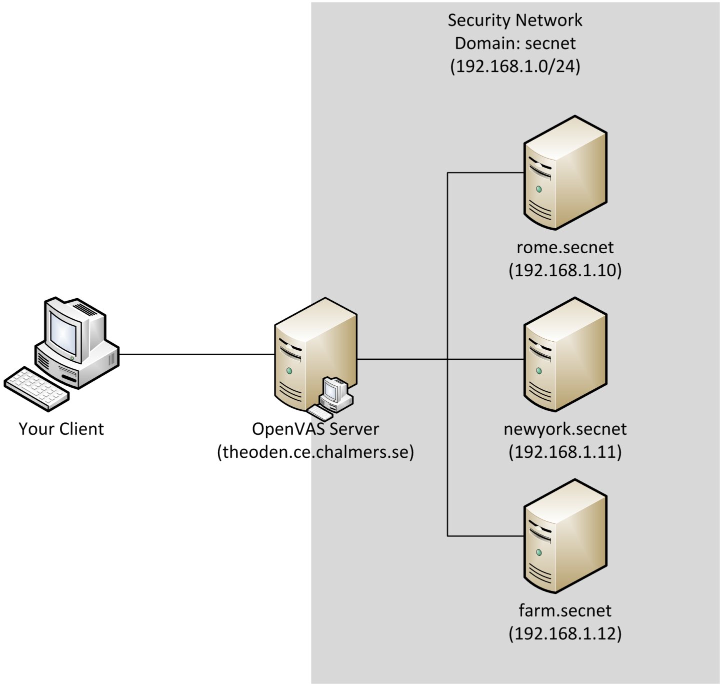


Figure 1: The network setup

We connect to the OpenVAS-client (on theoden.ce.chalmers.se), by the web-browser where Greenbone Security Assistant will forward requests from the OVAS-client and redirect them to the right endpoint in the /24 subnet security network within the domain secnet of TravelBiscuitAB. This network has three sub-domains: rome.secnet (192.168.1.10), newyork.secnet (192.168.1.11) and farm.secnet (192.168.1.12).

Host scanning is method showing how system are open to network. Its also method that may be used by an attacker to search for loophole in a system [2]. Several types of system scans exists, like: port scan, database scan, web app security scan, etc... [3].

This tasks included 3 related scans:

1. port scan: what ports are open with probable services
2. service fingerprint scan: list of services using opened ports
3. network vulnerability scan: list of issues of system and services at open ports

Mentioned 3 scans are performed in shown order, and settings of next one is based on previous one. This will result in attack tree of vulnerabilities that adverser may use to break into system. Besides full and deep scan was performed to find out hidden issues that are out of scope of host system specific scans and may be found by attacker if neglected by administrator.

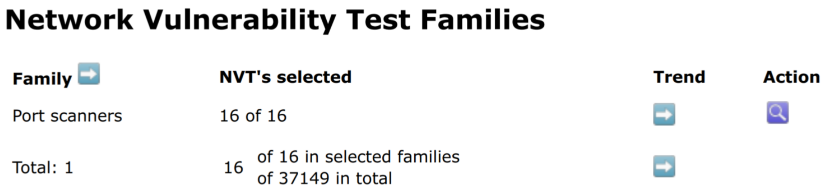
OpenVAS scanner require to be installed on server and then it may be used. NVT to be performed are selected in web-browser interface of OpenVAS. Also selected are port range of scan plus host target.

During selection of ports range, used was optimized OpenVAS default port range that allows to perform scan with reasonable time by only scanning amount of typically used ports.

In following subsections 2.1, 2.2 and 2.3 we will describe methods used to determine the security of the remote host "rome.secnet" of TravelBiscuitAB domain.

2.1 Port Scanning

Port scanning will result with list of open ports of the host system. OpenVAS has a family of Port Scanners with 16 NVT's in Network Vulnerability Test Families that were used to perform the port scanning, as in Figure 2.



Network Vulnerability Test Families

Family ➡	NVT's selected	Trend	Action
Port scanners	16 of 16	➡	🔍
Total: 1	16 of 16 in selected families of 37149 in total	➡	

Figure 2: Port Scanners NVT

During scan we may consider 3 kinds of ports. Ports from range 0-1023 are called well-known ports or system ports. They are used by system processes that provide widely used types of network services. On Unix-like operating systems, a process must execute with superuser privileges to be able to bind a network socket to an IP address using one of the well-known ports.

Next ports, those in range 1024-49151 are called registered or user ports. They are assigned by IANA for specific service upon application by a requesting entity. On most systems, registered ports can be used without superuser privileges.

Last ports in range 49152–65535 are called dynamic, private or ephemeral ports. The range 49152–65535 (215 + 214 to 216 1) contains dynamic or private ports that cannot be registered with IANA. This range is used for private or customized services, for temporary purposes, and for automatic allocation of ephemeral ports [4].

The most standard services are associated with the well-known ports. Most of the ports are closed, and only few standard ones are in use, depending of host purpose. Automatic port scan supplied by OpenVAS let us avoid scanning by hand of 65535 possibly open ports. Way of scanning ports is as follows: scanner sends a request to every port and notes down responses of opened ports. Result is list of opened ports that already gives some information about host and is cached for later for further scans. To scan TravelBiscuitAB host "rome.secnet" we used the OpenVAS default port list where it scan over 4481 of standard ports [1].

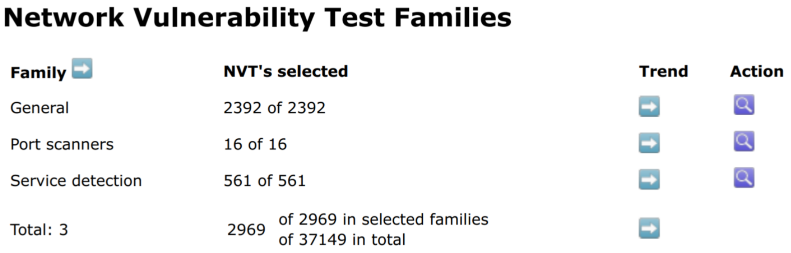
Port scans require least amount of time spent with result of clearly shown open ports. This scan allows to understand typical structure of host and its probable weaknesses. After that step, it is known which service ports on the target host are listening for incoming connections. For experienced attacker existence of some ports is usually enough to describe security level of host and what kind of ports will let him to penetrate server.

2.2 Fingerprinting

Fingerprinting in here is a further step of host security tests. After we got to know which of host ports are open we are checking response of this ports. Then our job its to find out what kind of services, software and applications could be listening behind these ports. This is called Service Fingerprinting.

2.2.1 Service Fingerprinting

Second scan searches through open ports and then generate a fingerprints describing services that are using previously found specific ports. Settings used in this scan are displayed in Figure 3.



Network Vulnerability Test Families

Family ➡	NVT's selected	Trend	Action
General	2392 of 2392	➡	🔍
Port scanners	16 of 16	➡	🔍
Service detection	561 of 561	➡	🔍
Total: 3	2969 of 2969 in selected families of 37149 in total	➡	

Figure 3: General NVT

Based on the port number and by referencing to "Service Name and Transport Protocol Port Number Registry" we may deduce service using given open port. Ie. if port 22 is open, we will find a application based on the SSH like OpenSSH [5], if port 80 is open it will correspond to HTTP web server and port 443 to HTTPS web server. Usually each port will have standard type of service behind it.

Fingerprint of each service is containing some chunk of its basic information's, like: version of service, operating system, vulnerability issues. Threats of bugs, errors, issues, weak configurations and generally vulnerabilities corresponding to this services are classified from high to low and as logs.

Some amount of information lay in simple logs of each port scan. Itself they may be out of classification, but still contain some data that let us to exactly see or guess issues and what operating system is used by host.

Existence of some services may be unnecessary in host system. Part of services may have more secure alternatives. Other services may act as threat without showing any vulnerabilities by scan in current version, but are simply known as vulnerable and new issues are periodically found in range of its versions. Next services may be secure from implementation point of view, but are weakly configured.

This step is meant to identifying information about services that are hidden behind open ports of host "rome.secnet". NVT selected in this setup were from families of “General” and “Service detection”.

2.2.2 Remote Host Fingerprinting

Fingerprinting on host "Rome.Secnet" is to reveal and collect chunks of information about host services. This information’s include:

- service version and known vulnerabilities
- machine operating system type and version

Each of scan results will be enriched by further research of host services. Pointed out will be notes and guidelines that allows reader to gain more understanding about host system state and services critical components from security point of view.

2.3 Vulnerability Scanning

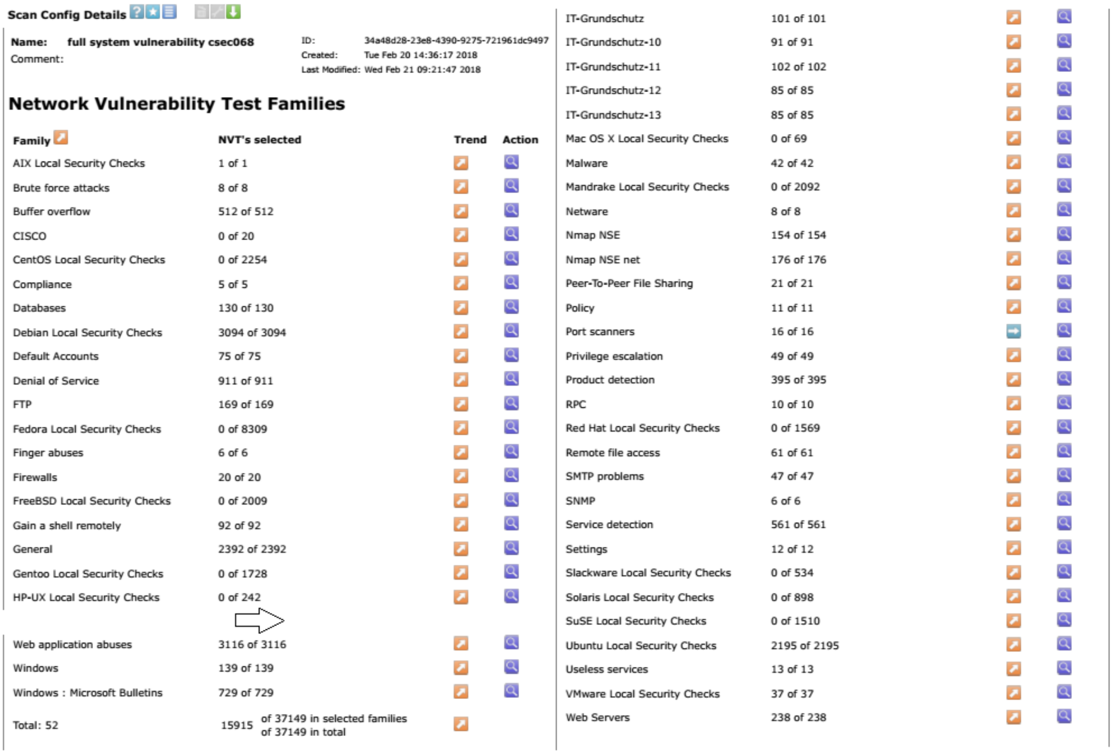
Third scan is to find vulnerabilities in host system and services. Usefully to it are results of previous both scans helping to generate attack trees. Even so, vulnerability scan is repeated 3 times, each time for different range of selected NVT’s (15915/37134/37134 of 37134) and with different trust to results of previous scans: (trust, trust, don’t trust).

Configuration of first vulnerabilities scan is displayed in Figure 4. This scan has manually selected range of NVT’s numbering 15915 of 37134 available, and is based on findings of host OS. Its meant to find vulnerabilities of used services and in terms of OS, to find vulnerabilities only specific to host OS with skipping scans of other OS.

Fist vulnerability scan is performed for previously found services vulnerabilities. It is set specially for discovered type of host OS. It is done with goal to look for wider range of issues than in previous port and fingerprint scans, but skip scans for threats of other types of systems than host found one. This scan have similar results to previous one of fingerprints scan, but for wider range of possible loopholes.

Each scan of some selected service will give result in form of: used port, used service on this port, version of service, level of security risk by using this version of this service, references about detailed issue of this service and logs.

During setup of vulnerability scan, we used more than half predefined NVTs, after excluding scans for non matching operating systems. Based on our observation of Second scan result, raised was conclusion that used OS is Ubuntu with services for Windows, so all other systems NVTs scans were disabled. Here OpenVAS would not made wild guess



Scan Config Details

Name: full system vulnerability csec068
Comment:

ID: 34a48d28-23e8-4390-9275-721961dc9497
Created: Tue Feb 20 14:36:17 2018
Last Modified: Wed Feb 21 09:21:47 2018

Network Vulnerability Test Families

Family ↗	NVT's selected	Trend	Action
AIX Local Security Checks	1 of 1	↗	🔍
Brute force attacks	8 of 8	↗	🔍
Buffer overflow	512 of 512	↗	🔍
CISCO	0 of 20	↗	🔍
CentOS Local Security Checks	0 of 2254	↗	🔍
Compliance	5 of 5	↗	🔍
Databases	130 of 130	↗	🔍
Debian Local Security Checks	3094 of 3094	↗	🔍
Default Accounts	75 of 75	↗	🔍
Denial of Service	911 of 911	↗	🔍
FTP	169 of 169	↗	🔍
Fedora Local Security Checks	0 of 8309	↗	🔍
Finger abuses	6 of 6	↗	🔍
Firewalls	20 of 20	↗	🔍
FreeBSD Local Security Checks	0 of 2009	↗	🔍
Gain a shell remotely	92 of 92	↗	🔍
General	2392 of 2392	↗	🔍
Gentoo Local Security Checks	0 of 1728	↗	🔍
HP-UX Local Security Checks	0 of 242	↗	🔍
IT-Grundschutz	101 of 101	↗	🔍
IT-Grundschutz-10	91 of 91	↗	🔍
IT-Grundschutz-11	102 of 102	↗	🔍
IT-Grundschutz-12	85 of 85	↗	🔍
IT-Grundschutz-13	85 of 85	↗	🔍
Mac OS X Local Security Checks	0 of 69	↗	🔍
Malware	42 of 42	↗	🔍
Mandrake Local Security Checks	0 of 2092	↗	🔍
Netware	8 of 8	↗	🔍
Nmap NSE	154 of 154	↗	🔍
Nmap NSE net	176 of 176	↗	🔍
Peer-To-Peer File Sharing	21 of 21	↗	🔍
Policy	11 of 11	↗	🔍
Port scanners	16 of 16	→	🔍
Privilege escalation	49 of 49	↗	🔍
Product detection	395 of 395	↗	🔍
RPC	10 of 10	↗	🔍
Red Hat Local Security Checks	0 of 1569	↗	🔍
Remote file access	61 of 61	↗	🔍
SMTP problems	47 of 47	↗	🔍
SNMP	6 of 6	↗	🔍
Service detection	561 of 561	↗	🔍
Settings	12 of 12	↗	🔍
Slackware Local Security Checks	0 of 534	↗	🔍
Solaris Local Security Checks	0 of 898	↗	🔍
SuSE Local Security Checks	0 of 1510	↗	🔍
Ubuntu Local Security Checks	2195 of 2195	↗	🔍
Useless services	13 of 13	↗	🔍
VMware Local Security Checks	37 of 37	↗	🔍
Web Servers	238 of 238	↗	🔍
Web application abuses	3116 of 3116	↗	🔍
Windows	139 of 139	↗	🔍
Windows : Microsoft Bulletins	729 of 729	↗	🔍
Total: 52	15915 of 37149 in selected families of 37149 in total	↗	

Figure 4: Vulnerability scan with OS NVT selected for host OS

about used OS, but stated that we have Ubuntu. If it would be not clear, it will stated that host system is simply of Unix family.

Scan of services vulnerability was made with setup similar to predefined scan “full and fast” but with "Local Security Checks" family type scans mostly disabled. Enabled ones were for Ubuntu, Windows and VMware, see Figure 4. Ubuntu were found as host OS. Selection of Windows OS scan comes from existence of NetBIOS and Samba services. VMware from possibility that some services are set on virtual machines, that is HTTP on one, EMail on second, etc....

First scan of this subset should be enough to find any issues existing within host system. But in reality it is not and may not reveal issues documented for other OS’s that belongs to similar family, so similar family that its issues are shared with "Ubuntu". Thus vulnerabilities of similar OS to Ubuntu may anyway happen in host OS.

Second scan of vulnerability scan subset is build-in scan of OpenVAS named "Full and fast ultimate" with description as "Most NVT’s including those that can stop services/hosts; optimized by using previously collected information".

Third scan of subset is called "Full and very deep ultimate" with difference to previous scan laying in lack of trust to previous scans and in its slowness. Its longest and most wide scan available in OVAS that is meant to display any other issues or information about system that stays hidden previously. If neglected, hacker may find it and use under watchful eyes of administrator.

3 Results

Table 1 show us what ports are opened and what services are probably using them within host "Rome.secnet". Host local network IP address is 192.168.1.10. Next, fingerprint scan tells what services are exactly there. The services detected are presented in Table 2, even though there are very few of them. Lastly, vulnerabilities set of 3 scans display existing issues of host services as in Table 3.

3.1 Port Scanning

When performing a port scan on the system, the ports found to be open are listed in Table 1. Ten TCP opened ports were found and zero of UDP. Already in here, it may be seen that some of opened ports are pointing out services that are not really secure. Unused ports and ports for deprecated services should be closed. There are suggestions to remove ports 110, 143, 445, 139. Add ports 443, 8443. Disable traffic on port 0. Change services on port 80, 8080.

Table 1: Information about open ports

Port	**Service**	**Info**	**Advice**
0	TCP	Counted 10 opened ports in range	Disable traffic
53	DNS	Domain Name System	Keep
80	HTTP	Web Server	Keep and open 443 with HTTPS
8080	HTTP-alt	Web Apps	Keep or change to 8443 to use HTTPS
143	IMAP	Email retrieval	Remove
993	IMAPS	Secure Email retrieval	Keep if used
445	Microsoft-DS	Microsoft network services [1]	Close
139	NetBIOS	Used by Microsoft-DS	Close
110	POP3	Email retrieval	Close
995	POP3S	Secure Email retrieval	Close
22	SSH	Secure data communication	Keep

If email retrieval server is present, then it is suggest to use imaps over pop3s (on ports 993, 995), and this service should be located on different server. If we are short on hardware, it is worth to consider VMware and create two VMs - one for web (80, 443, 8080, 8443)

[1] Includes 'Active Directory: authentication and authorization' and 'SMB: File and printer sharing'.

and one for email (993, 995). Email access to them should be limited by usage of VPN with authentication.

Web server on port 80 should be kept but other port 443 should be opened with HTTPS server. Packets should be redirected from 80 to 443. Similary, web app server should be not with HTTP but with HTTPS, set on port 8080 or new port 8443.

Services of Microsoft-DS and NetBIOS on ports 445, 139 are very outdated and make system vulnerable to attacks, preferably should be removed/replaced by alternative and more secure services with same capabilities like NFS.

DNS on port 53 and SSH on 22 should be kept open.

3.1.1 Port 0

Network traffic sent across the Internet to hosts listening on port 0 might be generated from network attackers or accidentally by applications programmed incorrectly. The response messages that hosts generate in response to port 0 traffic can help attackers learn more about the behavior and potential network vulnerabilities of those devices.

Many internet service providers (ISPs) block traffic on port 0 (both incoming and outgoing messages) to help guard against these exploits.

3.1.2 IMAP/IMAPS (143, 993) and POP3/POP3S (110, 995)

From this scan one may notice presence of IMAP/IMAPS and POP3/POP3S. POP3 is a plain-text protocol, meaning user credentials and emails are sent in plain text, making it easy to hijack email traffic from/to host Rome.Secnet. POP3 over SSL/TLS routes over a SSL-encrypted port, meaning the data is encrypted rather than sent in plain text. Similar is with IMAP and IMAPS, so during interaction with emails, using only POP3S and IMAPS would raise privacy over usage of standard IMAP and POP3 without SSL.

3.1.3 HTTP (80, 8080)

HTTP uses port 80 and 8080. Port 80 is default port in browsers, when client opens page www.webpage.com its actually opening page on TCP port 80, that is: www.webpage.com:80. After oncoming requests pass throught firewall, they go to webserver (nginx/Apache) on port 80, then are pushed to reverse proxy such as back-end Application Server (django, tomcat, node), Static Website, etc... that are on port 8080. Webserver is usually serving static files and app server serves dynamic ones. App server may be further connected to cache, sql server.

Normal usage for port 80 is an http web server to serve up HTML pages. Port 8080 is the defacto port for listening for proxy servers. The proxy listens on port 8080 and then acts as an intermediary between the client and the web server. The value of the proxy is to apply rules and policy to users and the destination site. Policy could be set to block all users for a site but allow an exception groups. They also would provide a common cache for content but as the internet moves to secure websites that value has diminished, see 80 vs 8080.

We should keep both ports open: 80, 8080. But HTTP should be replaced by secure, encrypted version of HTTPS that include adding port 443 and 8443. Even if "we don't have a login screen" or "we don't serve any sensitive data" in our website, usage of HTTPS is not only about confidentiality of data. It also rises overal security, that is assurance, integration and availability. Supporting HTTPS web site has so much more to offer than just protecting passwords and user's sensitive data. Benefits are:

- HTTPS makes things faster!
- Let us use HTTP/2 that replaces 15+ old HTTP/1.1 protocol and gives benefits like: header compression, a multiplexed connection, request priority, etc...! Popular webbrowsers require HTTPS to get benefits of HTTP/2.
- HTTP will be getting nasty warnings, ie. in form of red padlock!
- Stop 3rd party content injection: When you serve your pages over HTTP, anyone along the transport layer can do basically anything they want to your pages. This is where the integrity aspect of HTTPS comes into play and you can make sure that nobody is going to mess with your content along the way.
- Stop malicious content injection:

  Page served over HTTP gives an attacker the opportunity to inject malicious content into a page that is being served up right into the browser of your visitor. This sounds a little too extravagant you might think, but there is a really good, recent example of just how this can be abused.

  The 'Great Cannon of China' as it has been named is an attack tool that was used to launch a notable DDoS attack against GitHub in 2015. In simple terms, the Chinese authorities were intercepting unencrypted traffic and injecting a malicious piece of JavaScript into pages that would continuously submit requests against 2 specific pages on GitHub. These pages hosted technology that would allow users to bypass censorship by the Great Firewall of China and it was probably the hope that GitHub would remove them.
- Deprecating Powerful Features on Insecure Origins of HTTP: Device motion orientation, EME, Fullscreen, Geolocation, getUserMedia(), AppCache
- Better Referrer Data
- iOS and Android are forcing HTTPS. Apple doesn't know what type of data your app is going to send or receive and it might not even be private or sensitive; the

standard has been set and if you want your content or API to be consumed by mobile apps, HTTPS is going to be required.

- Brotli Compression requires HTTPS.
- Encryption introduces only small server overheads: around 1-3%
- Encryption is not at all expensive (ie. Let's Encrypt by Mozilla serves for free)

Closing port 80 is bad for security. We would lose redirects. Browsers still default to HTTP on port 80. It doesn't make us more secure. Another reason that is often mentioned is that if we close port 80 then no communications can happen over the insecure HTTP protocol and no Man in The Middle attacks can take place as a result. Unfortunately, this just isn't the case.

If we close port 80 it doesn't stop the client trying to make their initial connection there and this is where the problem lies. Whether or not we as the host have port 80 open, an attacker can still impersonate us and answer the initial query from the client, which never even needs to reach us.

Keeping port 80 open doesn't directly solve above problem, but if we can catch the client on a previous request and redirect them to port 443 with HTTPS and get a HSTS policy over, we can avoid them using port 80 again in the future. At worst they would hopefully cache the 301 from HTTP to HTTPS for some time and at least get some additional protection.

We give big suggestion to keep 80 open, respond with 301 redirects to move traffic to port 443 with HTTPS, serve a strong HSTS policy and HSTS preload served domain. In the current situation this is the best we can do until something changes.

3.1.4 Microsoft-DS (445) and NetBIOS (139)

The two biggest culprits that we need to worry about in host "Rome.Secnet" are the Server Message Block (SMB) protocol (here Microsoft-DS) and NetBIOS over TCP/IP.

NetBIOS, Microsoft-DS (SMB) and DNS belong to Active Directory Related Ports. Which of these ports actually need to be allowed through the firewall depends on the scenario we are implementing and of used environment.

For instance, support for NetBIOS services may unnecessary in situations where you have newer Windows systems supporting the SMB over IP protocol. Similarly, newer Windows environments make use DNS, instead of Windows-DS for name resolution. For further reference look at ADP.

Serving data to users outside of an internal network, public Web servers are typically the first point of contact for an external attack. In addition, internal networking ports are the most revealing and most often attacked ports on a server. Both services can reveal a wealth of security information and are reoccurring vectors for hacks and attacks. They're unnecessary for the operation of a public Web server.

SMB and NetBios/NetBT services are designed to be accessed by trusted clients inside trusted environments. This means that usually it is not a good idea to expose these services directly to the Internet or, in general, to an environment where untrusted clients can directly access these services. Different options are available to mitigate this issue and protect your server or device:

- Disable NetBios/NetBT and SMB services if you are not using them
- Use your firewall to filter inbound connections to SMB and NetBios/NetBT services, and only allow the trusted IPs and hosts.

In addition to the above suggestions, you should install the OS security updates as soon as possible and ensure SMBv1 is not in use. Closing port 445 may rise problems too, but if you really want 445 closed, any NAT router or personal firewall should be able to block port 445 from the outside world without trouble. Why to close 445?

It is true that SMB protocol is comparably fast in gigabit networks for transferring huge files, but we recommend NFS one of the fastest protocols, because it is directly using the TCP/IP Service. NFSv4 comes with hard security so this one should be used. Also good alternative is WebDAV protocol, that is recognized by many clients, for instance the Windows Explorer. It is much more reliable and standardized than SMB/CIFS (the protocol used by Samba). Here is how-to install the Apache-based WebDAV server on Linux. There is also last possibility how to share files in LAN network, that is usage of SSH protocol.

Note that NetBIOS is legacy and you only need it if you are using old applications or old versions of Windows that require it or use WINS. If your running applications or OS's that require it still, NetBIOS is probably not the real problem here but your outdated environment and system itself. When require netbios?

3.1.5 SSH on port 22

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SSH file transfer (SFTP) or secure copy (SCP) protocols. The standard TCP port 22 has been assigned for contacting SSH servers. It should be kept open. But proper configuration with strong ciphers should be set for it to be secure. If available are weak ciphers usage of SSH may put host under threat ie. by some error.

SSH servers that gives support for 2.0 and 1.99 (e.g. SSH-1.99-OpenSSH_4.1) are really SSH-2 servers that are configured to fall back to using SSH-1 if requested. Fallback to SSH-1 should be avoided, unless you have very specific reasons to keep allowing it.

3.2 Fingerprinting Services

As seen in Table 2, few service was identified from the service fingerprinting scan. Biggest vulnerability was detected in Web-App server container having default files. Next issue lays in possibility of Man-In-The-Middle-Attack using POP3 or IMAP services by OpenSSL protocol of STARTTLS. More secured POP3S and IMAPS were found to have weak ciphers. Most detailed information were found about Domain Name System (DNS) server software called bind 9.7.0-p1 that comes from 2010 and is outdated, when new version is 9.11. From HTTP server service log we know version of this software and host OS, that is Ubuntu.

Table 2: Service fingerprint

Port	Service	Version	Information Retrieved
53	DNS server	bind 9.7.0-p1	Determine which version of BIND name daemon is running.
445	SMB	Samba 3.4.7	Log general/CPE-T determine Samba version on host.
80	HTTP Server	Apache 2.2.14 (Ubuntu)	Log of http (80/tcp) shows version of service.
22	SSH	SSHv2 1.99/2.0	Detected fingerprint and supported version.
8080	Web-App	Apache Tomcat servlet/JSP	Default files detected that may point to specific version.
993 995	SSL ciphers in IMAPS/POP3	SSLv2/3, TLSv1	Weak cipher standards are enabled,

Vulnerability scan of services fingerprints found other services by their issues. All of listed services are old and outdated, generally from 2010, as in table 3. But outdated may not necessarily mean a security problem if all security fixes are applied. Many supported distributions apply security fixes to the version of software they ship. Having report from OpenVAS that only shows outdated version of service, we have to determine whether the proper security patches have been applied.

Unfortunately, we may see that OS of host "Rome.Secnet" which were found is of Ubuntu 10.04 LTS Lucid distribution, that End of Life date is May 9, 2013 for Desktop and April 30, 2015 for Server. After 2013/2015 it was not longer supported, so no new fixed and patches are available for it.

3.2.1 Host "Rome.Secnet" OS

Based on used software, ie. Bind 9.7.0-p1, Apache 2.2.14, Samba 3.47, server OS was determined to be Ubuntu Lucid from 2010, with list of packages in here (link). Also by Samba it was assumed that server is part of SMB/Windows workgroup with the name “WORKGROUP” and user "Rome".

All of the aforementioned services have multiple known security vulnerabilities. They should be updated, removed or changed. Summary with issues is in table 2. Best solution would be upgrade of OS to Ubuntu 16.04.3 LTS that has End of Life dated on 2021.

Table 3: Vulnerability scan fingerprint

Port	**Service**	**Version**	**Issues (mostly outdated, OS end of life with no fixes)**
80	HTTP Web server	Apache HTTP 2.2.14 (Ubuntu)	Replay server type, version and OS
8080	Java servlet/JSP	Apache Tomcat 6.0.24	Replay server type and version.
143 993	IMAP, IMAPS Mail server	Dovecot	-
445	Samba server	3.4.7	Tend to be insecure
22	OpenSSH	SSH-2.0 v5.3p1	Outdated with no new fixes
143 110	IMAP, POP3 (STARTTLS)	-	OpenSSL CVE-2014-0224 Man in the Middle Security Bypass Vulnerability
TCP	TCP Timestamps	RFC1323	Guess uptime of system and see if security patches that require reboot has been applied or not.
993, 995	IMAPS POP3S (SSL Ciphers)	-	Services offers ciphers that are to weak and short.

3.2.2 Ports 80/8080, Apache Tomcat, Apache HTTP

Apache Tomcat 6.0.24 is a java servlet/jsp server that was released in 2010 and comes with Apache Coyote-1.1. Apache HTTP web server of version 2.2.14 (Ubuntu) is from 2009.

What is component in Tomcat and what is role of it in Tomcat server? Tomcat - is a web server, which is having the following components:

- Catalina - Servlet container name. Catalina is Tomcat's servlet container. Catalina implements Sun Microsystems' specifications for servlet and JavaServer Pages (JSP). In Tomcat, a Realm element represents a "database" of usernames, passwords, and roles (similar to Unix groups) assigned to those users. Different implementations of Realm allow Catalina to be integrated into environments where such authentication information is already being created and maintained, and then use that information to implement Container Managed Security as described in the Servlet Specification
- Jasper - JSP engine
- Coyote - HTTP connector. Coyote is a Connector component for Tomcat that supports the HTTP 1.1 protocol as a web server. This allows Catalina, nominally a Java Servlet or JSP container, to also act as a plain web server that serves local files as HTTP documents. Coyote listens for incoming connections to the server on a specific TCP port and forwards the request to the Tomcat Engine to process the request and send back a response to the requesting client. Another Coyote Connector, Coyote JK, listens similarly but instead forwards its requests to another web server, such as Apache, using the JK protocol. This usually offers better performance.
- Cluster - is load balancer to manage large scale application.

Apache Tomcat is used to deploy Java Servlets and JSPs. So in Java project we can build WAR (Web ARchive) file, and just drop it in the deploy directory in Tomcat. Basically Apache is an HTTP Server, serving HTTP. Tomcat is a Servlet and JSP Server serving Java technologies. Tomcat is a servlet container. A servlet, at the end, is a Java class. JSP files (which are similar to PHP, and older ASP files) are generated into Java code (HttpServlet), which is then compiled to .class files by the server and executed by the Java virtual machine.

Apache JSP refers to the Apache Tomcat Server, which is sometimes called Jakarta Tomcat, which is an open source web server. Although it was developed by the Apache Software Foundation (ASF), it uses Java Servlet and JavaServer Pages (JSP) specs to provide an efficient Java HTTP web server environment. JavaServerPages(JSP) itself is a technology that is used to create dynamically generated web sites.

Apache is a general-purpose http server, which supports a number of advanced options that Tomcat doesn't. Although Tomcat can be used as a general purpose HTTP server, you can also set up Apache and Tomcat to work together with Apache serving static content and forwarding the requests for dynamic content to Tomcat. Tomcat is primarily an application server, which serves requests to custom-built Java servlets or JSP files on your server. It is usually used in conjunction with the Apache HTTP server. We use it to manually process incoming requests. The HTTP server, by itself, is best for serving up static content... html files, images, etc.

Each of Apache tomcat base components of Catalina, Coyote and Jasper may have vulnerabilities that transforms them as threats to host security. This threats comes for wide range of versions for Catalina and Coyote, thought not for Jasper.

Catalina may become threat that let attacker to perform: Arbitrary Code Execution, Access Restriction Bypass, Directory Traversal, Cache Poisoning, Timing Attack, Denial of Service (DoS), Information Exposure, Cross-site Scripting (XSS), Improper Authentication, Improper Input Validation, Arbitrary File Read, Cross-site Request Forgery (CSRF), Cryptographic Issues.

Coyote in similar means may let attacker to perform: Information Exposure, Denial of Service (DoS), Arbitrary file upload, Cross-site Scripting (XSS), Access Restriction Bypass, HTTP Request Smuggling, Improper Input Validation.

Least amount of issues is usually found in Jasper and for narrow range of subversions of Jasper 6.0. This threats corresponds to: Access Restriction Bypass, Improper Access Control, Arbitrary File Read, Information Exposure.

Fingerprinting scan let us find that host have high level of vulnerability by existence of default files in servlet/JSP container.

3.2.3 Ports 445, Samba

The SMB server, Samba, is used for Linux/UNIX program interoperability with Windows. The "file and printer sharing" feature of Linux distros is mostly Samba. Samba is an interpretation of Microsoft's network filesystem. Why are Linux systems defaulting to this Microsoft technology? There are lots of users who require that their Linux boxes be able to participate in a heterogeneous network. SMB is the lowest common denominator that seems to be supported on all common operating systems. Is Microsoft's network filesystem so good? From the perspective that it is everywhere, then yes it is good, but as of version from 2010 what we have here: its bad protocol.

Samba of version 3.4.7 found in fingerprint scan, from 2010, has large problems on links with high latency and security issues. It has far too many redundant commands. Samba clearly works, but it's terribly slow, especially compared to NFS. Microsoft has fixed a lot of this with SMB2. Currently there is SMB3. Samba is good for cases where there's Windows boxen involved in the sharing needs. What would be alternative of Linux-native way to share files and printers across a network? NFS is probably the most standard *nix file sharing protocol. LPR or CUPS is the most common Printing protocol.

Security of Samba 3.4.7 or newer? Some versions of Samba 3.6.3 and lower suffer serious security issues which can allow anonymous users to gain root access to a system from an anonymous connection, through the exploitation of an error in Samba's remote procedure call. On 12 April 2016, Badlock, a crucial security bug in Windows and Samba, was disclosed. Badlock for Samba is referenced by CVE-2016-2118 (SAMR and LSA man in the middle attacks possible). On 24 May 2017, it was announced that a remote code execution vulnerability had been found in Samba named EternalRed or SambaCry, affecting all versions since 3.5.0. This vulnerability was assigned identifier CVE-2017-7494. We may see that old and new versions of Samba has vulnerabilities, they best way is to avoid this service.

3.2.4 Port 22, OpenSSH

OpenSSH 5.3p1, used for secure connections between computers, is of a version from 2010, it is obsolete, but it is not necessarily a security problem.

Should we install new version of OpenSSH? Having recommendation to install the latest version, there is no benefit in running the latest version unless we want the latest features. For security, what matters is that we have all the security fixes applied. Many distributions apply security fixes to the version they ship. For example, CentOS 6 still ships OpenSSH 5.3p1 and will be receiving security updates until 2020; CentOS 7, the current release, ships OpenSSH 6.6.1p1. Debian jessie ships OpenSSH 6.7p1 and will also be receiving security updates until 2020, while the latest release stretch ships OpenSSH7.4p1.

In general, we should not install packages outside current distribution for critical infrastructure components such as OpenSSH. If we do, we have to make sure to subscribe to security bulletins and apply security updates as soon as possible. If we just install OpenSSH new version now and forget about it later, we are significantly weakening security of host "Rome.Secnet".

Here we have it on Ubuntu 10.04 Lucid that is no longer supported, so new fixes are not applied to OpenSSH service, like in CentOS 6.9 ported with OpenSSH 5.3p1. CentOS 6.9 it still has bug fixes and oldest item in changelog is from Aug-03-2017.

If OpenSSH service is needed, host OS need to be updated to Ubuntu 16.04.3 LTS, otherwise it port has to be closed.

Is closing the port equivalent to mitigation of all SSH security issues, no matter the version? Closing external SSH access on servers that don't need them is a good idea regardless. One machine where the security updates are falling behind, or one machine where a user's password or key have been compromised, could get the attacker into your network. It's often a good idea to limit external access to a single gateway machine (or a small set of machines for redundancy) where updates and account are more closely monitored. Closing the port in the firewall will mitigate the issue of direct access. Indirect access (where the attacker gets into the network on a machine that's doing nothing important, and uses that as a relay to get into more important machine) will still be a concern.

3.2.5 Ports 143, 110, 993, 995, POP3, IMAP, POP3S, IMAPS

Pop3 and Imap with STARTTLS itself is not a vulnerability, though it offers a larger attack surface given the complexity of the typical TLS implementation. If we don't need it, this service should be taken down according to NIST SP800-123 §4.2.1. Pop3s and Imaps on "rome.secnet" host machine, are supporting SSLv2/3 and TLSv1 ciphers that are too short and weak, and this ciphers should be disabled.

3.3 Vulnerability Scan

As mentioned in 3.2, the vulnerability scan revealed the version of many of the system's services and that they are outdated. With outdated software, that is no longer maintained, or with deprecated OS, it is common that there are publicly known vulnerabilities and weaknesses without fixes or patches. OpenVAS classifies the threats found in the vulnerability scan by severity of high, medium and low with additional logs of performed NVS. This threats, high or low level still gave us information required to find what OS is used by host and to gain some information about users.

About services with issues found in host "Rome.Secnet" we may especially say:

- part of used services are tending to have vulnerabilities in old or new versions, had to be replaced by alternative and less bugged, ie. buggy Samba by NFS and LPR or CUPS
- some services versions are outdated or deprecated, ie. OpenSSH
- there are more secure versions of used ones ie. imap when used should be imaps, or pop3 when should be used pop3s,
- these are publicly known vulnerabilities and weaknesses, that attacker may easly use to penetrate system, ie. ssh with weak ciphers,
- OS of host Ubuntu 10.04 is simply deprecated with no new available fixes to is, should be upgraded to newest LTS version

For manually selected vulnerability scans fitting to OS Ubuntu, vulnerabilities found were: 4 High, 9 Medium, 1 Low, 77 Logs and 0 False Positives. Additionally for automatic scan named Full and Fast Ultimate of OpenVAS based on previous results of port scan and fingerprint scan, we found: 6 High, 14 Medium, 2 Low, 61 Logs and 0 False Positives. Last scan with automatic settings called Full and Very Deep Ultimate found: 7 High, 14 Medium, 2 Low, 61 Logs and 0 False Positives.

Difference in scan settings lay for selection of NVS for OSs. It shows that some services in host OS have vulnerabilities/services not only of Ubuntu, but also of other OSs. Thus we have to secure this host not only for issues known to Ubuntu OS but for matching issues from other distros of Unix family, that make it more complicated. Knowing that host OS is deprecated Ubuntu, attacker may search for critical threats and perform penetration. First required step to rise security is to upgrade system to new LTS Ubuntu, then further security steps should be applied.

Service with issues that were found are:

1. Apache HTTP 2.2.14 server comes with one high and two medium issues:

- High complex vulnerabilities of multiple issues, that may lead to information disclosure or other attacks. Solution lays in upgrade to Apache 2.2.15 or later. This issue is composed of multiple other issues.
- Medium issues is of ETag Header Information Disclosure Weakness that allows to gather information about inode and size.
- Medium issue of 'httpOnly' Cookie Information Disclosure Vulnerability of which successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
- Received response log of HTTP Server type and version shows that host remote web server type is: Apache/2.2.14 (Ubuntu). Solution is to can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

2. Apache Tomcat 6.0.24 Java servlet/JSP Web App server has 2 high risk vulnerabilities and few medium ones plus non-marked logs that in descending order are:

   - High vulnerability by containing default files (doumentation, default Servlets and JSPs) that has to be removed from container to prevent guessing of server information.
   - High vulnerability by Transfer-Encoding information disclosure that may lead to leak of privacy and DOS vulnerabilities. Wide range of versions is affected: 6.0.0 to 6.0.27 and 7.0.0. If current version do not contain available fixes, should be upgraded to outside affected range.
   - Medium issue of 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabilities. This makes Apache Tomcat prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user supplied input.
   - Medium issue of Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability. Apache Tomcat is prone to a remote information-disclosure vulnerability. Remote attackers can exploit this issue to obtain the host name or IP address of the Tomcat server. Information harvested may lead to further attacks.
   - Medium vulnerability of security bypass that allows for remote attackers to exploit this issue to obtain the host name or IP address of the Tomcat server. Information harvested may aid in further attacks.

3. Dovecot server of IMAP (STARTTLS), IMAPS, POP3 (STARTTTLS) and POP3d both using OpenSSL and meant to retrieve, send emails were found to have high risk and two medium risk vulnerabilities:

   - The most critical vulnerability is Middle Security Bypass Vulnerability: a session can be hijacked or compromised.

- OpenSSL uses weak ciphers ie. RC4, DES with short keys of lenght ie. 40. Preferred in descending order are ciphers with key exchange algorithm like ECDH, DH, RSA and encryption algorithms ie. AESGCM, AES256, 3DES, AES. Protocols of SSL 2.0, 3.0 and TLS 1.0 should be disabled. Following configuration of OpenSSL is recommended: ECDH+AESGCM:DH+AESGCM: ECDH+AES256:DH+AES256: ECDH+AES128:DH+AES: ECDH+3DES: DH+3DES: RSA+AESGCM: RSA+AES:RSA+3DES: !aNULL:!MD5
- Other medium issue lays in POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability. The POODLE attack can be used against any system or application that supports SSL 3.0 with CBC mode ciphers. This affects most current browsers and websites, but also includes any software that either references a vulnerable SSL/TLS library (e.g. OpenSSL) or implements the SSL/TLS protocol suite itself. By exploiting this vulnerability in a likely web-based scenario, an attacker can gain access to sensitive data passed within the encrypted web session, such as passwords, cookies and other authentication tokens that can then be used to gain more complete access to a website (impersonating that user, accessing database content, etc.). Recommended are following upgrades: OpenSSL 1.0.1 users should upgrade to 1.0.1j, OpenSSL 1.0.0 users should upgrade to 1.0.0o, OpenSSL 0.9.8 users should upgrade to 0.9.8zc.
- The SSL certificate of the remote service expired 2015-12-04 15:16:06 GMT! Certificate should be reneved.

4. Remaining security risks classified as medium threats were a denial-of-service vulnerability in the SMB server Samba, risk of information-disclosure by the OpenSSH server and one vulnerability related to giving away timestamps, which can potentially open the system for denial-of-service attacks.

5. One threat were classified as low risk, the DNS server bind. The issues related to system's version of bind is mostly related to availability issues, as in cause the DNS server to crash or denial-of-service.

6. Open-ssh server has one medium issue, that is Forced Command Handling Information Disclosure Vulnerability. It reveals version of OpensSSH, that attacker may use to find well know vulnerabilities of this service.

7. BIND DNS has one low NVT issue that lets to determine which version of BIND name daemon is running. Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts. Its still better to hide any information about host system from disclosure.

4 Discussion

First scan of opened ports allowed us to find what kind of services host is having open. Together they compose to web application with email box, files transfer from to Windows workgroup, remote connection and web page hosting. No directly unexpected ports were found, but still some ports should be closed, other opened and else redirected.

Second scan showed what kind of operating system host has and versions of used services. OS of host is deprecated version of Ubuntu 10.04 LTS with passed End of Life Data, no longer maintained, fixes and patched. Many of its services has vulnerabilities that may be used to penetrate system, steal privacy and do denial of service for users. Vulnerability issues were found already during this scan of service fingerprinting.

Third set of vulnerability scans allowed us to see more vulnerabilities, explicit issues for Ubuntu were found and then implicit issues from other OS tend to appear in host system too. Primary reason for issues were outdated system with outdated services without no new patches, layman configuration with garbage files left, configuration left for spying general services information, weak ciphers in OpenSSL.

Recommended is to upgrade OS to new version with LTS, like Ubuntu 16.04 LTS with End of Life Data at 2021. Then delete default files from Apache Tomcat Container. Set flags hiding services information. Disable SSL 2/3, TLS 1 in Dovecot. Use strong ciphers for SSH. Configure OpenSSL with: ECDH+AESGCM: DH+AESGCM:ECDH+AES256: DH+AES256:ECDH+AES128: DH+AES:ECDH+3DES: DH+3DES:RSA+AESGCM: RSA+AES: RSA+3DES:!aNULL:!MD5. Change Samba to NFS or stay only with SSH. Open HTTPS web HTTP server on port 443 and HTTPS web app server on port 8080/8443 with reverted proxy of port 80 with HTTP.

Table 4 contains summary of discussed services. After upgrade to new OS, it is required to bring all of security fixes and patches to used services, then further steps are described in table for each service that need to be tended after OS upgrade.

Table 4: Summary of vulnerability scan recommendations

Service Name	**Problems**	**Suggestions**
Ubuntu 10.04 LTS	End of Life	Upgrade to 16.04 LTS
Apache Tomcat 6.0.24	Contains default files.	Clean JPS container from default files. Use Web-App server with SSL on 8443 or 8080.
Apache 2.2.14	Limit response headers content. Usage of plaintext HTTP	Set directive ’ServerTokens Prod’. Redirects to HTTPS on port 443. Open HTTPS server on port 443.
OpenSSL	Weak ciphers	Configure as mentioned in section 4.
Samba 3.4.7	Tend to be vulnerable	Close by firewall or replace by NFS or LPR and CUPS
OpenSSH 5.3p1	Fallback to SSHv1	config line "Protocol 2,1" should have ",1" removed
Dovecot POP3, IMAP	POP3 and IMAP are in plaintext	Disable POP3 and IMAP
Dovecot POP3s, IMAPs	Weak ciphers	Disable SSLv2/3, TLSv1
NetBIOS	Unnecessary with Bind DNS	Remove

5 Conclusion

Conclusion is stated as the host “Rome.Secnet” is not secure, because of outdated OS and software. The host could be considered initially secure after upgrade and update. After recommended setup is done, further checks should be performed with new security evaluation.

OpenVAS is great tool that allows for security personnel to get familiar with tested system in short amount of time. Having given by it possibility of scheduled scans, the frequently updated NVTs and the alert function, security personnel can periodically collect overview over a host state and to monitor its security issues.

Sometimes we can’t remove some services or use alternative ones. This way by introduction of OpenVAS, we can discover vulnerabilities with some suggestions as fast as OpenVAS database is updated. Then we may apply fixes in fastest time possible on in worst case disable service (but this should be avoided).

Security personnel has yet to keep in mind, than OVAS is only a tool, and security of system is put in their hand. Constant research over services, familiarity with services and manual tests for more sensitive ones is required.

Updates of system by fixes and patches should be done in daily basis without necessity of version change. Deprecated OS and services should be avoided, specially services open to network. If they exist on system, should be removed. Services that tend to have vulnerabilities should be avoided and more secure ones should be used. It is possible to use OS that has longer time of support than Ubuntu, like CentOS. Otherwise new Ubuntu 16.04 LTS should be used. Suggested strongly is to not use many services with similar functions, but only one service for one kind of activity.

System should lay behind firewall, with only part of services open to outside, like HTTP server, EMail server, DNS server and SSH server. Other ports should have blocked access by default by firewall, so this access can only be granted to narrow range of trusted personnel. SSH should give access only by key pair, not by password.

6 Comments

Some of the points that you should discuss in your review:

6.1 Check if all the requirements from the template have been covered.

No all are covered.

6.2 Is the report written in a clear voice? Is it easy to follow?

Special attention was put to it. Report was read few times with correction each time.

6.3 Introduction:

6.3.1 Is the purpose of the report clear?

It has been stated.

6.3.2 Is it clear what is contained in this report?

Content of report has been shortly described in order.

6.4 Description of OpenVAS setup

6.4.1 Does the report explain the different components of the vulnerability assessment system used?

Suggestions from feedback were used.

6.4.2 Does the report describe the scans that are performed (their configuration) and also a motivation for choosing them (what is their aim)?

It was correct, but some changes were added.

6.4.3 Is it possible to repeat the scans (for result validation) based on the information presented here?

As above.

6.5 Presentation of results

Results were presented with additional research.

6.5.1 Does the report contain results (most important ones) for each of the scans performed?

Report contain results which were deduced as important ones, but even if security of system is graded by its weakest point we can not forgot about less weak points.

6.5.2 Is there enough information describing the results in the report?

Information were added.

6.6 Discussion of results

6.6.1 Does the report contain a detailed discussion of most of the results obtained (at least for the most important ones)?

No it does. All important aspects were mentioned with solutions.

6.6.2 Are the suggestions and decisions properly motivated?

Yes.

6.6.3 Are the initial recommendations updated (with the help of new results and findings)?

Yes.

6.7 Conclusions

6.7.1 Are the main findings of the report highlighted?

They are.

6.7.2 Do the authors present a strategy (a short list of actions) that can be followed to better secure the system?

Strategy is granted.

6.8 References

Additional references were given.

6.8.1 Are the external sources used in the report properly referred to?

Yes.

6.9 General

6.9.1 Are the figures and tables properly used and referred to?

Yes, this was corrected.

6.9.2 Grammar/structure of paper?

Grammar error were corrected.

6.9.3 Spelling errors (we hope all authors will use a spell checker before submitting the report, but please also comment if that is the case)?

Spelling errors were corrected.

References

[1] OpenVAS. *About OpenVAS*. 2015. URL: `http://www.openvas.org/about.html` (visited on 03/03/2015).

[2] Wikipedia. *Vulnerability scanner*. 2014. URL: `http://en.wikipedia.org/wiki/Vulnerability_scanner` (visited on 03/03/2015).

[3] The Government of the Hong Kong Special Administrative Region. *AN OVERVIEW OF VULNERABILITY SCANNERS*. 2008. URL: `http://www.infosec.gov.hk/english/technical/files/vulnerability.pdf` (visited on 03/03/2015).

[4] URL: `https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers`.

[5] *Service Name and Transport Protocol Port Number Registry*. 2018. URL: `https://www.iana.org/assignments/service-names-port-numbers/service-namesport-numbers.xhtml`.

A Report from OpenVAS Vulnerability Scanning

Scan Report

February 25, 2018

Summary

This document reports on the results of an automatic security scan. The scan started at Sun Feb 25 07:38:09 2018 UTC and ended at Sun Feb 25 08:04:06 2018 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview **2**

2 Results per Host **2**

2.1 192.168.1.10 2

2.1.1 High http (80/tcp) 3

2.1.2 High http-alt (8080/tcp) 3

2.1.3 High imap (143/tcp) 5

2.1.4 High imaps (993/tcp) 5

2.1.5 High pop3 (110/tcp) 6

2.1.6 High pop3s (995/tcp) 6

2.1.7 Medium http (80/tcp) 7

2.1.8 Medium http-alt (8080/tcp) 8

2.1.9 Medium imaps (993/tcp) 10

2.1.10 Medium pop3s (995/tcp) 12

2.1.11 Medium general/tcp 13

2.1.12 Medium netbios-ssn (139/tcp) 14

2.1.13 Medium ssh (22/tcp) 14

2.1.14 Low domain (53/tcp) 15

2.1.15 Low general/icmp 15

2.1.16 Log http (80/tcp) 16

2.1.17 Log http-alt (8080/tcp) 17

2.1.18 Log imap (143/tcp) 19

2.1.19 Log imaps (993/tcp) 20

2.1.20 Log pop3 (110/tcp) 23
2.1.21 Log pop3s (995/tcp) 23
2.1.22 Log general/tcp 25
2.1.23 Log netbios-ssn (139/tcp) 28
2.1.24 Log ssh (22/tcp) 28
2.1.25 Log domain (53/tcp) 29
2.1.26 Log general/icmp 30
2.1.27 Log domain (53/udp) 31
2.1.28 Log general/CPE-T 31
2.1.29 Log general/HOST-T 31
2.1.30 Log general/SMBClient 32
2.1.31 Log microsoft-ds (445/tcp) 32
2.1.32 Log netbios-ns (137/udp) 34

1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.1.10 (rome.secnet)	Severity: High	7	14	2	61	0
Total: 1		7	14	2	61	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 84 results selected by the filtering described above. Before filtering there were 85 results.

2 Results per Host

2.1 192.168.1.10

Host scan start	Sun Feb 25 07:38:14 2018 UTC
Host scan end	Sun Feb 25 08:04:06 2018 UTC

Service (Port)	Threat Level
http (80/tcp)	High
http-alt (8080/tcp)	High
imap (143/tcp)	High
imaps (993/tcp)	High
pop3 (110/tcp)	High
pop3s (995/tcp)	High
http (80/tcp)	Medium
http-alt (8080/tcp)	Medium
imaps (993/tcp)	Medium
pop3s (995/tcp)	Medium
general/tcp	Medium
netbios-ssn (139/tcp)	Medium
ssh (22/tcp)	Medium
domain (53/tcp)	Low
general/icmp	Low
http (80/tcp)	Log
http-alt (8080/tcp)	Log
imap (143/tcp)	Log
imaps (993/tcp)	Log
pop3 (110/tcp)	Log

. . . (continues) . . .

. . . (continued) . . .

Service (Port)	Threat Level
pop3s (995/tcp)	Log
general/tcp	Log
netbios-ssn (139/tcp)	Log
ssh (22/tcp)	Log
domain (53/tcp)	Log
general/icmp	Log
domain (53/udp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/SMBClient	Log
microsoft-ds (445/tcp)	Log
netbios-ns (137/udp)	Log

2.1.1 High http (80/tcp)

High (CVSS: 10.0)
NVT: Apache Multiple Security Vulnerabilities

```
 Summary:
 Apache is prone to multiple vulnerabilities.
These issues may lead to information disclosure or other attacks.
Apache versions prior to 2.2.15 are affected.
 Solution:
 Upgrade to  Apache 2.2.15 or Later.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100514

References

```
CVE: CVE-2010-0425, CVE-2010-0434, CVE-2010-0408, CVE-2007-6750
BID:38494, 38491
Other:
  URL:http://www.securityfocus.com/bid/38494
   URL:http://httpd.apache.org/security/vulnerabilities_22.html
   URL:http://httpd.apache.org/
   URL:https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
   URL:http://svn.apache.org/viewvc?view=revision&amp;revision=917870
```

[return to 192.168.1.10]

2.1.2 High http-alt (8080/tcp)

High (CVSS: 6.8)
NVT: Apache Tomcat servlet/JSP container default files

```
Default files, such as documentation, default Servlets and JSPs were found on
the Apache Tomcat servlet/JSP container.
Remove default files, example JSPs and Servlets from the Tomcat
Servlet/JSP container.
These files should be removed as they may help an attacker to guess the
exact version of Apache Tomcat which is running on this host and may provide
other useful information.
The following default files were found :
/examples/servlets/index.html
/examples/jsp/snp/snoop.jsp
/examples/jsp/index.html
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.12085

High (CVSS: 6.4)
NVT: Apache Tomcat 'Transfer-Encoding' Information Disclosure and Denial Of Service Vulnerabilities

Product detection result

```
cpe:/a:apache:tomcat:6.0.24
Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)
```

```
 Summary:
 Apache Tomcat is prone to multiple remote vulnerabilities including
information-disclosure and denial-of-service issues.
Remote attackers can exploit these issues to cause denial-of-service
conditions or gain access to potentially sensitive information;
information obtained may lead to further attacks.
The following versions are affected:
Tomcat 5.5.0 to 5.5.29 Tomcat 6.0.0 to 6.0.27 Tomcat 7.0.0
Tomcat 3.x, 4.x, and 5.0.x may also be affected.
 Solution:
 The vendor released updates. Please see the references for more
information.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100712

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
CVE: CVE-2010-2227
BID:41544
Other:
  URL:https://www.securityfocus.com/bid/41544
   URL:http://tomcat.apache.org/security-5.html
   URL:http://tomcat.apache.org/security-6.html
   URL:http://tomcat.apache.org/security-7.html
   URL:http://tomcat.apache.org/
   URL:http://www.securityfocus.com/archive/1/512272
```

[return to 192.168.1.10]

2.1.3 High imap (143/tcp)

High (CVSS: 6.8)
NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)

OID of test routine: 1.3.6.1.4.1.25623.1.0.105043

References

```
CVE: CVE-2014-0224
BID:67899
Other:
  URL:http://www.securityfocus.com/bid/67899
   URL:http://openssl.org/
```

[return to 192.168.1.10]

2.1.4 High imaps (993/tcp)

High (CVSS: 6.8)
NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

OID of test routine: 1.3.6.1.4.1.25623.1.0.105042

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
CVE: CVE-2014-0224
BID:67899
Other:
  URL:http://www.securityfocus.com/bid/67899
   URL:http://openssl.org/
```

[return to 192.168.1.10]

2.1.5 High pop3 (110/tcp)

High (CVSS: 6.8)
NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)

OID of test routine: 1.3.6.1.4.1.25623.1.0.105043

References

```
CVE: CVE-2014-0224
BID:67899
Other:
  URL:http://www.securityfocus.com/bid/67899
   URL:http://openssl.org/
```

[return to 192.168.1.10]

2.1.6 High pop3s (995/tcp)

High (CVSS: 6.8)
NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

OID of test routine: 1.3.6.1.4.1.25623.1.0.105042

References

```
CVE: CVE-2014-0224
BID:67899
Other:
  URL:http://www.securityfocus.com/bid/67899
   URL:http://openssl.org/
```

[return to 192.168.1.10]

2.1.7 Medium http (80/tcp)

Medium (CVSS: 4.3)
NVT: Apache Web Server ETag Header Information Disclosure Weakness

```
Information that was gathered:
Inode: 152086
Size: 177
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103122

References

```
CVE: CVE-2003-1418
BID:6939
Other:
  URL:https://www.securityfocus.com/bid/6939
   URL:http://httpd.apache.org/docs/mod/core.html#fileetag
   URL:http://www.openbsd.org/errata32.html
   URL:http://support.novell.com/docs/Tids/Solutions/10090670.html
```

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

```
  Summary:
  This host is running Apache HTTP Server and is prone to cookie
  information disclosure vulnerability.
  Vulnerability Insight:
  The flaw is due to an error within the default error response for
  status code 400 when no custom ErrorDocument is configured, which can be
  exploited to expose 'httpOnly' cookies.
  Impact:
  Successful exploitation will allow attackers to obtain sensitive information
  that may aid in further attacks.
  Impact Level: Application
  Affected Software/OS:
  Apache HTTP Server versions 2.2.0 through 2.2.21
  Solution:
  Upgrade to Apache HTTP Server version 2.2.22 or later,
  For updates refer to http://httpd.apache.org/
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.902830

References

```
CVE: CVE-2012-0053
BID:51706
Other:
  URL:http://osvdb.org/78556
   URL:http://secunia.com/advisories/47779
   URL:http://www.exploit-db.com/exploits/18442
   URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html
   URL:http://httpd.apache.org/security/vulnerabilities_22.html
   URL:http://svn.apache.org/viewvc?view=revision&amp;revision=1235454
   URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l
```

[return to 192.168.1.10]

2.1.8 Medium http-alt (8080/tcp)

Medium (CVSS: 4.3)
NVT: Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabilities

Product detection result

```
cpe:/a:apache:tomcat:6.0.24
Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)
```

```
 Summary:
 Apache Tomcat is prone to multiple cross-site scripting
vulnerabilities because it fails to properly sanitize user-
supplied input.
An attacker may leverage these issues to execute arbitrary script code
in the browser of an unsuspecting user in the context of the affected
site. This may let the attacker steal cookie-based authentication
credentials and launch other attacks.
 Solution:
 Updates are available; please see the references for more information.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103032

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
CVE: CVE-2010-4172
BID:45015
Other:
  URL:https://www.securityfocus.com/bid/45015
   URL:http://tomcat.apache.org/security-6.html
   URL:http://tomcat.apache.org/security-7.html
   URL:http://tomcat.apache.org/security-6.html
   URL:http://tomcat.apache.org/security-7.html
   URL:http://jakarta.apache.org/tomcat/
   URL:http://www.securityfocus.com/archive/1/514866
```

Medium (CVSS: 2.6)
NVT: Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability

Product detection result

```
cpe:/a:apache:tomcat:6.0.24
Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)
```

```
 Summary:
 Apache Tomcat is prone to a remote information-disclosure
vulnerability.
Remote attackers can exploit this issue to obtain the host name or IP
address of the Tomcat server. Information harvested may lead to
further attacks.
The following versions are affected:
Tomcat 5.5.0 through 5.5.29 Tomcat 6.0.0 through 6.0.26
Tomcat 3.x, 4.0.x, and 5.0.x may also be affected.
 Solution:
 Updates are available. Please see the references for more information.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100598

References

```
CVE: CVE-2010-1157
BID:39635
Other:
  URL:http://www.securityfocus.com/bid/39635
   URL:http://tomcat.apache.org/security-5.html
   URL:http://tomcat.apache.org/security-6.html
   URL:http://tomcat.apache.org/
   URL:http://svn.apache.org/viewvc?view=revision&amp;revision=936540
   URL:http://svn.apache.org/viewvc?view=revision&amp;revision=936541
   URL:http://www.securityfocus.com/archive/1/510879
```

Medium (CVSS: 2.6)
NVT: Apache Tomcat Security bypass vulnerability

Product detection result

```
cpe:/a:apache:tomcat:6.0.24
Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)
```

```
  Summary:
  This host is running Apache Tomcat server and is prone to security
  bypass vulnerability.
  Vulnerability Insight:
  The flaw is caused by 'realm name' in the 'WWW-Authenticate' HTTP header for
  'BASIC' and 'DIGEST' authentication that might allow remote attackers to
  discover the server's hostname or IP address by sending a request for a
  resource.
  Impact:
  Remote attackers can exploit this issue to obtain the host name or IP address
  of the Tomcat server. Information harvested may aid in further attacks.
  Impact Level: Application
  Affected Software/OS:
  Apache Tomcat version 5.5.0 to 5.5.29
  Apache Tomcat version 6.0.0 to 6.0.26
  Solution:
  Upgrade to the latest version of Apache Tomcat 5.5.30 or 6.0.27 or later,
  For updates refer to http://tomcat.apache.org
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.901114

References

```
CVE: CVE-2010-1157
BID:39635
Other:
  URL:http://tomcat.apache.org/security-5.html
   URL:http://tomcat.apache.org/security-6.html
   URL:http://www.securityfocus.com/archive/1/510879
```

[return to 192.168.1.10]

2.1.9 Medium imaps (993/tcp)

Medium (CVSS: 4.3)
NVT: Check for SSL Weak Ciphers

. . . continues on next page . . .

. . . continued from previous page . . .

```
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

Medium (CVSS: 4.3)
NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

OID of test routine: 1.3.6.1.4.1.25623.1.0.802087

References

```
CVE: CVE-2014-3566
BID:70574
Other:
  URL:http://osvdb.com/113251
   URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
   URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
   URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit
↪ing-ssl-30.html
```

Medium (CVSS: 0.0)
NVT: SSL Certificate Expiry

```
The SSL certificate of the remote service expired 2015-12-04 15:16:06 GMT!
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.15901

[return to 192.168.1.10]

2.1.10 Medium pop3s (995/tcp)

Medium (CVSS: 4.3)
NVT: Check for SSL Weak Ciphers

```
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

Medium (CVSS: 4.3)
NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.802087

References

```
CVE: CVE-2014-3566
BID:70574
Other:
  URL:http://osvdb.com/113251
   URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
   URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
   URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit
↪ing-ssl-30.html
```

Medium (CVSS: 0.0)
NVT: SSL Certificate Expiry

```
The SSL certificate of the remote service expired 2015-12-04 15:16:06 GMT!
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.15901

[return to 192.168.1.10]

2.1.11 Medium general/tcp

Medium (CVSS: 2.6)
NVT: TCP timestamps

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 404802583
Paket 2: 404802685
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80091

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

[return to 192.168.1.10]

2.1.12 Medium netbios-ssn (139/tcp)

Medium (CVSS: 5.0)
NVT: Samba Multiple Remote Denial of Service Vulnerabilities

```
 Summary:
 Samba is prone to multiple remote denial-of-service vulnerabilities.
An attacker can exploit these issues to crash the application, denying
service to legitimate users.
Versions prior to Samba 3.4.8 and 3.5.2 are vulnerable.
 Solution:
 Updates are available. Please see the references for more information.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100644

References

```
CVE: CVE-2010-1635
BID:40097
Other:
  URL:http://www.securityfocus.com/bid/40097
   URL:https://bugzilla.samba.org/show_bug.cgi?id=7254
   URL:http://samba.org/samba/history/samba-3.4.8.html
   URL:http://samba.org/samba/history/samba-3.5.2.html
   URL:http://www.samba.org
```

[return to 192.168.1.10]

2.1.13 Medium ssh (22/tcp)

Medium (CVSS: 3.5)
NVT: openssh-server Forced Command Handling Information Disclosure Vulnerability

```
According to its banner, the version of OpenSSH installed on the remote
host is older than 5.7:
 ssh-2.0-openssh_5.3p1 debian-3ubuntu7
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103503

References

```
CVE: CVE-2012-0814
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
BID:51702
Other:
  URL:http://www.securityfocus.com/bid/51702
   URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445
   URL:http://packages.debian.org/squeeze/openssh-server
   URL:https://downloads.avaya.com/css/P8/documents/100161262
```

[return to 192.168.1.10]

2.1.14 Low domain (53/tcp)

Low (CVSS: 5.0)
NVT: Determine which version of BIND name daemon is running

```
BIND 'NAMED' is an open-source DNS server from ISC.org.
Many proprietary DNS servers are based on BIND source code.
The BIND based NAMED servers (or DNS servers) allow remote users
to query for version and type information.  The query of the CHAOS
TXT record 'version.bind', will typically prompt the server to send
the information back to the querying source.
The remote bind version is : 9.7.0-P1
Solution :
Using the 'version' directive in the 'options' section will block
the 'version.bind' query, but it will not log such attempts.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10028

[return to 192.168.1.10]

2.1.15 Low general/icmp

Low (CVSS: 0.0)
NVT: Record route

```
Here is the route recorded between 192.168.1.1 and 192.168.1.10 :
192.168.1.10.
192.168.1.10.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.12264

[return to 192.168.1.10]

2.1.16 Log http (80/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: HTTP Server type and version

```
The remote web server type is :
Apache/2.2.14 (Ubuntu)
Solution : You can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10107

Log (CVSS: 0.0)
NVT: Services

```
A web server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Directory Scanner

```
The following directories were discovered:
/cgi-bin, /icons
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11032

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
Other:
  OWASP:OWASP-CM-006
```

Log (CVSS: 0.0)
NVT: wapiti (NASL wrapper)

```
wapiti could not be found in your system path.
OpenVAS was unable to execute wapiti and to perform the scan you
requested.
Please make sure that wapiti is installed and that wapiti is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80110

Log (CVSS: 0.0)
NVT: Apache Web ServerVersion Detection

```
Detected Apache version: 2.2.14
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.2.14
Concluded from version identification result:
Server: Apache/2.2.14
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900498

[return to 192.168.1.10]

2.1.17 Log http-alt (8080/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: HTTP Server type and version

```
The remote web server type is :
Apache-Coyote/1.1
and the 'ServerTokens' directive is ProductOnly
Apache does not permit to hide the server type.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10107

Log (CVSS: 0.0)
NVT: Services

```
A web server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Web mirroring

```
The following CGI have been discovered :
Syntax : cginame (arguments [default value])
/examples/servlets/servlet/RequestParamExample (firstname [] lastname [] )
/examples/jsp/jsp2/el/implicit-objects.jsp (foo [bar] )
/examples/jsp/jsp2/el/functions.jsp (foo [JSP+2.0] )
/examples/servlets/servlet/CookieExample (cookiename [] cookievalue [] )
/examples/servlets/servlet/SessionExample;jsessionid=B238ED29D00E87A60B10880058D
↪1BC11 (dataname [] datavalue [] )
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10662

Log (CVSS: 0.0)
NVT: Directory Scanner

```
The following directories were discovered:
/docs, /examples
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.11032

References

```
Other:
  OWASP:OWASP-CM-006
```

Log (CVSS: 0.0)
NVT: Apache Tomcat Version Detection

```
Detected Apache Tomcat version: 6.0.24
Location: 8080/tcp
CPE: cpe:/a:apache:tomcat:6.0.24
Concluded from version identification result:
Apache Tomcat/6.0.24
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.800371

Log (CVSS: 0.0)
NVT: wapiti (NASL wrapper)

```
wapiti could not be found in your system path.
OpenVAS was unable to execute wapiti and to perform the scan you
requested.
Please make sure that wapiti is installed and that wapiti is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80110

[return to 192.168.1.10]

2.1.18 Log imap (143/tcp)

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
An IMAP server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: IMAP STARTTLS Detection

```
 Summary:
 The remote IMAP Server supports the STARTTLS command.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.105007

Log (CVSS: 0.0)
NVT: IMAP Banner

```
The remote imap server banner is :
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS L
↪OGINDISABLED] Dovecot ready.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11414

[return to 192.168.1.10]

2.1.19 Log imaps (993/tcp)

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
A TLSv1 server answered on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Services

```
An IMAP server is running on this port through SSL
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: IMAP Banner

```
The remote imap server banner is :
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN
↪] Dovecot ready.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11414

Log (CVSS: 0.0)
NVT: Check for SSL Ciphers

```
Service supports SSLv2 ciphers.
Service supports SSLv3 ciphers.
Service supports TLSv1 ciphers.
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_EDH_RSA_DES_192_CBC3_SHA
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
No non-ciphers are supported by this service
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802067

Log (CVSS: 0.0)
NVT: Check for SSL Medium Ciphers

```
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.902816

[return to 192.168.1.10]

2.1.20 Log pop3 (110/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
A pop3 server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: POP3 STARTTLS Detection

```
 Summary:
 The remote POP3 Server supports the STARTTLS command.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.105008

[return to 192.168.1.10]

2.1.21 Log pop3s (995/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
A TLSv1 server answered on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Services

```
A pop3 server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Check for SSL Ciphers

```
Service supports SSLv2 ciphers.
Service supports SSLv3 ciphers.
Service supports TLSv1 ciphers.
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
Weak ciphers offered by this service:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
No non-ciphers are supported by this service
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802067

Log (CVSS: 0.0)
NVT: Check for SSL Medium Ciphers

```
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902816

[return to 192.168.1.10]

2.1.22 Log general/tcp

Log (CVSS: 7.8)
NVT: 3com switch2hub

```
Fake IP address not specified. Skipping this check.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80103

Log (CVSS: 0.0)
NVT: OS fingerprinting

```
ICMP based OS fingerprint results: (91% confidence)
Linux Kernel
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102002

References

```
Other:
  URL:http://www.phrack.org/issues.html?issue=57&amp;id=7#article
```

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

```
DIRB could not be found in your system path.
OpenVAS was unable to execute DIRB and to perform the scan you
requested.
Please make sure that DIRB is installed and is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103079

Log (CVSS: 0.0)
NVT: Checks for open udp ports

```
Open UDP ports: [None found]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103978

Log (CVSS: 0.0)
NVT: arachni (NASL wrapper)

```
Arachni could not be found in your system path.
OpenVAS was unable to execute Arachni and to perform the scan you
requested.
Please make sure that Arachni is installed and that arachni is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.110001

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

```
Nikto could not be found in your system path.
OpenVAS was unable to execute Nikto and to perform the scan you
requested.
Please make sure that Nikto is installed and that nikto.pl or nikto is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.14260

Log (CVSS: 0.0)
NVT: Traceroute

```
Here is the route from 192.168.1.1 to 192.168.1.10:
192.168.1.1
192.168.1.10
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

Log (CVSS: 0.0)
NVT: Microsoft SMB Signing Disabled

```
SMB signing is disabled on this host
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802726

Log (CVSS: 0.0)
NVT: Checks for open tcp ports

```
Open TCP ports: 80, 110, 445, 993, 22, 8080, 995, 139, 53, 143
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 192.168.1.10]

2.1.23 Log netbios-ssn (139/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: SMB on port 445

```
An SMB server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11011

[return to 192.168.1.10]

2.1.24 Log ssh (22/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
SSHv2 Fingerprint: 0c:d8:26:b3:dd:f0:d4:83:57:95:78:f8:5a:0c:ae:53
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100259

Log (CVSS: 0.0)
NVT: SSH Server type and version

```
Detected SSH server version: SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7
Remote SSH supported authentication: publickey,password
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:5.3p1
Concluded from remote connection attempt with credentials:
  Login: OpenVAS
  Password: OpenVAS
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10267

Log (CVSS: 0.0)
NVT: Services

```
An ssh server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 192.168.1.10]

2.1.25 Log domain (53/tcp)

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

Log (CVSS: 0.0)
NVT: DNS Server Detection

```
 Summary:
 A DNS Server is running at this Host.
A Name Server translates domain names into IP addresses. This makes it
possible for a user to access a website by typing in the domain name instead of
the website's actual IP address.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

[return to 192.168.1.10]

2.1.26 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

```
 Summary:
 The remote host responded to an ICMP timestamp request. The Timestamp Reply is
an ICMP message which replies to a Timestamp message. It consists of the
originating timestamp sent by the sender of the Timestamp as well as a receive
timestamp and a transmit timestamp. This information could theoretically be used
to exploit weak time-based random number generators in other services.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103190

References

```
CVE: CVE-1999-0524
Other:
  URL:http://www.ietf.org/rfc/rfc0792.txt
```

[return to 192.168.1.10]

2.1.27 Log domain (53/udp)

Log (CVSS: 0.0)
NVT: DNS Server Detection

```
 Summary:
 A DNS Server is running at this Host.
A Name Server translates domain names into IP addresses. This makes it
possible for a user to access a website by typing in the domain name instead of
the website's actual IP address.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

[return to 192.168.1.10]

2.1.28 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
192.168.1.10|cpe:/a:samba:samba:3.4.7
192.168.1.10|cpe:/a:apache:tomcat:6.0.24
192.168.1.10|cpe:/a:apache:http_server:2.2.14
192.168.1.10|cpe:/a:openbsd:openssh:5.3p1
192.168.1.10|cpe:/o:canonical:ubuntu_linux
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 192.168.1.10]

2.1.29 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:192.168.1.1,192.168.1.10
TCP ports:80,110,445,993,22,8080,995,139,53,143
UDP ports:
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 192.168.1.10]

2.1.30 Log general/SMBClient

Log (CVSS: 0.0)
NVT: SMB Test

```
The tool "smbclient" is not available for openvasd.
Therefore none of the tests using smbclient are executed.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

[return to 192.168.1.10]

2.1.31 Log microsoft-ds (445/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

```
 Summary:
 It is possible to extract OS, domain and SMB server information
from the Session Setup AndX Response packet which is generated
during NTLM authentication.Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.4.7
Detected OS: Unix
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102011

Log (CVSS: 0.0)
NVT: SMB log in

```
It was possible to log into the remote host using the SMB protocol.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10394

Log (CVSS: 0.0)
NVT: SMB on port 445

```
A CIFS server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11011

Log (CVSS: 0.0)
NVT: SMB Brute Force Logins With Default Credentials

```
It was possible to log into the remote host using the SMB protocol.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.804449

Log (CVSS: 0.0)
NVT: SMB Brute Force Logins With Default Credentials

```
It was possible to log into the remote host using the SMB protocol.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.804449

Log (CVSS: 0.0)
NVT: Microsoft Windows SMB Accessible Shares

```
The following shares where found
IPC$
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.902425

[return to 192.168.1.10]

2.1.32 Log netbios-ns (137/udp)

Log (CVSS: 0.0)
NVT: Using NetBIOS to retrieve information from a Windows host

```
The following 7 NetBIOS names have been gathered :
 ROME            = This is the computer name registered for workstation services
↪ by a WINS client.
 ROME            = This is the current logged in user registered for this workst
↪ation.
 ROME            = Computer name
   __MSBROWSE__
 WORKGROUP
 WORKGROUP       = Workgroup / Domain name (part of the Browser elections)
 WORKGROUP       = Workgroup / Domain name
. This SMB server seems to be a SAMBA server (this is not a security
risk, this is for your information). This can be told because this server
claims to have a null MAC address
If you do not want to allow everyone to find the NetBios name
of your computer, you should filter incoming traffic to this port.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10150

[return to 192.168.1.10]