

Data security testing

Lab 4: Configurations

Timo Lehosvuori, M3426@student.jamk.fi

Raportti

Data Security Testing, Markku Vajaranta

Syksy 2020

Tieto- ja viestintätekniikan koulutusohjelma

Tekniikan ja liikenteen ala

Sisällysluettelo

1	Benchmarks.....	2
1.1	Tehtävä 1	2
1.2	Windows	2
1.3	Linux.....	5
1.4	Tehtävä 2	7
1.5	Checklist.....	7
1.5.1	Kohta 1	7
1.5.2	Kohta 2	8
1.5.3	Kohta 3	10
1.5.4	Kohta 4	11
1.5.5	Kohta 5	11
1.5.6	Kohta 6	12
1.5.7	Kohta 7	12
1.5.8	Kohta 8	13
1.5.9	Kohta 9	13
1.5.10	Kohta 10	14
1.5.11	Kohta 11	15
1.5.12	Kohta 12	16
1.5.13	Kohta 13	17
1.5.14	Kohta 14	17
1.5.15	Kohta 15	17
1.5.16	Kohta 16	17
1.5.17	Kohta 17	18
1.5.18	Kohta 18	18
1.5.19	Kohta 19	19
1.5.20	Kohta 20	19
1.5.21	Kohta 21	20
1.5.22	Kohta 22	20
1.5.23	Kohta 23	21
1.5.24	Kohta 24	21

1 Benchmarks

1.1 Tehtävä 1

Task 1.

- Find suitable CIS Benchmarks for Windows and Linux versions in target environment (registration is needed for downloads).
- Select one area (second level header 1.1, 1.2, 2.1 etc.) from each guide and check the configurations
 - Notice that there are LEVEL-1 and LEVEL-2 -settings. Find out what these LEVELS mean.

Kuva 1: Tehtävänanto 1

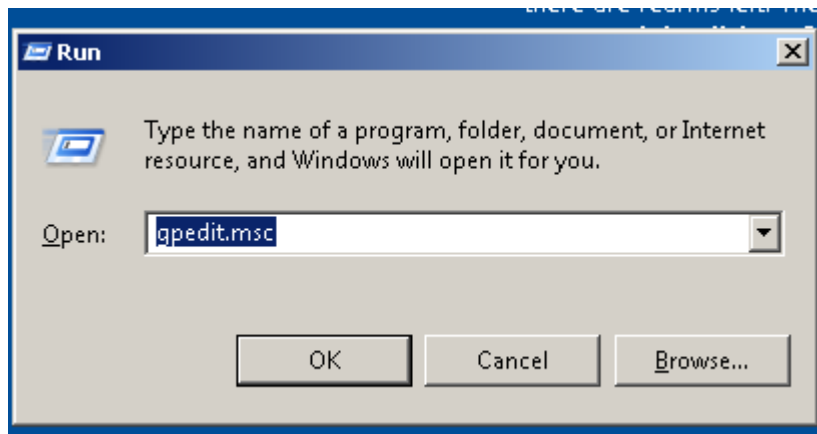
1.2 Windows

Valitsin Windowsin benchmarkiksi: "Administrative Templates(User)". Dokumentin kohdat 19.1, 19.1.1, 19.1.2 olivat tyhjä, joten luonnollisesti skippasin kyseiset kohdat. Seuraavasta kuvasta ilmenee mitkä kohdat minun piti tarkistaa benchmarkista:

19.1.3.1 (L1) Ensure 'Enable screen saver' is set to 'Enabled' (Scored)	951
19.1.3.2 (L1) Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (Scored)	953
19.1.3.3 (L1) Ensure 'Password protect the screen saver' is set to 'Enabled' (Scored)	955
19.1.3.4 (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (Scored)	957

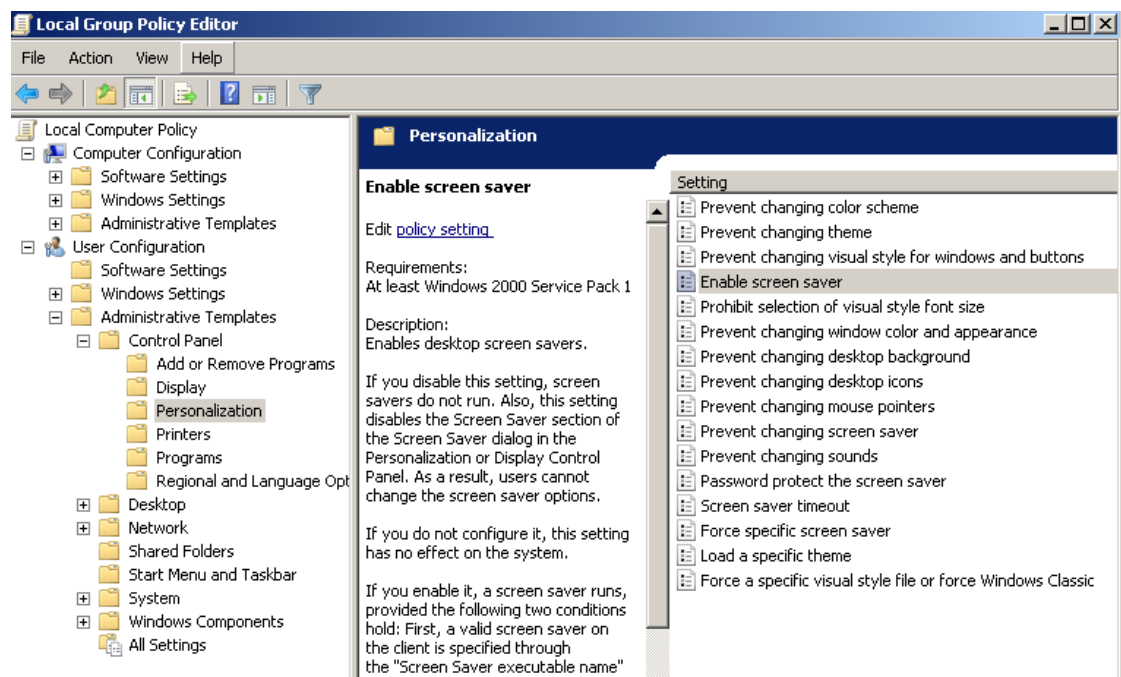
Kuva 2: Tarkistettavat asetukset.

Näytönsäästäjän asetuksiin pääsi klikkaamalla "windows + r" ja kirjoittamalla komennoksi "gpedit.msc"



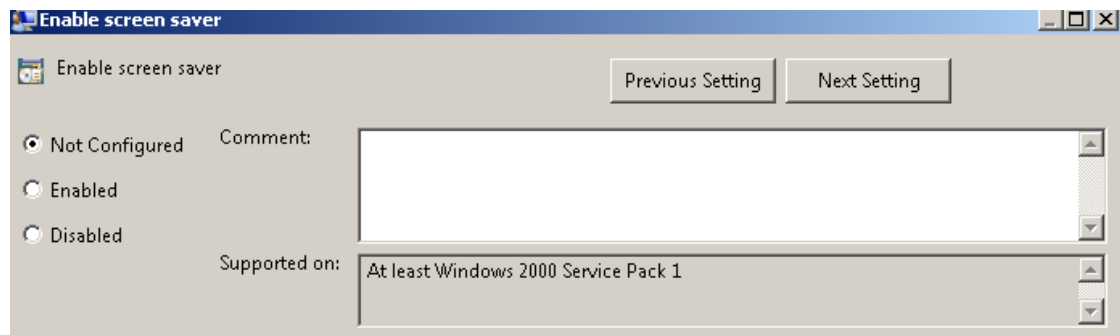
Kuva 3: Run.

Avautuvasta valikosta pääsi näytönsäästäjän asetuksiin klikkaamalla User configuration -> Administrative Templates -> Control Panel -> Personalization.



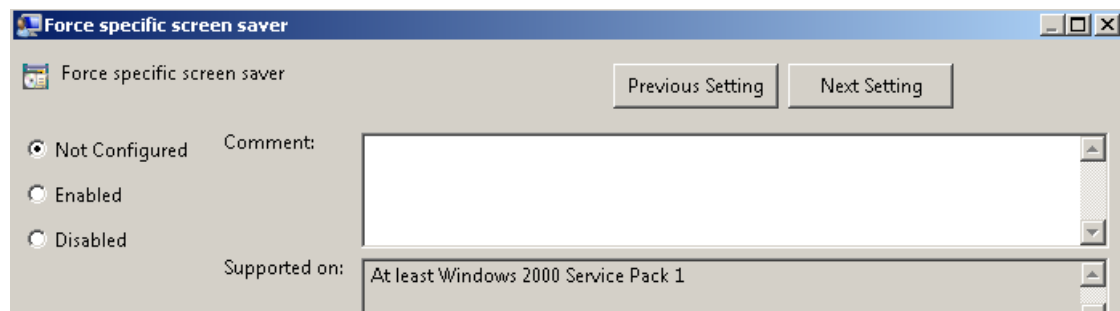
Kuva 4: Näytönsäästäjän asetuksia.

Täältä löytyi kaikki tehtävään kuuluvat asetukset. Aloitin katsomalla onko näytönsäästäjä enabloitu:



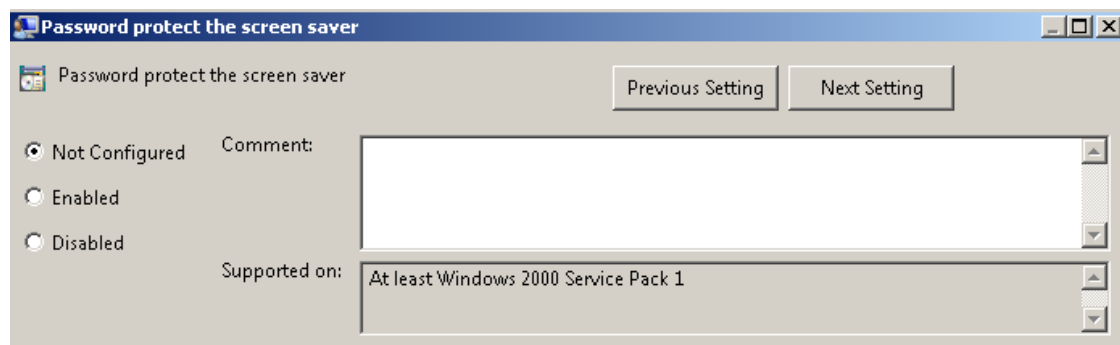
Kuva 5: "Enable screen saver".

seuraavaksi katsoin, onko jokin tietty näytönsäästäjä pakotettu



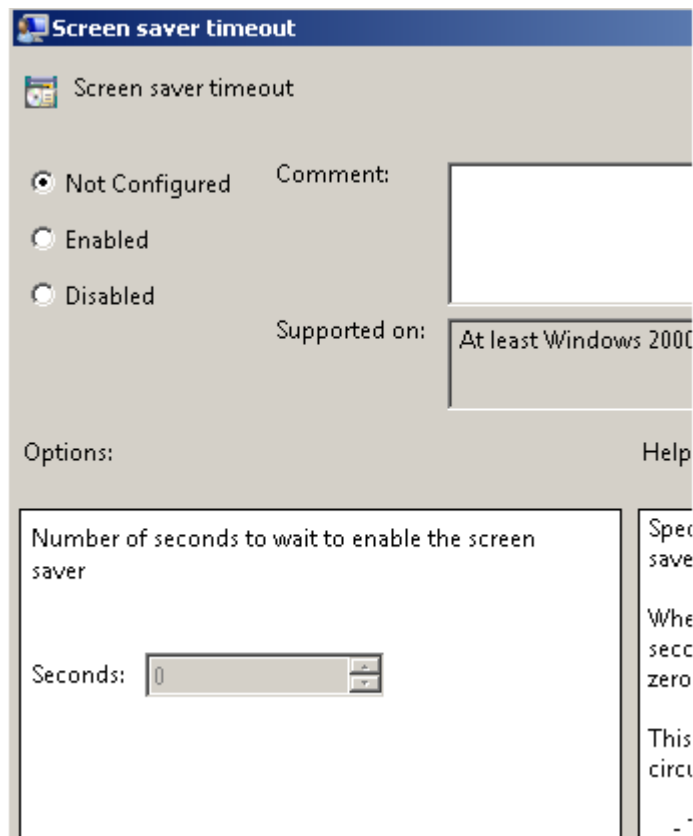
Kuva 6: "Force specific screen saver".

Sitten tarkistin onko näytönsäästäjä salasanalla suojattu



Kuva 7: Näytönsäästäjän suojaus salasanalla.

viimeisenä tarkistin onko näytönsäästäjän käynnistys ajastettu 900 sekuntiin.



Kuva 8: Näytönsäästäjän ajastus.

Kuten kuvista huomataan mitkään suositeltavista asetuksista eivät olleet päällä.

1.3 Linux

Valitsin Linuxin benchmarkiksi "Configure sudo".

1.3 Configure sudo	72
1.3.1 Ensure sudo is installed (Automated)	73
1.3.2 Ensure sudo commands use pty (Automated)	75
1.3.3 Ensure sudo log file exists (Automated)	77

Kuva 9: Tarkistettavat asetukset Linux

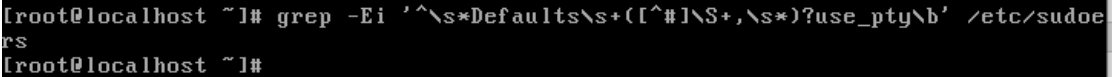
Aloitin tehtävän tarkistamalla, onko sudo asennettu. Käytin tähän komentoa "rpm -q sudo":

```
[root@localhost ~]# rpm -q sudo
sudo-1.8.19p2-10.el7.x86_64
[root@localhost ~]# _
```

Kuva 10: sudo.

Koska sudo oli jo asennettuna ei minun tarvinnut sitä erikseen ladata uudestaan.

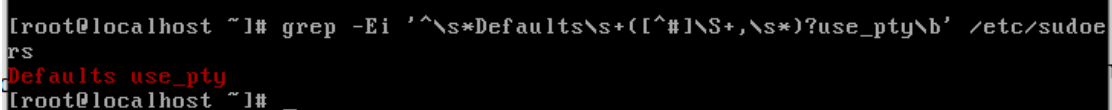
Seuraavaksi tarkistin, että sudo voi vain ajaa komentoja pseudo-pty:ltä komennolla ”
`grep -Ei '^\\s*Defaults\\s+([\\#]\\S+,\\s*)?use_pty\\b' /etc/sudoers`”



```
[root@localhost ~]# grep -Ei '^\\s*Defaults\\s+([\\#]\\S+,\\s*)?use_pty\\b' /etc/sudoers
[root@localhost ~]#
```

Kuva 11: pseudo-pty tarkistus

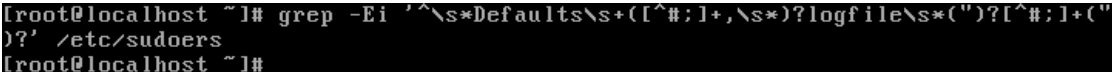
Lisäsin tiedostoon tekstin ”Defaults use_pty” käyttäen tekstieditoria nano (voi käyttää myös visudo:a) ”`nano /etc/sudoers`. Testasin greppiä tämän jälkeen:



```
[root@localhost ~]# grep -Ei '^\\s*Defaults\\s+([\\#]\\S+,\\s*)?use_pty\\b' /etc/sudoers
Defaults use_pty
[root@localhost ~]#
```

Kuva 12: grep pseudo-pty.

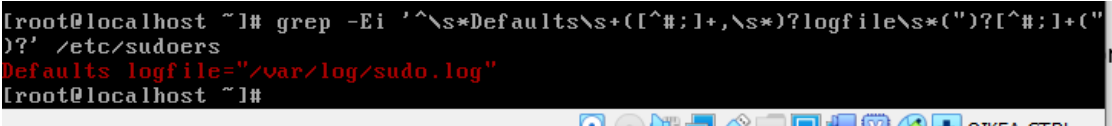
Viimeiseksi tarkistin että sudolla on log tiedosto komennolla ”`grep -Ei '^\\s*Defaults\\s+([\\#;]+,\\s*)?logfile\\s*=\\s*\"([\\#;]+(\"))?' /etc/sudoers`”



```
[root@localhost ~]# grep -Ei '^\\s*Defaults\\s+([\\#;]+,\\s*)?logfile\\s*=\\s*\"([\\#;]+(\"))?' /etc/sudoers
[root@localhost ~]#
```

Kuva 13: logfilen tarkistus.

Lisäsin tiedostoon polun sudon logi-tiedostoon:



```
[root@localhost ~]# grep -Ei '^\\s*Defaults\\s+([\\#;]+,\\s*)?logfile\\s*=\\s*\"([\\#;]+(\"))?' /etc/sudoers
Defaults logfile="/var/log/sudo.log"
[root@localhost ~]#
```

Kuva 14: grep logfile.

1.4 Tehtävä 2

Task 2.

- Audit pfsense -firewall RULES using following checklist
<https://www.sans.org/media/score/checklists/FirewallChecklist.pdf>
 (Select applicable parts from the checklist)

Kuva 15: Tehtävänanto 2.

1.5 Checklist

1.5.1 Kohta 1

No.	Security Elements
1.	<p>Review the rulesets to ensure that they follow the order as follows:</p> <ul style="list-style-type: none"> • anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside) • User permit rules (e.g. allow HTTP to public webserver) • Management permit rules (e.g. SNMP traps to network management server) • Noise drops (e.g. discard OSPF and HSRP chatter) • Deny and Alert (alert systems administrator about traffic that is suspicious) • Deny and log (log remaining traffic for analysis) <p>Firewalls operate on a first match basis, thus the above structure is important to ensure that suspicious traffic is kept out instead of inadvertently allowing them in by not following the proper order.</p>

Aloitin sääntöjen tarkastelun:

<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.47.66	3389 (MS RDP)	*	none
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.47.0/24	53 (DNS)	*	none
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	10.99.67.0/24	21 (FTP)	*	none
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	10.99.67.0/24	22 (SSH)	*	none
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.47.66	3389 (MS RDP)	*	none

Säännöt eivät ole halutussa järjestyksessä

- anti-spoofing: Tämä sääntö on pfsensessä automaattisesti WAN-interfacsessa.
- User permit rules: http liikenne sallittu.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	✓	0/0 B	IPv4	*	*	*	80 (HTTP)	*	none	
			TCP							

Kuva 16: HTTP.

- Management permit rules: Windows 7 remote desktop liikenne sallittu.

<input type="checkbox"/>	✓	0/0 B	IPv4	*	*	192.168.47.66	3389 (MS RDP)	*	none	
			TCP							

Kuva 17: MS-RDP.

<input type="checkbox"/>	✓	0/0 B	IPv4	*	*	192.168.47.66	3389 (MS RDP)	*	none	NAT remote management
			TCP							

Kuva 18: MS-RDP 2.

- Noise drops: En löytänyt tälle mitään sääntöä, vaikka pingit eivät mene läpi.
- Deny and alert & deny and log: Palomuurissa ei ole yhtään kieltävää sääntöä tai loggausta päällä millään interfacella.

1.5.2 Kohta 2

The following commands should be blocked for SMTP at the application level firewall:

- EXPN (expand)
- VRFY (verify)
- DEBUG
- WIZARD

The following command should be blocked for FTP:

- PUT

Palomuurin säännöissä ei ole lainkaan sääntöjä SMTP-protokollaa varten. En

löytänyt säännöistä estoa FTP "PUT komennolle niin se luultavasti sallittu koska

FTP on sallittu

<input type="checkbox"/>	✓	0/0 B	IPv4	*	*	10.99.67.0/24	21 (FTP)	*	none	
			TCP							

Kuva 19: FTP.

Review the denied URL's and ensure that they are appropriate for e.g. any URL's to hacker sites should be blocked. In some instances organisations may want to block access to x-rated sites or other harmful sites. As such they would subscribe to sites, which maintain listings of such harmful sites. Ensure that the URL's to deny are updated as released by the sites that warn of harmful sites.

Ensure that only authorised users are authenticated by the application level firewall.


Kuva 20: Autentikointi.


Palomuurissa ei ole lainkaa blacklistattuja sivuja mutta käyttäjän autentikointi toimii.

The following input errors were detected:

- Authentication failed.

Authentication Test

<u>Authentication Server</u>	Local Database 
	Select the authentication server to test against.
<u>Username</u>	asd
<u>Password</u>	*****

 Test

Kuva 21: Autentikointi testi 1.

User admin authenticated successfully. This user is a member of groups:

- all
- admins

Authentication Test

**Authentication
Server**

Local Database

Select the authentication server to test against.

Username

admin

Password

 Test

Kuva 22: Autentikointi testi 2.

1.5.3 Kohta 3

3.	<p>Stateful inspection</p> <p>Review the state tables to ensure that appropriate rules are set up in terms of source and destination IP's, source and destination ports and timeouts. Ensure that the timeouts are appropriate so as not to give the hacker too much time to launch a successful attack.</p> <p>For URL's</p> <ul style="list-style-type: none"> • If a URL filtering server is used, ensure that it is appropriately defined in the firewall software. If the filtering server is external to the organisation ensure that it is a trusted source. • If the URL is from a file, ensure that there is adequate protection for this file to ensure no unauthorised modifications. <p>Ensure that specific traffic containing scripts; ActiveX and java are striped prior to being allowed into the internal network.</p> <p>If filtering on MAC addresses is allowed, review the filters to ensure that it is restricted to the appropriate MAC's as defined in the security policy.</p>
----	--

Kuva 23: States.

- State pöytien ip osoitteet ovat ok, timeoutista ei löytynyt tietoa.
- Ulkoisen liikenne ei pääse sisäverkkoon.
- Palomuurissa ei ole MAC filteröintiä päällä.

MAC Address

xxxxxxxxxxxx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxxxx or leave blank.

Kuva 24: MAC-osoite

1.5.4 Kohta 4

4.	Logging Ensure that logging is enabled and that the logs are reviewed to identify any potential patterns that could indicate an attack.
----	---

Kuva 25: Lokitus.

Palomuurissa on lokitus päällä. Kaavojen tunnistus ei ole päällä.

Nov 6 15:14:53	php-fpm	343	/firewall_rules.php: Successful login for user 'admin' from: 192.168.47.66
Nov 6 15:27:48	php-fpm	342	/index.php: User logged out for user 'admin' from: 192.168.47.66
Nov 6 15:27:51	php-fpm	342	/index.php: webConfigurator authentication error for 'asd' from 192.168.47.66
Nov 6 15:27:55	php-fpm	342	/index.php: webConfigurator authentication error for 'agaer' from 192.168.47.66
Nov 6 15:27:59	php-fpm	342	/index.php: Successful login for user 'admin' from: 192.168.47.66

Kuva 26: Lokitietoja.

1.5.5 Kohta 5

5.	Patches and updates Ensure that the latest patches and updates relating to your firewall product is tested and installed. If patches and updates are automatically downloaded from the vendors' websites, ensure that the update is received from a trusted site.
----	--

Kuva 27: Päivitykset.

Palomuurin versio ei ole uusin mahdollinen eikä sitä päivitetä automaattisesti.

Current Base System	2.4.3
Latest Base System	2.4.5_1

Kuva 28: Palomuurin versio.

1.5.6 Kohta 6

6.	<p>Location – DMZ</p> <p>Ensure that there are two firewalls – one to connect the web server to the internet and the other to connect the web server to the internal network. In the event of two firewalls ensure that it is of different types and that dual NIC's are used. This would increase security since a hacker would need to have knowledge of the strengths, weaknesses and bugs of both firewalls. The rulesets for both firewalls would vary based on their location e.g. between web server and the internet and between web server and the internal network.</p>
----	---

Kuva 29: DMZ

Käytössä on vain yksi palomuuuri mutta siinä on kolme verkkorajapintaa.

```

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.43.72/24
LAN (lan)      -> em1      -> v4: 10.99.67.254/25
                v6: fe80::afd1:63d7:9f23:aa11/64
LAN2 (opt1)    -> em2      -> v4: 192.168.47.1/24

```

Kuva 30: Palomuurin verkkorajapinnat.

1.5.7 Kohta 7

7.	<p>Vulnerability assessments/ Testing</p> <p>Ascertain if there is a procedure to test for open ports using nmap and whether unnecessary ports are closed.</p> <p>Ensure that there is a procedure to test the rulesets when established or changed so as not to create a denial of service on the organisation or allow any weaknesses to continue undetected.</p>
----	---

Palomuuuri ei ole niin hyvin konfiguroitu, että se estäisi DoS hyökkäyksen. Labra 2 nmappasimme avoimia portteja ja niitä löytyi kaksi.

```

sudouser@kali:~$ nmap -e eth1 -A -p1-65535 192.168.43.72
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-22 09:13 EDT
Nmap scan report for TheGreatFirewall (192.168.43.72)
Host is up (0.0011s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         nginx
|_http-title: Login
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-cert: Subject: commonName=IE8WIN7
|_Not valid before: 2020-10-05T19:23:01
|_Not valid after: 2021-04-06T19:23:01
|_ssl-date: 2020-10-22T13:15:56+00:00; +3s from scanner time.

Host script results:
|_clock-skew: 2s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.86 seconds
sudouser@kali:~$

```

Kuva 31: Nmap.

1.5.8 Kohta 8

- | | |
|----|---|
| 8. | Compliance with security policy
Ensure that the ruleset complies with the organisation security policy. |
|----|---|

Kuva 32: Organisaation turvallisuuspolitiikka.

Palomuuuri on yksityisellä koneella, joten tämä kohta on turha.

1.5.9 Kohta 9

- | | |
|----|--|
| 9. | Ensure that the following spoofed, private (RFC 1918) and illegal addresses are blocked:
Standard unroutables <ul style="list-style-type: none"> • 255.255.255.255 • 127.0.0.0 Private (RFC 1918) addresses <ul style="list-style-type: none"> • 10.0.0.0 – 10.255.255.255 • 172.16.0.0 – 172.31.255.255 • 192.168.0.0 - 192.168.255.255 Reserved addresses <ul style="list-style-type: none"> • 240.0.0.0 Illegal addresses <ul style="list-style-type: none"> • 0.0.0.0 UDP echo
ICMP broadcast (RFC 2644)
Ensure that traffic from the above addresses is not transmitted by the interface. |
|----|--|

Nämä pitäisi olla automaattisesti WAN rajapinnassa estetty mutta tarkistin vielä pingaamalla ulkoverkosta LAN ja WAN rajapintoja. En testannut kaikkia, koska oletan että palomuuuri estää kaikki, jos se estää yhden näistä. Näihi ei ole itse tehty sääntöjä erikseen.

```
[root@localhost ~]# ip a l
2: enp0s8: <BROADCAST,MULTICAST>
    qlen 1000
    inet 192.168.43.87/24 brd 192.168.43.255 scope global enp0s8
    [root@localhost ~]#
```

Kuva 33: IP-osoite mistä skannasin.

```
[root@localhost ~]# ping 10.99.67.254
PING 10.99.67.254 (10.99.67.254) 56(84) bytes of data.
^C
--- 10.99.67.254 ping statistics ---
263 packets transmitted, 0 received, 100% packet loss, time 262269ms
[root@localhost ~]#
```

Kuva 34: Ping LAN.

```
PING 192.168.43.72 (192.168.43.72) 56(84) bytes of data.
^C
--- 192.168.43.72 ping statistics ---
50 packets transmitted, 0 received, 100% packet loss, time 49017ms
[root@localhost ~]#
```

Kuva 35: Ping WAN.

Labra 2 tehty icmp skannaus tuotti tuloksia.

```
sudo@kali:~$ sudo nmap -sP -PI 10.99.67.129/25
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-19 08:02 EDT
Nmap scan report for 10.99.67.145
Host is up (0.00025s latency).
MAC Address: 08:00:27:BB:7D:D0 (Oracle VirtualBox virtual NIC)
Nmap scan report for TheGreatFirewall.localdomain (10.99.67.254)
Host is up (0.00077s latency).
MAC Address: 08:00:27:F9:E8:F0 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.99.67.132
Host is up.
Nmap done: 128 IP addresses (3 hosts up) scanned in 1.88 seconds
```

Kuva 36: ICMP -skannaus.

1.5.10 Kohta 10

10. | Ensure that loose source routing and strict source routing (lsrr & ssrr) are blocked and logged by the firewall.

Kuva 37: LSR & SSR

En löytänyt palomuurista mitään tähän viittaavaa eli tuskin on estetty?

1.5.11 Kohta 11

11.	Port restrictions		
	The following ports should be blocked:		
	Service	Port Type	Port Number
	DNS Zone Transfers	TCP	53
	TFTP Daemon	UDP	69
	Link	TCP	87
	SUN RPC	TCP & UDP	111
	BSD UNIX	TCP	512 – 514
	LPD	TCP	515
	UUCPD	TCP	540
	Open Windows	TCP & UDP	2000
	NFS	TCP & UDP	2049
	X Windows	TCP & UDP	6000 – 6255
	Small services	TCP & UDP	20 and below

Kuva 38: Suljettavat portit 1.

Small services	TCP & UDP	20 and below
FTP	TCP	21
SSH	TCP	22
Telnet	TCP	23
SMTP (except external mail relays)	TCP	25
NTP	TCP & UDP	37
Finger	TCP	79
HTTP (except to external web servers)	TCP	80
POP	TCP	109 & 110
NNTP	TCP	119
NTP	TCP	123
NetBIOS in Windows NT	TCP & UDP	135
NetBIOS in Windows NT	UDP	137 & 138
NetBIOS	TCP	139
IMAP	TCP	143
SNMP	TCP	161 & 162
SNMP	UDP	161 & 162
BGP	TCP	179
LDAP	TCP & UDP	389
SSL (except to external web servers)	TCP	443
NetBIOS in Win2k	TCP & UDP	445
Syslog	UDP	514
SOCKS	TCP	1080
Cisco AUX port	TCP	2001
Cisco AUX port (stream)	TCP	4001
Lockd (Linux DoS Vulnerability)	TCP & UDP	4045
Cisco AUX port (binary)	TCP	6001
Common high order HTTP ports	TCP	8000, 8080, 8888

Kuva 39: Suljettavat portit 2.

Tarkistin mitkä portit ovat auki ja tulokseksi sain vain portit 80,53 ja 954

```
[2.4.3-RELEASE][root@TheGreatFirewall.localdomain]/root: netstat -an | grep
EN
tcp6      0      0 *.80                *.*                LISTEN
tcp4      0      0 *.80                *.*                LISTEN
tcp4      0      0 127.0.0.1.953       *.*                LISTEN
tcp4      0      0 *.53                *.*                LISTEN
tcp6      0      0 *.53                *.*                LISTEN
[2.4.3-RELEASE][root@TheGreatFirewall.localdomain]/root: █
```

Kuva 40: Netstat portit.

Tosin tarkistin portin 953 palomuurista ja se siellä portti oli kiinni.

Diagnostics / Test Port

Connection failed.

Test Port

Hostname
TheGreatFirewall

Port
953

Kuva 41: Portti 953 testaus.

1.5.12 Kohta 12

- | | |
|-----|--|
| 12. | Remote access
If remote access is to be used, ensure that the SSH protocol (port 22) is used instead of Telnet. |
|-----|--|

Kuva 42: Remote access.

Microsoftin remote desktop protokolla käyttää porttia 3389

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4	*	*	192.168.47.66	3389 (MS RDP)	*	none
			TCP						

Kuva 43: Etäyhteys.

1.5.13 Kohta 13

13.	File Transfers If FTP is a requirement, ensure that the server, which supports FTP, is placed in a different subnet than the internal protected network.
-----	---

Kuva 44: FTP.

Ainoastaan Kali Linux tukee FTP:tä ja se on ulkoverkossa.

1.5.14 Kohta 14

14.	Mail Traffic Ascertain which protocol is used for mail and ensure that there is a rule to block incoming mail traffic except to internal mail.
-----	---

Kuva 45: Sähköposti protokolla.

PFsense tukee useampaa sähköposti protokollaa esim. SMTP mutta erillisiä sääntöjä näille ei ole palomuriin laitettu.

1.5.15 Kohta 15

15.	ICMP (ICMP 8, 11, 3) Ensure that there is a rule blocking ICMP echo requests and replies. Ensure that there is a rule blocking outgoing time exceeded and unreachable messages.
-----	---

Kuva 46: ICMP sääntöjen tarkastus.

Tälle ei ole laitettu erillistä sääntöä kuten huomataan kohdassa 9 olevassa ICMP skannauksesta.

1.5.16 Kohta 16

16.	IP Readdressing/IP Masquerading Ensure that the firewall rules have the readdressing option enabled such that internal IP addresses are not displayed to the external untrusted networks.
-----	--

Pfsense uudelleen kirjoittaa kaikki portit, jotka ovat liitöksissä ulosmenevään liikenteeseen. ” By default, pfSense rewrites the source port on all outgoing connections except for UDP port 500 (IKE for VPN traffic). Some operating systems do a poor job of source port randomization, if they do it at all. This makes IP address

spoofing easier and makes it possible to fingerprint hosts behind the firewall from their outbound traffic. Rewriting the source port eliminates these potential (but unlikely) security vulnerabilities.” Pfsense myös piilottaa sisäverkossa olevat osoitteet kuten aikaisemmissa pingeissä nähdään (kohta 9).

1.5.17 Kohta 17

17. Zone Transfers

If the firewall is stateful, ensure packet filtering for UDP/TCP 53. IP packets for UDP 53 from the Internet are limited to authorised replies from the internal network. If the packet were not replying to a request from the internal DNS server, the firewall would deny it. The firewall is also denying IP packets for TCP 53 on the internal DNS server, besides those from authorised external secondary DNS servers, to prevent unauthorised zone transfers.

Kuva 47: Tilallinen vai tilaton.

Pfsense on tilallinen palomuuuri. WAN rajapinnassa on UDP/TCP 53 sallittu kuten myös LAN2 rajapinnassa. LAN2 tcp liikenteestä on 2 tilaa (state) jotka voisivat viitata siihen, että takaisin päin liikenne LAN2 on sallittu osoitteiden 192.168.47.66 -> 192.168.43.72 välillä. En ole tästä tosin varma koska tilassa näkyy eri portti kuin 53 mutta samalla pfsense muokaa ulospäin menevät source portit niin näkykö portit oikein täällä?

States					
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
LAN2	tcp	192.168.47.66:49166 -> 192.168.43.72:80	FIN_WAIT_2:FIN_WAIT_2	11 / 19	2 KiB / 15 KiB
LAN2	tcp	192.168.47.66:49167 -> 192.168.43.72:80	ESTABLISHED:ESTABLISHED	12 / 19	2 KiB / 15 KiB

Kuva 48: LAN2 tilat.

1.5.18 Kohta 18

18. Egress Filtering

Ensure that there is a rule specifying that only traffic originating from IP's within the internal network be allowed. Traffic with IP's other than from the Internal network are to be dropped.
Ensure that any traffic originating from IP's other than from the internal network are logged.

Kuva 49: Liikenne lähtöisin sisäverkosta sallitaan.

Rules (Drag to Change Order)										
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	0/0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	0/0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
<input type="checkbox"/>	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule

Kuva 50: LAN säännöt.

Sallii liikenteen LAN verkosta. Palomuurista ei löydy lokitietoja eikä sääntöä, joka tiputtaa muut kuin lähiverkon IP:t.

1.5.19 Kohta 19

19. **Critical servers**
Ensure that there is a deny rule for traffic destined to critical internal addresses from external sources. This rule is based on the organisational requirements, since some organisations may allow traffic via a web application to be routed via a DMZ.

Tälläistä sääntöä ei ole asetettu palomuriin.

1.5.20 Kohta 20

20. **Personal firewalls**
Ensure that laptop users are given appropriate training regarding the threats, types of elements blocked by the firewall and guidelines for operation of the personal firewall. This element is essential, since often times personal firewalls rely on user prompt to respond to attacks e.g. whether to accept/deny a request from a specific address.
Review the security settings of the personal firewall to ensure that it restricts access to specific ports, protects against known attacks, and that there is adequate logging and user alerts in the event of an intrusion.
Ensure that there is a procedure to update the software for any new attacks that become known.
Alternatively most tools provide the option of transferring automatic updates via the internet. In such instances ensure that updates are received from trusted sites.

Palomuri ei ole konfiguroitu tiukaksi eli se ei ole kaikista turvallisista vaihtoehdoista.

Tapahtumia lokitetaan vähän eikä tapahtumista varoiteta. Automaattisia päivityksiä ei myöskään ole.

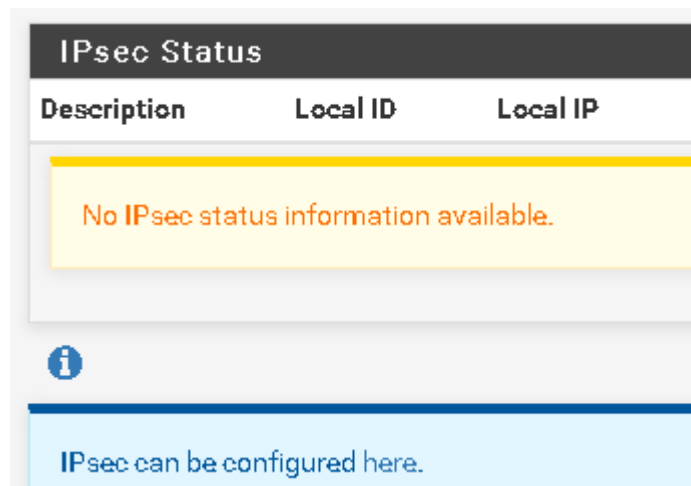
1.5.21 Kohta 21

21.	<p>Distributed firewalls</p> <p>Ensure that the security policy is consistently distributed to all hosts especially when there are changes to the policy.</p> <p>Ensure that there are adequate controls to ensure the integrity of the policy during transfer, e.g. IPSec to encrypt the policy when in transfer.</p> <p>Ensure that there are adequate controls to authenticate the appropriate host. Again IPSec can be used for authentication with cryptographic certificates.</p>
-----	--

Kuva 51: Muutettujen sääntöjen autenttisuus.

IPsecciä ei ole konfiguroitu palomuriin eikä muutoksista ilmoiteta kenellekään.

Onhan kyseessä yksityishenkilön palomuri. Myöskään sääntöjen tai hostien autenttisuutta ei tarkisteta.



Kuva 52: IPsec.

1.5.22 Kohta 22

22.	<p>Stealth Firewalls</p> <p>Ensure that default users and passwords are reset.</p> <p>Ensure that the firewall is appropriately configured to know which hosts are on which interface.</p> <p>Review the firewall access control lists to ensure that the appropriate traffic is routed to the appropriate segments.</p> <p>A stealth firewall does not have a presence on the network it is protecting and it makes it more difficult for the hacker to determine which firewall product is being used and their versions and to ascertain the topology of the network.</p>
-----	---

Palomuri käyttää tehdas salasanaa ja käyttäjätunnusta. Admin kuuluu ryhmään "all" ja "admins"

User admin authenticated successfully. This user is a member of groups:

- all
- admins

Kuva 53: Adminin ryhmät.

En löytänyt palomuurista myöskään minkäänlaista ACL-listaa. Palomuuuri ei myöskään ole piilossa sillä se näkyy skannauksessa (labra 2).

```

sudouser@kali:~$ nmap -e eth1 -A -p1-65535 192.168.43.72
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-22 09:13 EDT
Nmap scan report for TheGreatFirewall (192.168.43.72)
Host is up (0.0011s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         nginx
|_http-title: Login
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-cert: Subject: commonName=IE8WIN7
|_Not valid before: 2020-10-05T19:23:01
|_Not valid after: 2021-04-06T19:23:01
|_ssl-date: 2020-10-22T13:15:56+00:00; +3s from scanner time.

Host script results:
|_clock-skew: 2s

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.86 seconds
sudouser@kali:~$

```

Kuva 54: "TheGreatFirewall".

1.5.23 Kohta 23

23.	Ensure that ACK bit monitoring is established to ensure that a remote system cannot initiate a TCP connection, but can only respond to packets sent to it.
-----	--

Tätä ei ole asetettu.

1.5.24 Kohta 24

24.	Continued availability of Firewalls Ensure that there is a hot standby for the primary firewall.
-----	---

Tätäkään ei ollut asetettuna palomuurissa.

State Synchronization Settings (pfsync)

Synchronize states	<input type="checkbox"/> pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize Interface	<div>WAN</div> <p>If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.</p>
pfsync Synchronize Peer IP	<div>IP Address</div> <p>Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.</p>

Kuva 55: High avail. sync.