Security Testing Report for KIPITO OY

Ville – Pulkkinen

Mikael – Romanov

Niko – Tamminen

Juho - Askola

DST_Group8

Table of Contents

Task: Scan for kipito

Name:	**Scan for kipito**
Comment:	
Target:	Kipito IP
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes
	Apply Overrides: yes
	Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner)
	Scan Config: Full and fast
	Order for target hosts: Sequential
	Network Source Interface:
	Maximum concurrently executed NVTs per host: 4
	Maximum concurrently scanned hosts: 20
Status:	Done
Duration of last scan:	45 minutes 11 seconds
Average scan duration:	22 minutes 53 seconds
Reports:	2 (Finished: 2, Last: Oct 12 2017)
Results:	30
Notes:	0
Overrides:	0

1.0 SUMMARY

1.1 Introduction

The objective of this assessment is to perform an external and internal network security test against the KIPITO OY corporate network.

1.2 Objective

Objective is to find possible external and internal vulnerabilities and do a security assessment to KIPITO OY

1.3 Requirements

To complete this task, we need to have specified IP address range and access to the network for penetration and vulnerability testing. We also need to have tools to achieve our goal. We obtain our goal by using Kali Linux, which has OpenVAS installed.

1.4 Kipito report –Summary

This report contains results from the network security test towards Kipito OY's public network. The focus of this test is to evaluate the network security, identify systems, and perform vulnerability analysis while reporting the findings back to Kipito OY.

2. Kipito data security testing – Technical Report

2.1 Tools

The tools we used to conduct the security assessment were following.

Tool and version	
Nmap	Version 7.60
OpenVAS	Version 7.02
Zenmap	Version 7.60
Netdiscover	Version 0.3-pre-beta7

2.2 Executed Test Cases

Test Cases	
Executed tests provided by Nmap	Port and service enumeration scan.
Executed tests provided by OpenVAS	Vulnerability scan.

2.3 Information Gathering

Our assignment was to scan external network vulnerabilities only for IP address: 192.58.41.108 and internal networks two subnets 192.168.1.0/24 and 192.168.2.0/24. We tested the assigned network for vulnerabilities and reported our findings to the customer. We started to gather information by scanning the assigned IP address with nmap and netdiscovery. We scanned for open ports, services and operating systems. We also used zenmap in case something was undiscovered. Lastly, we assigned OpenVas scan to all TCP/UDP ports on 192.58.41.108

2.4 Report – Service Enumeration

By using Nmap we can scan target's open ports and services.

Open Ports			
Host	Port	Protocol	Usage
192.58.41.108	443	TCP	HTTPS
192.58.41.108	1723	TCP	PPTP
192.58.41.108	3389	TCP	RDP

2.5 Test from External network

First network security and penetration test was from public network. From external network first, we used NMAP to evaluate open ports on the network. Nmap shows that there were three TCP ports open 443, 1723 and 3389(Figure 1 Open ports). The Nmap commands are on the attachments below.

Open Ports			
Host	Port	Protocol	Usage
192.58.41.108	443	TCP	HTTPS
192.58.41.108	1723	TCP	PPTP
192.58.41.108	3389	TCP	RDP

Figure 1 Open ports

The HTTPS protocol secures HTTP traffic over SSL (Secure Socket Layer). PPTP protocol creates VPN connection between point-to-point hosts. RDP protocol creates Remote Desktop connection to machine.

For obtaining more information from the network, we run OpenVAS vulnerability scanner. The OpenVAS output shows multiple high/critical vulnerabilities from the network.

Known vulnerabilities from OpenVAS Scanner					
Vulnerability	Severity		Host	Location	Created
Lighthttpd Server Detection	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
Traceroute	0.0	log	194.58.41.108	general/TCP	Thu Oct 12 09:53:30 2017
TCP Timestamps	2.6	low	194.58.41.108	general/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Report Supported Cipher Suites	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
Lighthttpd Multiple vulnerabilities	7.5	high	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: SSLv3 Protocol CBC Cipher Suites information Disclosure vulnerability (POODLE)	4.3	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
Pfsense Remote Version Detection	0.0.	log	194.58.41.108	general/TCP	Thu Oct 12 09:53:30 2017
CPE inventory	0.0	log	194.58.41.108	general/CPE-T	Thu Oct 12 09:53:30 2017
SSL/TLS: Missing "secure" Cookie Attribute	6.4	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Report Medium Cipher Suites	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities	9.3	high	194.58.41.108	3389/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: HTTP Strict Transport Security (HSTS) Missing	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
Missing "httpOnly" Cookie Attribute	5.0	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
OS Detection Consolidation and Reporting	0.0	log	194.58.41.108	general/TCP	Thu Oct 12 09:53:30 2017
PPTP Detection and versioning	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strenght Vulnerability	4.0	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS Hostaname discovery fro server certificate	0.0	log	194.58.41.108	general/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
CGI Scanning Consolidation	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
HTTP Server type and version	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
DIRB (NASL wrapper)	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Certificate - Self-signed Certificate detection	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
Services	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
Services	0.0	log	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Report Weak Cipher Suites	4.3	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Report Non Weak Cipher Suites	0.0		194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Collect and Report Certificate details	0.0		194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: OpenSSL TLS "heartbeat" Extension Information Disclosure Vulnerability	5.0	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017

From the OpenVAS report we only look into those CVEs which are over medium. The report lists that we have 10 vulnerabilities and two of them are high priority.

Vulnerabilities over medium					
Lighthttpd Multiple vulnerabilities	7.5	high	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities	9.3	high	194.58.41.108	3389/TCP	Thu Oct 12 09:53:30 2017
Missing "httpOnly" Cookie Attribute	5.0	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strenght Vulnerability	4.0	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Missing "secure" Cookie Attribute	6.4	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: OpenSSL TLS "heartbeat" Extension Information Disclosure Vulnerability	5.0	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: Report Weak Cipher Suites	4.3	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017
SSL/TLS: SSLv3 Protocol CBC Cipher Suites information Disclosure vulnerability (POODLE)	4.3	medium	194.58.41.108	443/TCP	Thu Oct 12 09:53:30 2017

2.6 KIPITO data security testing - EXTERNAL Vulnerability Summary

2.6.1 **Microsoft Remote Desktop Protocol 2671387**

Synopsis: Attacker can hijack RD computer and access everything with full rights

Vulnerable Targets: 192.58.41.108 tcp/3389(RDP)

Vulnerability Explanation: Attacker can craft specially crafted RD packets, which will allow attacker to access of an object in memory that has not been properly initialized or been deleted. If the attack is successful, attacker can cause RDP to not respond, or take complete control of the system. Where he could install programs, change, delete or view data and create new users with full user rights.

Vulnerability Fix: Microsoft has issued a patch to fix the RD packet injection, it can be obtained by Microsofts Security Update. The patch can be found Start > Control Panel > Update&Security

Severity: HIGH

Reference: CVE-2012-0002

CVSS Base Score: 9.3

Proof of Concept Code Here

Screenshot Here:

Vulnerability	Severity	QoD	Host	Location	Created
Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)	9.3 (High)	99%	192.58.41.108	3389/tcp	Thu Oct 12 10:01:36 2017

√Apply to page contents

(Applied filter: first=31 rows=10 apply_overrides=0 min_qod=70 severity>Error and task_id=1d53a2f5-0684-4d65-bbab-cad96cf64d45 sort=nvt)

31 - 31 of 31

2.6.2 Lighttpd

Synopsis: SQL injection vulnerability in mod_mysql_vhost.c in lighttpd before 1.4.35 allows remote attackers to execute arbitrary SQL commands via the host name, related to request_check_hostname.

Vulnerable Targets: 192.58.41.108 tcp/443

Vulnerability Explanation: Lighttpd is prone to an SQL-injection vulnerability because it fails to sufficiently sanitize user-supplied input before using it in an SQL query.

Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Versions prior to lighttpd 1.4.35 are vulnerable.

Vulnerability Fix: The vulnerability can be fixed by updating lighttpd version to latest available version.

Severity: HIGH

Reference: CVE-2014-2323

CVSS Base Score: 7.5

Proof of Concept Code Here

Screenshot Here:

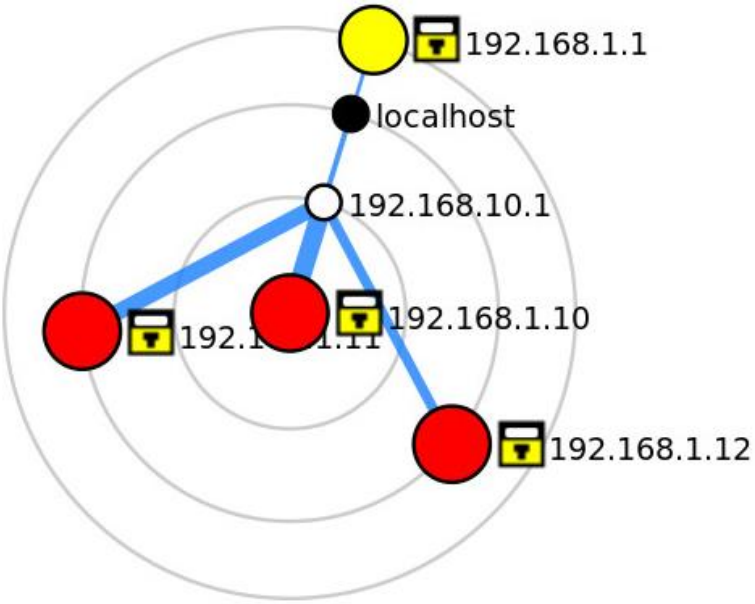
Vulnerability	Severity	QoD	Host	Location	Created
Lighttpd Server Detection	0.0 (Log)	80%	192.58.41.108	443/tcp	Thu Oct 12 09:53:30 2017
Traceroute	0.0 (Log)	80%	192.58.41.108	general/tcp	Thu Oct 12 09:50:29 2017
TCP timestamps	2.6 (Low)	80%	192.58.41.108	general/tcp	Thu Oct 12 10:01:35 2017
SSL/TLS: Report Supported Cipher Suites	0.0 (Log)	98%	192.58.41.108	443/tcp	Thu Oct 12 09:54:22 2017
Lighttpd Multiple vulnerabilities	7.5 (High)	99%	192.58.41.108	443/tcp	Thu Oct 12 10:07:15 2017

2.7 Test From internal network

The internal network security tests done behind consult connection were from 192.168.10.0/24 network. There was two LAN-subnets in our scope,192.168.1.0/24 and 192.158.2.0/24

As usual test began with Nmapping the networks. Both networks that we scanned were separate scans. Then we scanned each found ip address with nmap -A to see which services were used, open ports and operating systems.

Host	OS	Hostname
192.168.1.1	PFSENSE	GW.KIPITO.FI
192.168.1.10	Windows 7	W7-POMO
192.168.1.11	Windows 7	
192.168.1.12	Windows Server 2008 SP1	W7-BERTTA
192.168.2.1	PFSENSE	GW.KIPITO.FI
192.168.2.10	Windows Server 2008 SP1	DC
192.168.2.20	Windows Server 2008 SP1	FILES



2.8 Separate host scan 192.168.1.10

Vulnerabilities	Severity	Host	Location
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote(4013389)	9.3 High	192.168.1.10	445/TCP
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 Medium	192.168.1.10	135/TCP
SSL/TLS: Report Weak Cipher Suites	4.3 Medium	192.168.1.10	3389/TCP
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 Medium	192.168.1.10	3389/TCP

2.9 Separate host scan 192.168.1.11

Vulnerability	Severity	Host	Location
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote(4013389)	9.3 High	192.168.1.11	445/TCP
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 Medium	192.168.1.11	135/TCP
SSL/TLS: Report Weak Cipher Suites	4.3 Medium	192.168.1.11	3389/TCP
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 Medium	192.168.1.11	3389/TCP
TCP Timestamps	2.6 Low	192.168.1.11	general/TCP

2.10 Separate host scan 192.168.1.12

Vulnerabilities	Severity	Host	Location
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote(4013389)	9.3 High	192.168.1.12	445/TCP
TCP timestamps	2.6 Low	192.168.1.12	135/TCP

2.11 Separate host scan 192.168.2.10

Vulnerability	Severity	Host	Location
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote(4013389)	9.3 High	192.168.2.10	445/TCP
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 Medium	192.168.2.10	135/TCP
Use LDAP search request to retrieve information from NT Directory services	5.0 Medium	192.168.2.10	3268/TCP
Use LDAP search request to retrieve information from NT Directory services	5.0 Medium	192.168.2.10	389/TCP
TCP timstamps	2.6 Low	192.168.2.10	general/TCP

2.12 Separate host scan 192.168.2.20

Vulnerability	Severity	Host	Location
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote(4013389)	9.3 High	192.168.2.20	445/TCP
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 Medium	192.168.2.20	135/TCP
SSL/TLS: Report Weak Cipher Suites	4.3 Medium	192.168.2.20	3389/TCP
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 Medium	192.168.2.20	3389/TCP
TCP timestamps	2.6 Low	192.168.2.20	general/TCP

2.13 KIPITO data security testing - INTERNAL Vulnerability Summary

2.13.1 Microsoft Windows SMB Server Multiple Vulnerabilities-Remote(4013389)

Synopsis:

Vulnerable Targets: 192.168.1.10, 192.168.1.11, 192.168.1.12, 192.168.2.10, 192.168.2.20

Vulnerability Explanation: Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)
Vulnerability Fix: These can be fixed by updating your systems to latest available.

Severity: HIGH

Reference: (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148, CVE-2017-0147)

CVSS Base Score: 9.3

Proof of Concept Code Here

2.13.2 DCE/RPC and MSRPC Services Enumeration Reporting

Synopsis:

Vulnerable Targets: 192.168.1.11, 192.168.2.10, 192.168.2.20, 192.168.10

Vulnerability Explanation: Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRP services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about remote host.
Vulnerability Fix: Filter incoming traffic to this port

Severity: MEDIUM

Reference:

CVSS Base Score: 5.0

Proof of Concept Code Here

2.13.3 SSL/TLS: Report Weak Cipher Suites

Synopsis:

Vulnerable Targets: 192.168.1.11, 192.168.2.10, 192.168.2.20, 192.168.10

Vulnerability Explanation: This routine reports all Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Fix:

The configuration of this service should be changed so that it does not accept the listen weak cipher suites anymore. Please see the references for more resources supporting you with this task.

Severity: MEDIUM

Reference: CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000

Vulnerability Insight: These rules are applied for the evaluation of the cryptographic strength:

- RC4 is considered to be weak (CVE-2013-2556, CVE-2015-2808).
- Ciphers using 64bit or less are considered to be vulnerable to brute force methods and therefore considered weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the 10 years us conserved medium.
- Any Other cipher is considered as strong.

CVSS Base Score: 4.3

Proof of Concept Code Here

Screenshot here:

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.1.11	445/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.1.11	135/tcp	
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.168.1.11	3389/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%	192.168.1.11	3389/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.1.11	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70) 1 - 5 of 5

2.13.4 Use LDAP search request to retvieve information from NT Directory services

Synopsis:

Vulnerable Targets: 192.168.2.10

Vulnerability Explanation: It is possible to disclosure LDAP information. The directory base of the remote server is set to NULL. This allows information to be enumerated without any prior knownledge of the directory structure.

Vulnerability Fix: **Workaround:** If pre windows 2000 compatibility is not required, remove pre-windows 2000 compatibility as follows: -start cmd.exe, -execute the command: net localgroup “Pre-windows 2000 compatible Access” everyone/delete. –restart the remote host.

Severity: MEDIUM

Reference:

CVSS Base Score: 5.0

Proof of Concept Code Here

Screenshot here:

Vulnerability	Severity	QoD	Host	Location	Actions
Use LDAP search request to retrieve information from NT Directory Services	5.0 (Medium)	99%	192.168.2.10	389/tcp	

Summary
It is possible to disclose LDAP information.

Description :

The directory base of the remote server is set to NULL. This allows information to be enumerated without any prior knowledge of the directory structure.

Vulnerability Detection Result

The following information was pulled from the server via a LDAP request:
NTDS Settings,CN=DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=kipito,DC=fi

Solution
Solution type: Workaround

If pre-Windows 2000 compatibility is not required, remove pre-Windows 2000 compatibility as follows :

- start cmd.exe

- execute the command : net localgroup 'Pre-Windows 2000 Compatible Access' everyone /delete

- restart the remote host

Vulnerability Detection Method
Details: Use LDAP search request to retrieve information from NT Directory Services (OID: 1.3.6.1.4.1.25623.1.0.12105)

Version used: $Revision: 5190 $

2.13.5 SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Synopsis:

Vulnerable Targets: 192.168.1.10, 192.168.1.11, 192.168.2.20

Vulnerability Explanation: The remote service is using a SSL/TLS certificate chain that has been signed using a cryptographically weak hashing algorithm.
Vulnerability Insight: Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not secure enough for ongoing use. Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visit web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates
Vulnerability Fix: Servers that use SSL/TLS certificates signed using an SHA-1 signature will need to obtain new SHA-2 signed SSL/TLS certificates to avoid these web browser SSL/TLS certificate warnings.

Severity: MEDIUM

Reference:

CVSS Base Score: 4.0

Proof of Concept Code Here

Screenshot here:

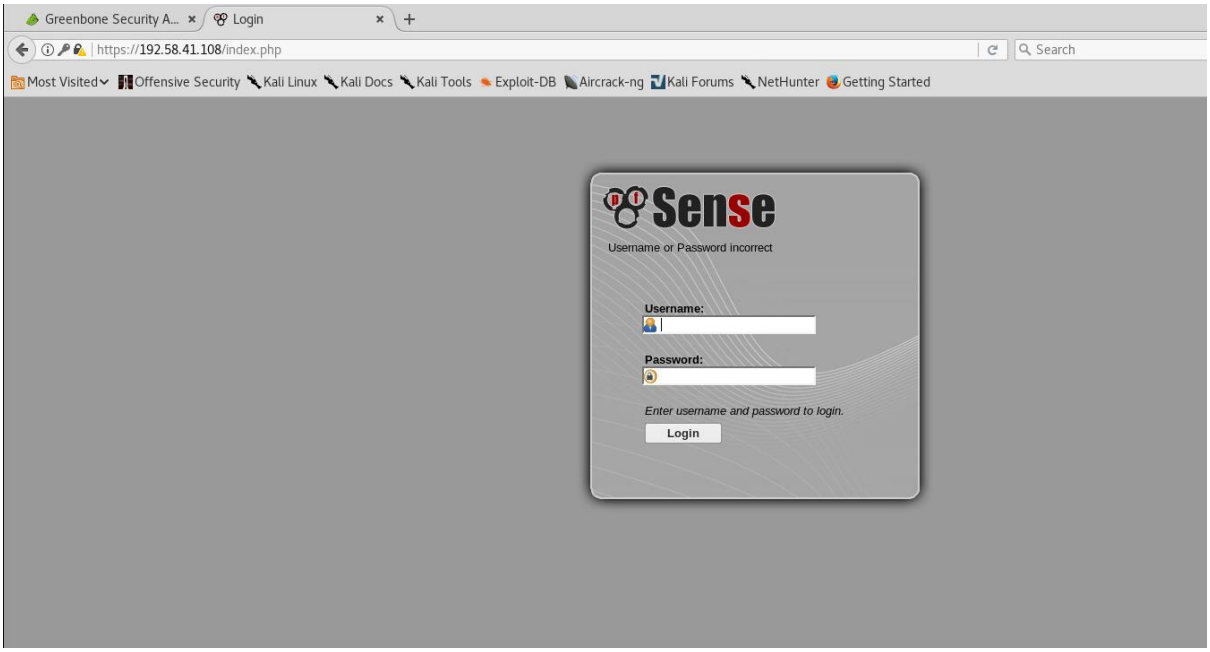
Vulnerability		Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)		9.3 (High)	95%	192.168.1.11	445/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	192.168.1.11	135/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	192.168.1.11	3389/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80%	192.168.1.11	3389/tcp	
TCP timestamps		2.6 (Low)	80%	192.168.1.11	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70) 1 - 5 of 5

3. KIPITO data security testing - External Attachments

The attached some screenshot to prove our findings from the tools.

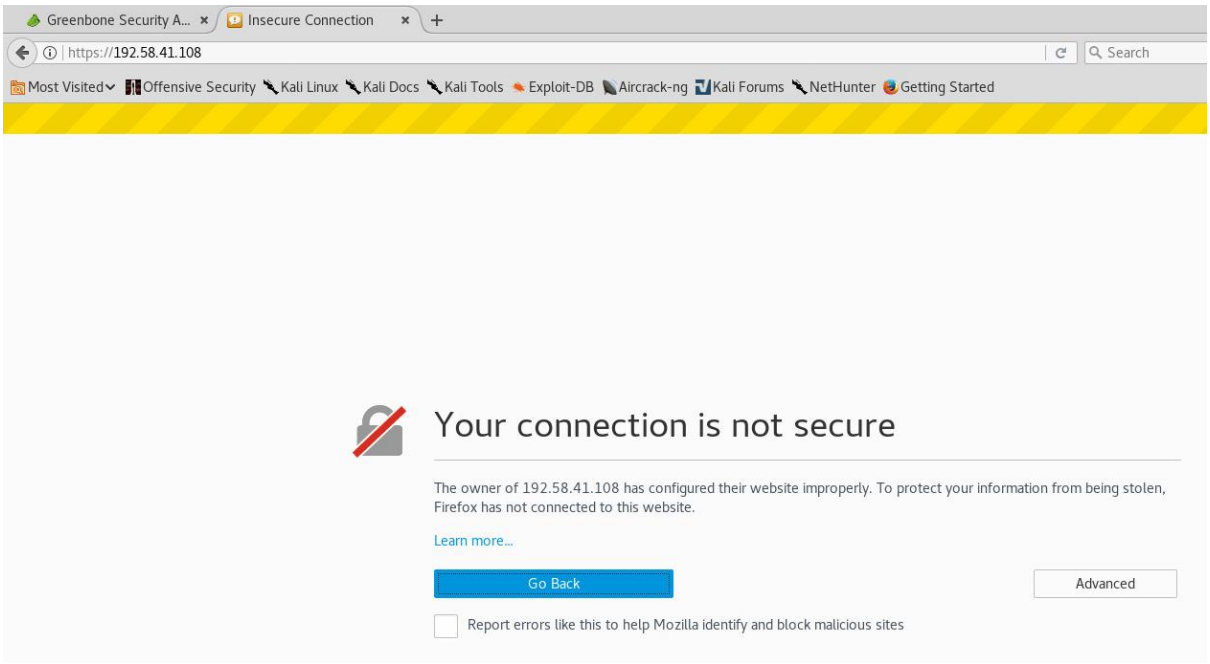
From the External network we can see the pfsense firewall login screen when typing IP-address of the host to the browser.

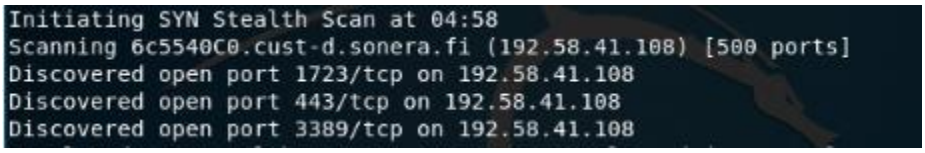


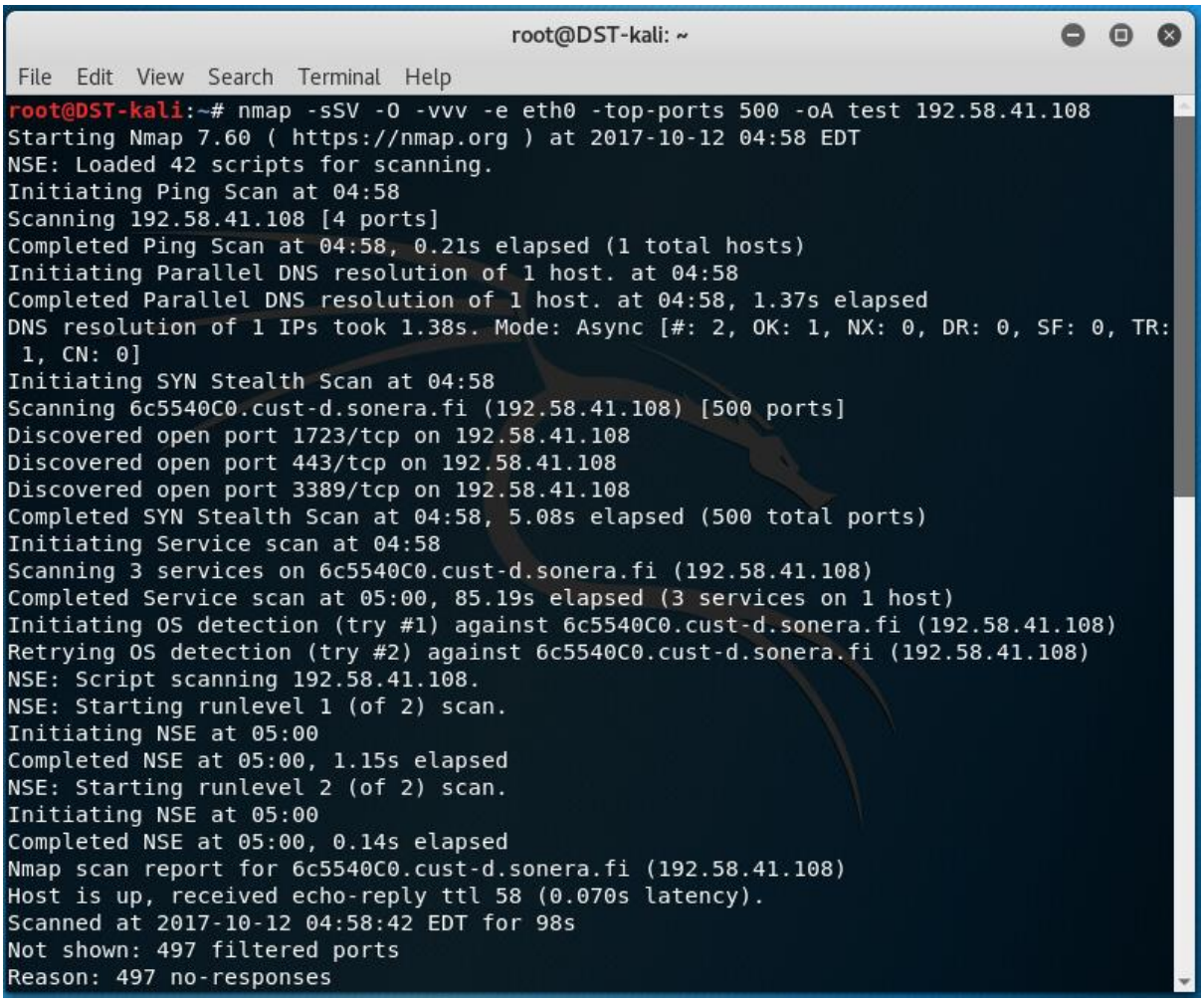
Pfsense login does not have valid SSL certificate. The login screen should not be seen from External network.

jamk.fi

Report
2.11.2017





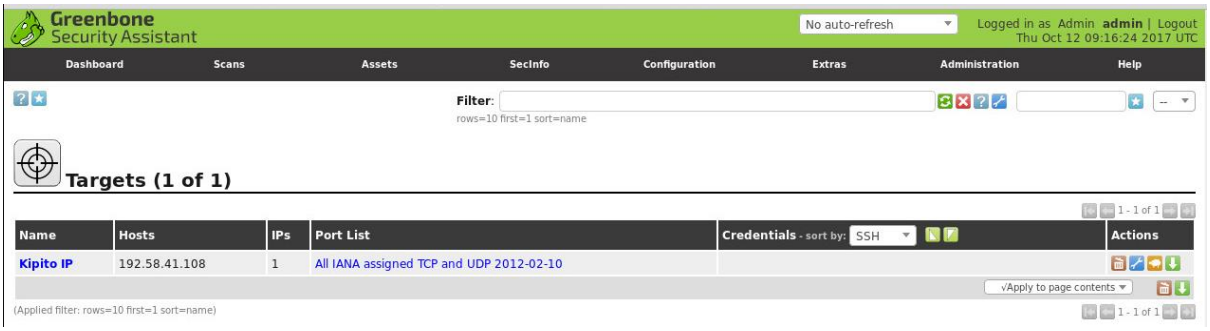


With NMAP tool we can see the open TCP/UDP ports on the interface.

```
root@DST-kali: ~
File  Edit  View  Search  Terminal  Help
Scanned at 2017-10-12 04:58:42 EDT for 98s
Not shown: 497 filtered ports
Reason: 497 no-responses
PORT     STATE SERVICE        REASON          VERSION
443/tcp  open  ssl/http       syn-ack ttl 58  lighttpd 1.4.32
1723/tcp open  pptp           syn-ack ttl 58  FreeBSD MPD (Firmware: 257)
3389/tcp open  ms-wbt-server? syn-ack ttl 121
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
Device type: general purpose|WAP
Running (JUST GUESSING): Linux 2.6.X (97%), D-Link embedded (96%), TRENDnet embedded (96%
)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:dlink:dwl-624%2b cpe:/h:dlink:dwl-2000ap cpe
:/h:trendnet:tew-432brp
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (97%), D-Link DWL-624+ or DWL-2000AP, or TRE
NDnet TEW-432BRP WAP (96%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.60%E=4%D=10/12%OT=443%CT=%CU=%PV=N%G=N%TM=59DF2F24%P=x86_64-pc-linux-gnu)
SEQ(SP=FB%GCD=2%ISR=10C%TI=RD%TS=21)
OPS(O1=M5B4NW7ST11%O2=M578NW7ST11%O3=M280NW7NNT11%O4=M5B4NW7ST11%O5=M218NW7ST11%O6=M109ST
11)
WIN(W1=FECC%W2=FECC%W3=FECC%W4=FECC%W5=FECC%W6=FECC)
ECN(R=Y%DF=N%TG=40%W=FECC%O=M5B4NW7SLL%CC=N%Q=)
ECN(R=N)
T1(R=Y%DF=N%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)

Uptime guess: 0.000 days (since Thu Oct 12 05:00:17 2017)
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: Host: gw.kipito.fi
```

```
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.34 seconds
           Raw packets sent: 1106 (53.688KB) | Rcvd: 40 (2.954KB)
```

Here is screenshot form OpenVAS scan settings.



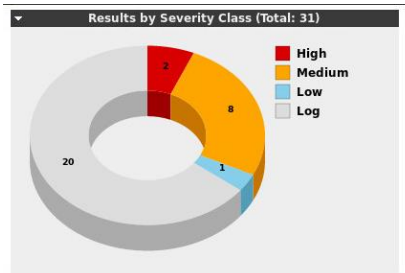
jamk.fi

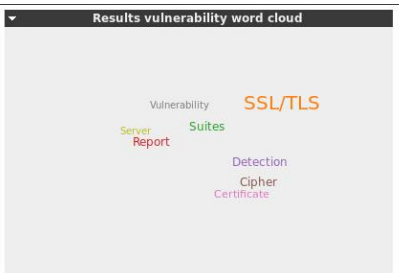
Report
2.11.2017

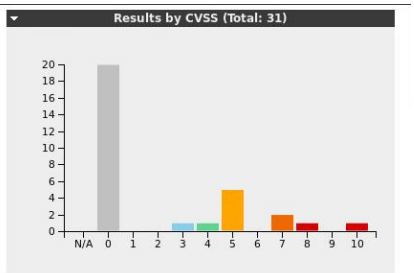
Task: Scan for kipito

Name:	**Scan for kipito**
Comment:	
Target:	Kipito IP
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes
	Apply Overrides: yes
	Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner)
	Scan Config: Full and fast
	Order for target hosts: Sequential
	Network Source Interface:
	Maximum concurrently executed NVTs per host: 4
	Maximum concurrently scanned hosts: 20
Status:	Done
Duration of last scan:	45 minutes 11 seconds
Average scan duration:	22 minutes 53 seconds
Reports:	2 (Finished: 2, Last: Oct 12 2017)
Results:	30
Notes:	0
Overrides:	0

Here we have the OpenVAS scanning result and founded vulnerabilities.







1 - 10 of 31

Vulnerability	Severity	QoD	Host	Location	Created
HTTP Server type and version	0.0 (Log)	80%	192.58.41.108	443/tcp	Thu Oct 12 09:52:12 2017
DIRB (NASL wrapper)	0.0 (Log)	80%	192.58.41.108	443/tcp	Thu Oct 12 10:00:23 2017
SSL/TLS: Certificate - Self-Signed Certificate Detection	0.0 (Log)	98%	192.58.41.108	443/tcp	Thu Oct 12 09:58:41 2017
SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN	0.0 (Log)	98%	192.58.41.108	443/tcp	Thu Oct 12 09:59:20 2017
Services	0.0 (Log)	80%	192.58.41.108	443/tcp	Thu Oct 12 09:50:15 2017
Services	0.0 (Log)	80%	192.58.41.108	443/tcp	Thu Oct 12 09:50:23 2017
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.58.41.108	443/tcp	Thu Oct 12 10:01:33 2017
SSL/TLS: Report Non Weak Cipher Suites	0.0 (Log)	98%	192.58.41.108	443/tcp	Thu Oct 12 09:51:54 2017
SSL/TLS: Collect and Report Certificate Details	0.0 (Log)	98%	192.58.41.108	443/tcp	Thu Oct 12 09:51:11 2017
SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability	5.0 (Medium)	99%	192.58.41.108	443/tcp	Thu Oct 12 10:09:29 2017

jamk.fi

Report
2.11.2017

KIPITO had one vulnerability ranked as “HIGH” which should be taken control immediately.

Vulnerability	Severity	QoD	Host	Location	Created
Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)	9.3 (High)	99%	192.58.41.108	3389/tcp	Thu Oct 12 10:01:36 2017

√Apply to page contents

(Applied filter: first=31 rows=10 apply_overrides=0 min_qod=70 severity>Error and task_id=1d53a2f5-0684-4d65-bbab-cad96cf64d45 sort=nvt)

31 - 31 of 31

Vulnerability	Severity	QoD	Host	Location	Created
SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites	0.0 (Log)	98%	192.58.41.108	443/tcp	Thu Oct 12 10:00:13 2017
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Medium)	70%	192.58.41.108	443/tcp	Thu Oct 12 10:02:44 2017
SSL/TLS: HTTP Strict Transport Security (HSTS) Missing	0.0 (Log)	80%	192.58.41.108	443/tcp	Thu Oct 12 10:00:22 2017
Missing `httpOnly` Cookie Attribute	5.0 (Medium)	80%	192.58.41.108	443/tcp	Thu Oct 12 09:59:18 2017
OS Detection Consolidation and Reporting	0.0 (Log)	80%	192.58.41.108	general/tcp	Thu Oct 12 09:52:39 2017
PPTP detection and versioning	0.0 (Log)	80%	192.58.41.108	1723/tcp	Thu Oct 12 09:57:39 2017
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80%	192.58.41.108	443/tcp	Thu Oct 12 10:00:39 2017
SSL/TLS: Hostname discovery from server certificate	0.0 (Log)	98%	192.58.41.108	general/tcp	Thu Oct 12 09:51:12 2017
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	192.58.41.108	443/tcp	Thu Oct 12 09:58:33 2017
CGI Scanning Consolidation	0.0 (Log)	80%	192.58.41.108	443/tcp	Thu Oct 12 10:01:48 2017

√Apply to page contents

(Applied filter: first=11 rows=10 apply_overrides=0 min_qod=70 severity>Error and task_id=1d53a2f5-0684-4d65-bbab-cad96cf64d45 sort=nvt)

11 - 20 of 31

Vulnerability	Severity	QoD	Host	Location	Created
Lighttpd Server Detection	0.0 (Log)	80%	192.58.41.108	443/tcp	Thu Oct 12 09:53:30 2017
Traceroute	0.0 (Log)	80%	192.58.41.108	general/tcp	Thu Oct 12 09:50:29 2017
TCP timestamps	2.6 (Low)	80%	192.58.41.108	general/tcp	Thu Oct 12 10:01:35 2017
SSL/TLS: Report Supported Cipher Suites	0.0 (Log)	98%	192.58.41.108	443/tcp	Thu Oct 12 09:54:22 2017
Lighttpd Multiple vulnerabilities	7.5 (High)	99%	192.58.41.108	443/tcp	Thu Oct 12 10:07:15 2017
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	192.58.41.108	443/tcp	Thu Oct 12 09:57:23 2017
Pfsense Remote Version Detection	0.0 (Log)	80%	192.58.41.108	general/tcp	Thu Oct 12 10:01:31 2017
CPE Inventory	0.0 (Log)	80%	192.58.41.108	general/CPE-T	Thu Oct 12 10:13:55 2017
SSL/TLS: Missing `secure` Cookie Attribute	6.4 (Medium)	99%	192.58.41.108	443/tcp	Thu Oct 12 10:01:33 2017
SSL/TLS: Report Medium Cipher Suites	0.0 (Log)	98%	192.58.41.108	443/tcp	Thu Oct 12 09:58:25 2017

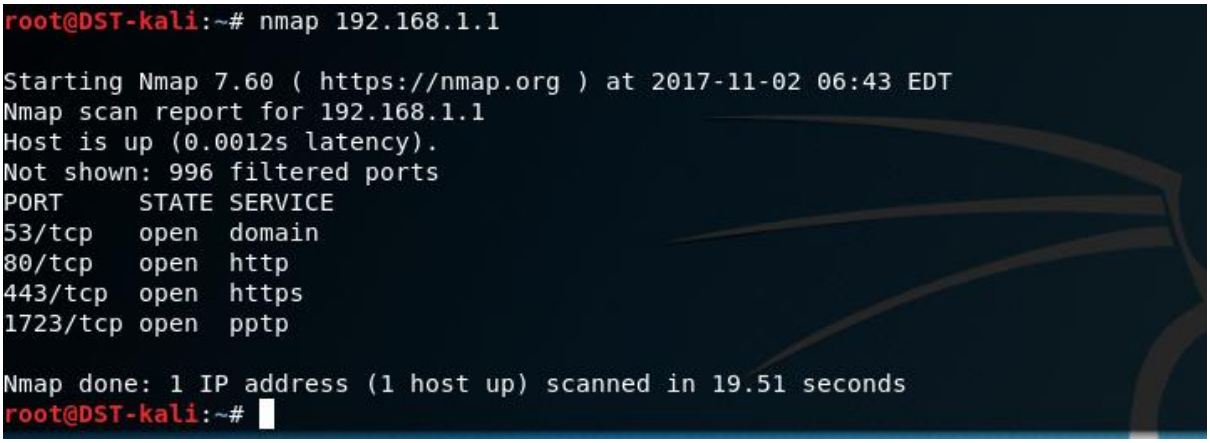
√Apply to page contents

(Applied filter: first=21 rows=10 apply_overrides=0 min_qod=70 severity>Error and task_id=1d53a2f5-0684-4d65-bbab-cad96cf64d45 sort=nvt)

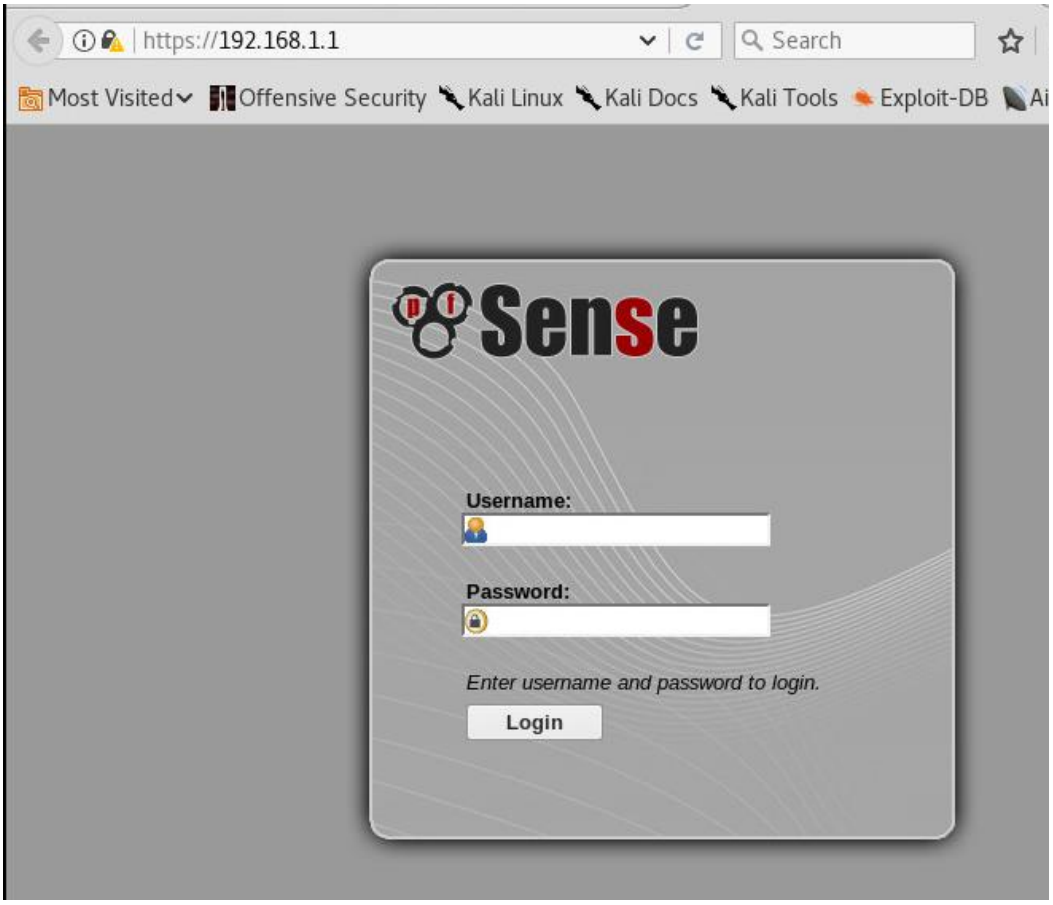
21 - 30 of 31

4. KIPITO - Internal Attachments

The Basic port enumerations were done with NMAP. We saw 3 open ports in the host 192.168.1.1 which is the firewall LAN interface.



192.168.1.0/24




```
root@DST-kali:~# nmap -A -sV 192.168.1.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-02 06:47 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00032s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   dnsmasq 2.66
| dns-nsid:
|_  bind.version: dnsmasq-2.66
80/tcp   open  http     lighttpd 1.4.32
|_http-server-header: lighttpd/1.4.32
|_http-title: Did not follow redirect to https://192.168.1.1/
443/tcp  open  ssl/http lighttpd 1.4.32
|_http-server-header: lighttpd/1.4.32
| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=Com
panyName/stateOrProvinceName=Somewhere/countryName=US
| Not valid before: 2014-01-21T18:09:48
|_Not valid after:  2019-07-14T18:09:48
|_ssl-date: 2017-11-02T10:50:24+00:00; -1s from scanner time.
1723/tcp open  pptp     FreeBSD MPD (Firmware: 257)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): OpenBSD 4.X (93%), Comau embedded (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: OpenBSD 4.0 (93%), Comau C4G robot control unit (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: gw.kipito.fi

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
```

```
TRACEROUTE (using port 1723/tcp)
HOP RTT     ADDRESS
1   0.32 ms 192.168.1.1

Nmap scan report for 192.168.1.10
Host is up (0.0069s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional N 7601 Service Pack 1 micros
oft-ds (workgroup: WORKGROUP)
3389/tcp  open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008
OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows Server 2008 SP1
Network Distance: 2 hops
Service Info: Host: W7-POMO; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: W7-POMO, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:
01:08:46 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional N 7601 Service Pack 1 (Windows 7 Professional N 6
.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: W7-POMO
```

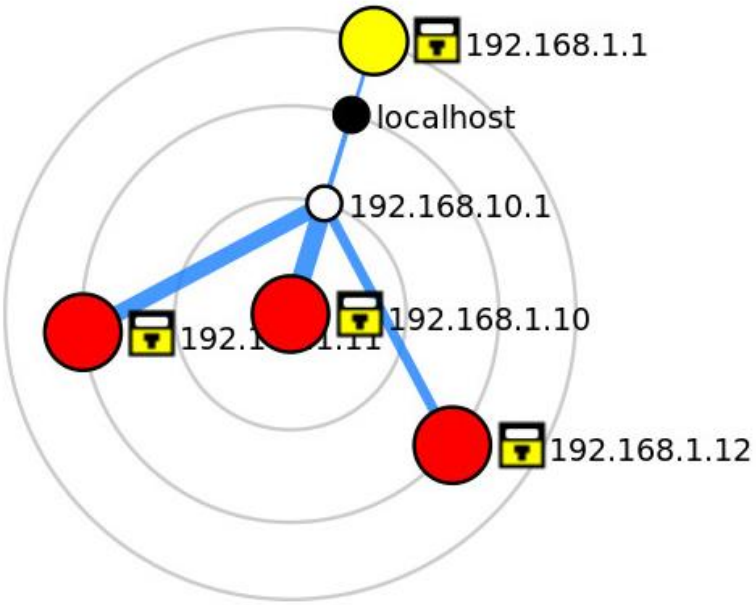
```
|   NetBIOS computer name: W7-POMO\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2017-11-02T12:50:19+02:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2017-11-02 06:50:24
|_  start_date: 2016-03-29 00:47:41

TRACEROUTE (using port 445/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 192.168.1.11
2   0.75 ms 192.168.1.10

Nmap scan report for 192.168.1.11
Host is up (0.0075s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional N 7601 Service Pack 1 micros
oft-ds (workgroup: KIPITO)
3389/tcp  open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
```

```
TRACEROUTE (using port 445/tcp)
HOP RTT     ADDRESS
1   0.44 ms 192.168.10.1
2   0.55 ms 192.168.1.11

Nmap scan report for 192.168.1.12
Host is up (0.0044s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional N 7601 Service Pack 1 micros
oft-ds (workgroup: KIPITO)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008
OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows Server 2008 SP1
Network Distance: 2 hops
Service Info: Host: W7-BERTTA; OS: Windows; CPE: cpe:/o:microsoft:windows
```

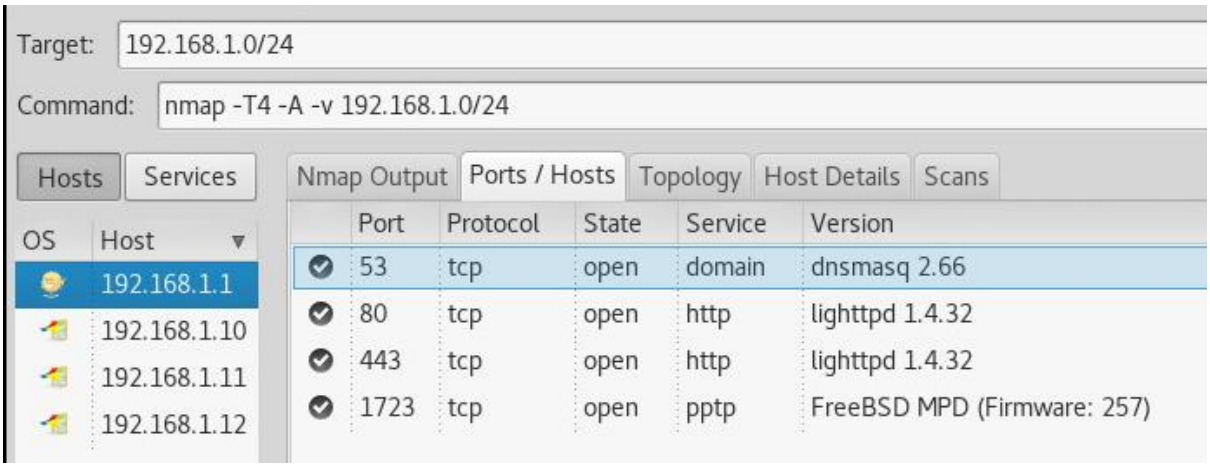
```
Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: W7-BERTTA, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:5
6:01:08:48 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional N 7601 Service Pack 1 (Windows 7 Professional N 6
.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: W7-BERTTA
|   NetBIOS computer name: W7-BERTTA\x00
|   Domain name: kipito.fi
|   Forest name: kipito.fi
|   FQDN: W7-BERTTA.kipito.fi
|_  System time: 2017-11-02T12:50:25+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2017-11-02 06:50:25
|_  start_date: 2016-03-29 00:47:26

TRACEROUTE (using port 445/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 192.168.1.11
2   0.66 ms 192.168.1.12
```

```
Post-scan script results:
| clock-skew:
|   -1s:
|     192.168.1.11
|     192.168.1.1
|     192.168.1.12
|_    192.168.1.10
OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 193.95 seconds
```

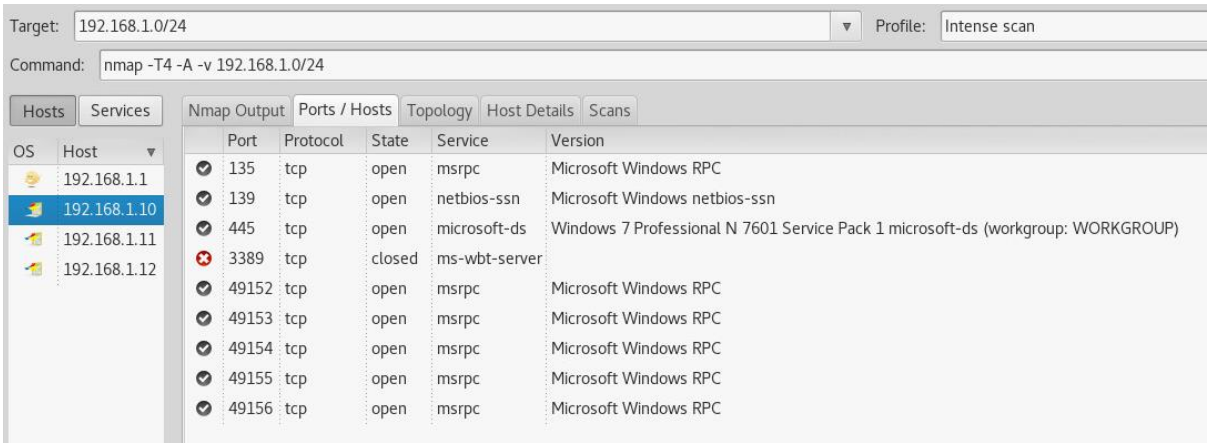
4 hosts



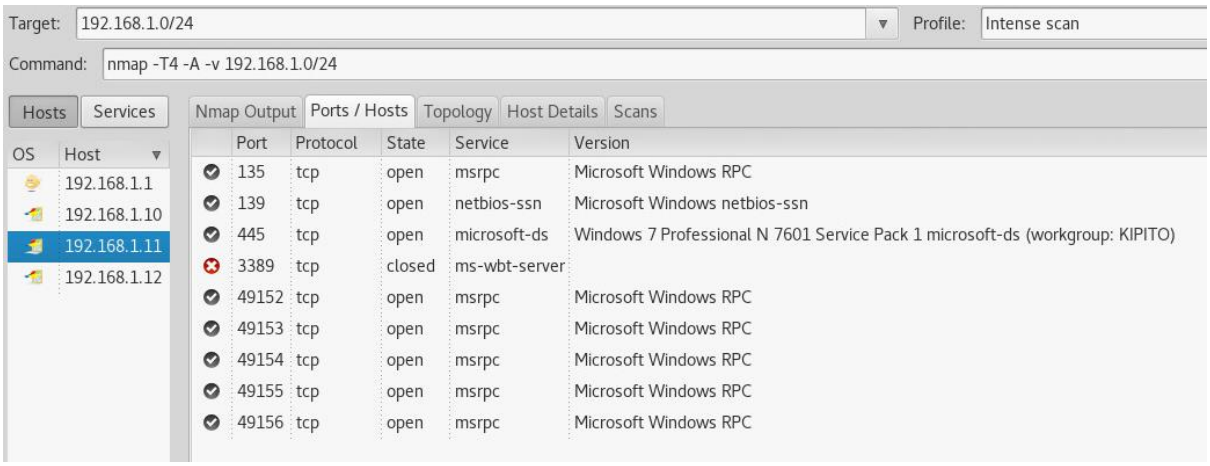
We scanned both internal networks separately with Zenmap. Zenmap shows that 4 host were found from the network 192.168.1.0/24. ZenMap shows the open ports and services from each host.



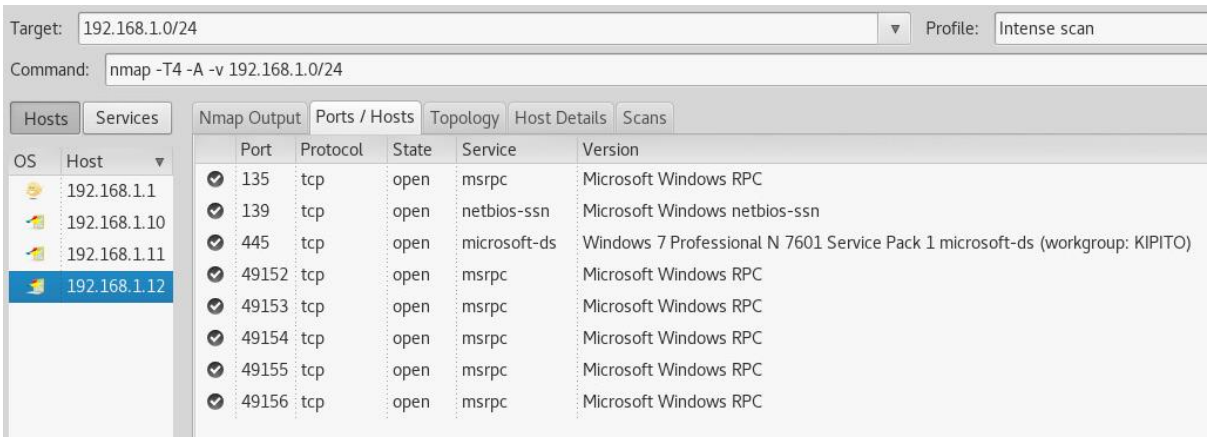
Host 192.168.1.10 open ports and services.



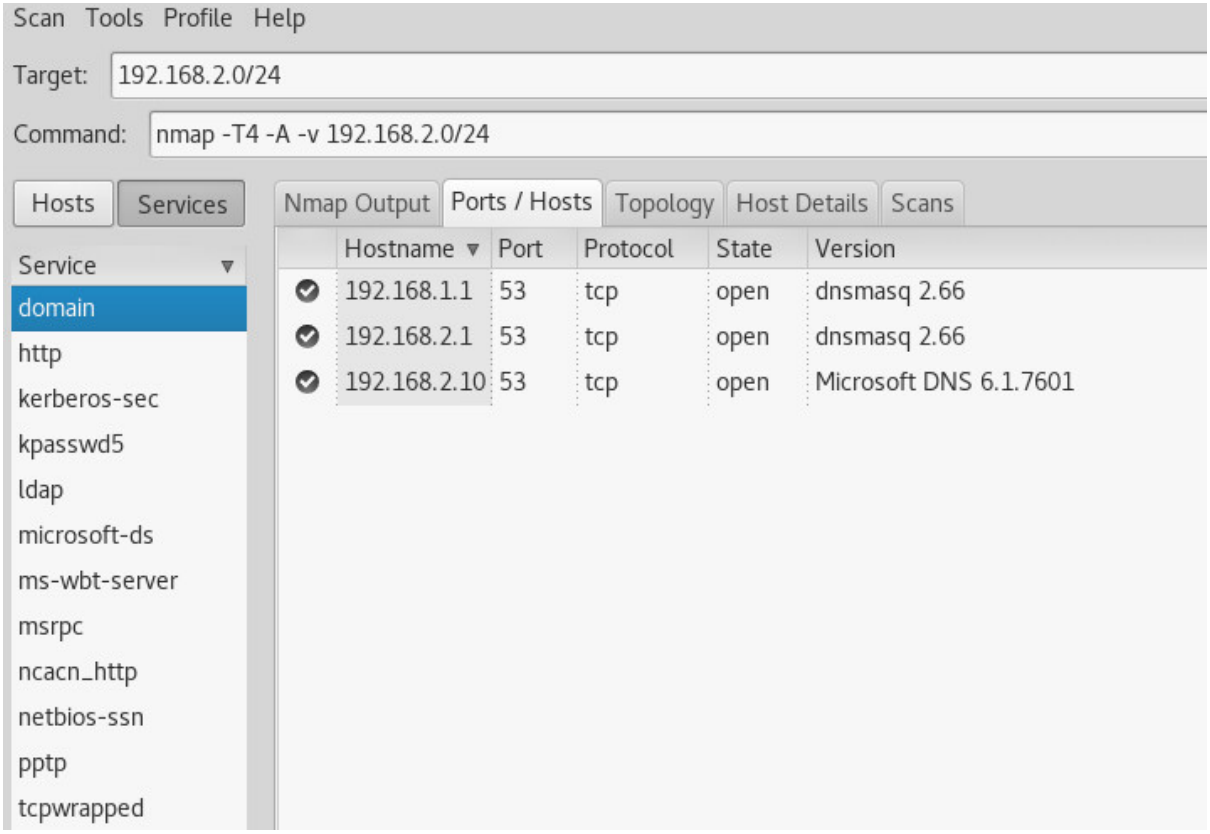
192.168.1.11 open ports and services.



192.168.1.12 open ports and services.



192.168.2.0/24



nmap -A -sV 192.168.2.0/24

```
root@DST-kali:~# nmap -A -sV 192.168.2.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-02 06:50 EDT
Nmap scan report for 192.168.2.1
Host is up (0.00047s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   dnsmasq 2.66
| dns-nsid:
|_  bind.version: dnsmasq-2.66
80/tcp   open  http     lighttpd 1.4.32
|_http-server-header: lighttpd/1.4.32
|_http-title: Did not follow redirect to https://192.168.2.1/
443/tcp  open  ssl/http lighttpd 1.4.32
|_http-server-header: lighttpd/1.4.32
|_http-title: Login
| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US
| Not valid before: 2014-01-21T18:09:48
|_Not valid after:  2019-07-14T18:09:48
|_ssl-date: 2017-11-02T10:52:33+00:00; -1s from scanner time.
1723/tcp open  pptp     FreeBSD MPD (Firmware: 257)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): OpenBSD 4.X (91%), Linux 2.6.X (89%), Comau embedded (86%)
OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:linux:linux_kernel:2.6.29
Aggressive OS guesses: OpenBSD 4.0 (91%), Linux 2.6.29 (89%), Comau C4G robot control unit (86%), OpenBSD 4.3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: gw.kipito.fi

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   0.34 ms 192.168.2.1

Nmap scan report for 192.168.2.10
Host is up (0.00097s latency).
Not shown: 981 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2017-11-02 10:51:29Z)
135/tcp   open  msrpc        Microsoft Windows RPC
```

2.10 kone

```
Nmap scan report for 192.168.2.10
Host is up (0.00097s latency).
Not shown: 981 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2017-11-02 10:51:29Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: kipito.fi, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (workgroup: KIPITO)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: kipito.fi, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49161/tcp open  msrpc        Microsoft Windows RPC
49165/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008
OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows Server 2008 SP1
Network Distance: 2 hops
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: DC, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:01:08:35 (VMware)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: dc
|   NetBIOS computer name: DC\x00
|   Domain name: kipito.fi
|   Forest name: kipito.fi
|   FQDN: dc.kipito.fi
|_  System time: 2017-11-02T12:52:33+02:00
| smb-security-mode:
|   account_used: guest
```

```
Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: DC, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:01:08:35 (VMware)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: dc
|   NetBIOS computer name: DC\x00
|   Domain name: kipito.fi
|   Forest name: kipito.fi
|   FQDN: dc.kipito.fi
|_  System time: 2017-11-02T12:52:33+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2017-11-02 06:52:33
|_  start_date: 2016-03-29 00:47:35

TRACEROUTE (using port 139/tcp)
HOP RTT     ADDRESS
1   0.46 ms 192.168.10.1
2   0.57 ms 192.168.2.10
```

2.20 machine

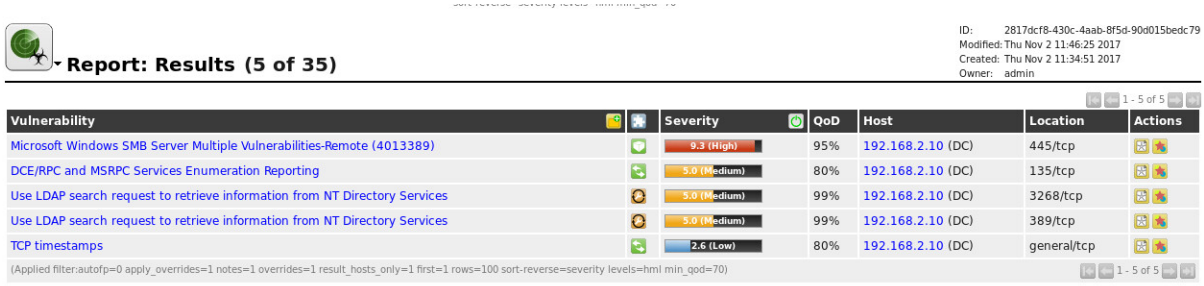
```
Nmap scan report for 192.168.2.20
Host is up (0.00087s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
3389/tcp  open  ms-wbt-server?
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008
OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows Server 2008 SP1
Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
|_nbstat: NetBIOS name: FILES, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:01:08:42 (VMware)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: files
|   NetBIOS computer name: FILES\x00
|   Domain name: kipito.fi
|   Forest name: kipito.fi
|   FQDN: files.kipito.fi
|_  System time: 2017-11-02T12:52:34+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2017-11-02 06:52:33
|_  start_date: 2016-03-29 00:47:24

TRACEROUTE (using port 139/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 192.168.2.10
2   0.89 ms 192.168.2.20

Post-scan script results:
| clock-skew:
|   -1s:
|     192.168.2.10
|_    192.168.2.1
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 163.74 seconds
root@DST-kali:~#
```

jamk.fi

Report
2.11.2017

scan results 192.168.2.10



Report: Results (5 of 35)

ID: 2817dcf8-430c-4aab-8f5d-90d015bedc79
Modified: Thu Nov 2 11:46:25 2017
Created: Thu Nov 2 11:34:51 2017
Owner: admin

1 - 5 of 5

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.2.10 (DC)	445/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.2.10 (DC)	135/tcp	
Use LDAP search request to retrieve information from NT Directory Services	5.0 (Medium)	99%	192.168.2.10 (DC)	3268/tcp	
Use LDAP search request to retrieve information from NT Directory Services	5.0 (Medium)	99%	192.168.2.10 (DC)	389/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.2.10 (DC)	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

1 - 5 of 5

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.2.10	445/tcp	

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Impact Level: System

Solution
Solution type: VendorFix

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS17-010

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

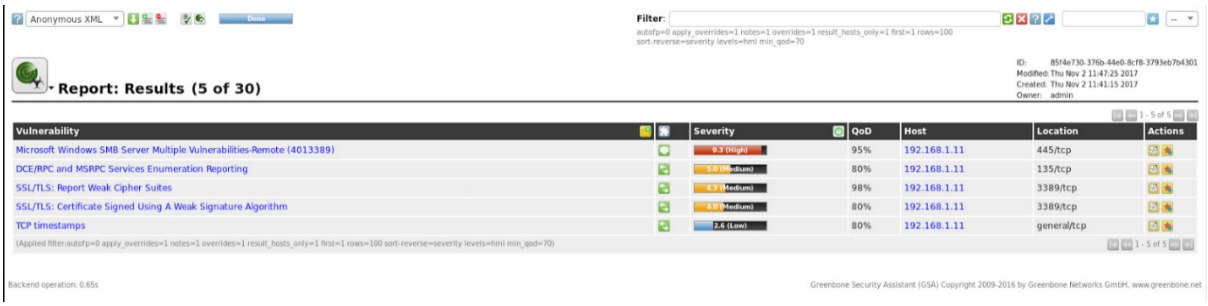
Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.

Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)

Version used: $Revision: 6223 $

192.168.1.11 Machine



Anonymous XML

Filter:

autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (5 of 30)

ID: 85f4e730-376b-44e0-8cf8-3793eb7b4301
Modified: Thu Nov 2 11:47:25 2017
Created: Thu Nov 2 11:41:15 2017
Owner: admin

1 - 5 of 5

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.1.11	445/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.1.11	135/tcp	
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.168.1.11	3389/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%	192.168.1.11	3389/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.1.11	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

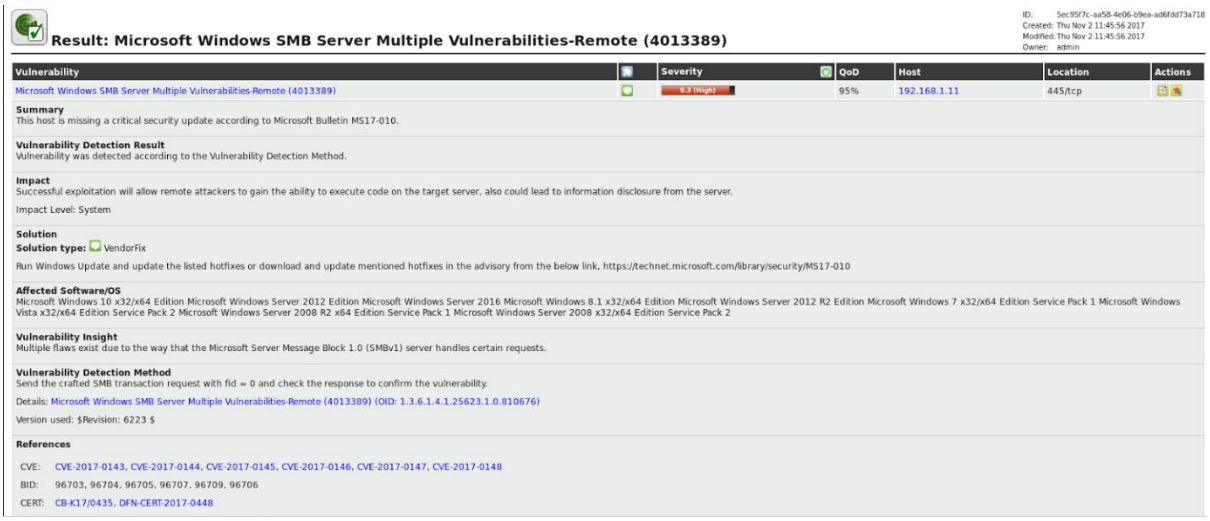
1 - 5 of 5

Backend operation: 0.65s

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

jamk.fi

Report
2.11.2017



Result: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

ID: 5ec95f7c-aa58-4e06-b9ea-ad6fdd73a718
Created: Thu Nov 2 11:45:56 2017
Modified: Thu Nov 2 11:45:56 2017
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.1.11	445/tcp	

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Impact Level: System

Solution
Solution type: VendorFix

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS17-010

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

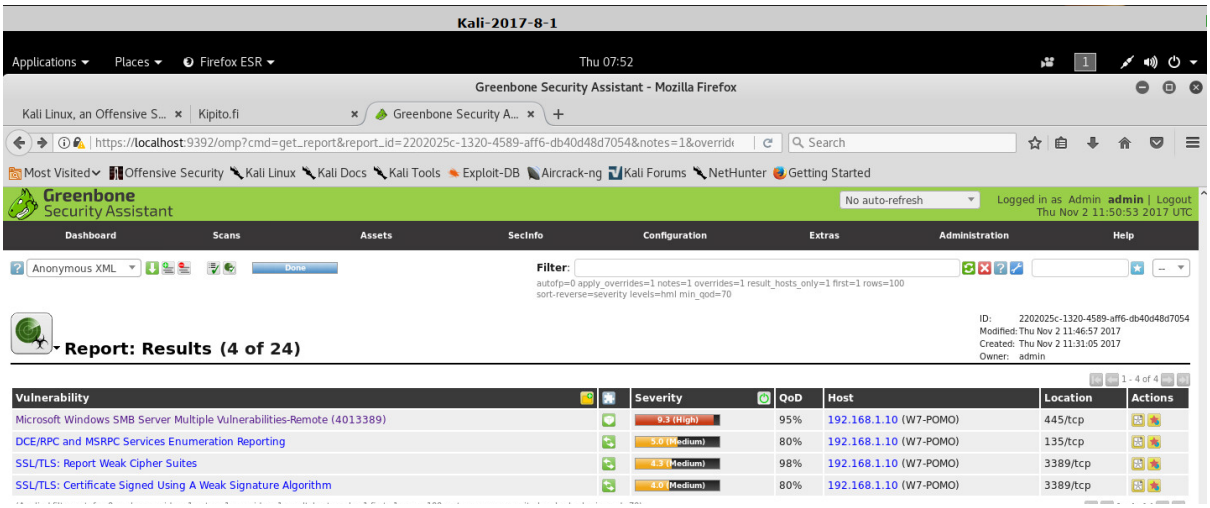
Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.

Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)

Version used: $Revision: 6223 $

References

CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148
BID: 96703, 96704, 96705, 96707, 96709, 96706
CERT: CB-K17/0435, DFN-CERT-2017-0448



scan for 192.168.1.12

1 - 2 of 2

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.1.12 (W7-BERTTA)	445/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.1.12 (W7-BERTTA)	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

1 - 2 of 2

scan for 192.168.2.20

1 - 5 of 5

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.2.20 (FILES)	445/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.2.20 (FILES)	135/tcp	
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.168.2.20 (FILES)	3389/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%	192.168.2.20 (FILES)	3389/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.2.20 (FILES)	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

1 - 5 of 5