

S5 L5

Svolgimento Progetto

Giulia Salani

Consegna

Traccia:

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

[...]

Consegna

- Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (ScansioneInizio.pdf)
- Screenshot e spiegazione dei passaggi della remediation (RemediationMeta.pdf)
- Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità
- (il grafico che mostra tutte le vulnerabilità) ScansioneFine.pdf.

Nota: i report possono essere lasciati in inglese.

Svolgimento

Scansione iniziale

Una prima scansione di Nessus su Meta senza alcun intervento di mitigazione restituisce questa situazione:

Metasploitable_aqst07.pdf

File Edit View Go Bookmarks Help

↑ Previous ↓ Next 4 (4 of 8) 85%

Index

- Table Of Contents 2
- ▼ Vulnerabilities b... 3
- 192.168.32.102 4

192.168.32.102

| | | | | |
|----------|------|--------|-----|------|
| 8 | 4 | 16 | 6 | 73 |
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 107

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|----------|-----------|-----------|--------|---|
| CRITICAL | 9.8 | 9.0 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | - | 51988 | Bind Shell Backdoor Detection |
| CRITICAL | 9.8 | - | 20007 | SSL Version 2 and 3 Protocol Detection |
| CRITICAL | 10.0 | - | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0* | 7.4 | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 7.4 | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0* | 5.9 | 11356 | NFS Exported Share Information Disclosure |
| CRITICAL | 10.0* | - | 61708 | VNC Server 'password' Password |
| HIGH | 8.6 | 5.2 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | - | 42256 | NFS Shares World Readable |
| HIGH | 7.5 | 6.1 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 6.7 | 90509 | Samba Badlock Vulnerability |
| MEDIUM | 6.5 | 3.6 | 139915 | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS |
| MEDIUM | 6.5 | - | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | - | 57582 | SSL Self-Signed Certificate |
| MEDIUM | 6.5 | - | 104743 | TLS Version 1.0 Protocol Detection |
| MEDIUM | 5.9 | 4.4 | 136808 | ISC BIND Denial of Service |

Mitigazione delle vulnerabilità

```
GNU nano 2.0.7      File: /etc/hosts.allow      Modified
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

```
GNU nano 2.0.7      File: /etc/hosts.deny      Modified
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
ALL: ALL

Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
Y Yes
N No      ^C Cancel
```

NFS EXPORTED SHARE INFORMATION DISCLOSURE

SOLUTION

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

NFS (Network File System) è un servizio di condivisione file di rete. Permette ai client di accedere e montare directory da un server remoto su una rete. Se non adeguatamente configurato o protetto, potrebbe presentare vulnerabilità che possono essere sfruttate per attacchi.

È il nostro caso.

Per mitigare questa vulnerabilità, intervengo sui file `hosts.allow` e `hosts.deny` di Metasploitable, che sono utilizzati per configurare le regole di accesso per servizi di rete come SSH o NFS.

Il file `hosts.allow` specifica quali indirizzi IP o host possono accedere ai servizi. Se un servizio non è elencato in `hosts.allow`, l'accesso viene negato per impostazione predefinita.

Il file `hosts.deny`, al contrario, specifica a quali indirizzi IP o host è vietato accedere ai servizi. Se un host è elencato sia in `hosts.allow` che in `hosts.deny`, `hosts.deny` avrà la precedenza.

Sono intervenuta sui file svuotando `hosts.allow` e specificando in `hosts.deny` che è negato l'accesso a qualsiasi host (`ALL: ALL`).


```
Password:
Last login: Wed Dec 20 09:48:40 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin# _
```

VNC SERVER PASSWORD «PASSWORD»

SOLUTION

Secure the VNC server with a strong password.

VNC (Virtual Network Computing) su Metasploitable 2 è un software che consente di controllare un computer da remoto attraverso una connessione di rete. Se non protetto adeguatamente, un attaccante potrebbe sfruttare VNC per ottenere accesso non autorizzato al sistema ospite.

Durante la scansione, Nessus ha rilevato che la password per accedervi è "password".

Sono intervenuta sulla criticità cambiando la password con una stringa forte: la nuova è una combinazione di lettere maiuscole e minuscole, numeri e simboli.

Per farlo ho usato il comando "vncpasswd".

BIND SHELL BACKDOOR DETECTION

SOLUTION

Verify if the remote host has been compromised and reinstall the system if necessary.

```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# ufw status
Firewall not loaded
root@metasploitable:/home/msfadmin# ufw enable
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded
root@metasploitable:/home/msfadmin# ufw deny 1524
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded
```

| To | Action | From |
|----------|--------|----------|
| 1524:tcp | DENY | Anywhere |
| 1524:udp | DENY | Anywhere |

```
root@metasploitable:/home/msfadmin# _
```

Mi trovo nell'ambiente di test, Metasploitable è sulla rete interna di Kali e nessuno vi ha accesso se non, appunto, io con Kali. In questo caso quindi non seguo alla lettera le istruzioni di Nessus perché il sistema non può essere stato compromesso non avendo io eseguito azioni in tal senso.

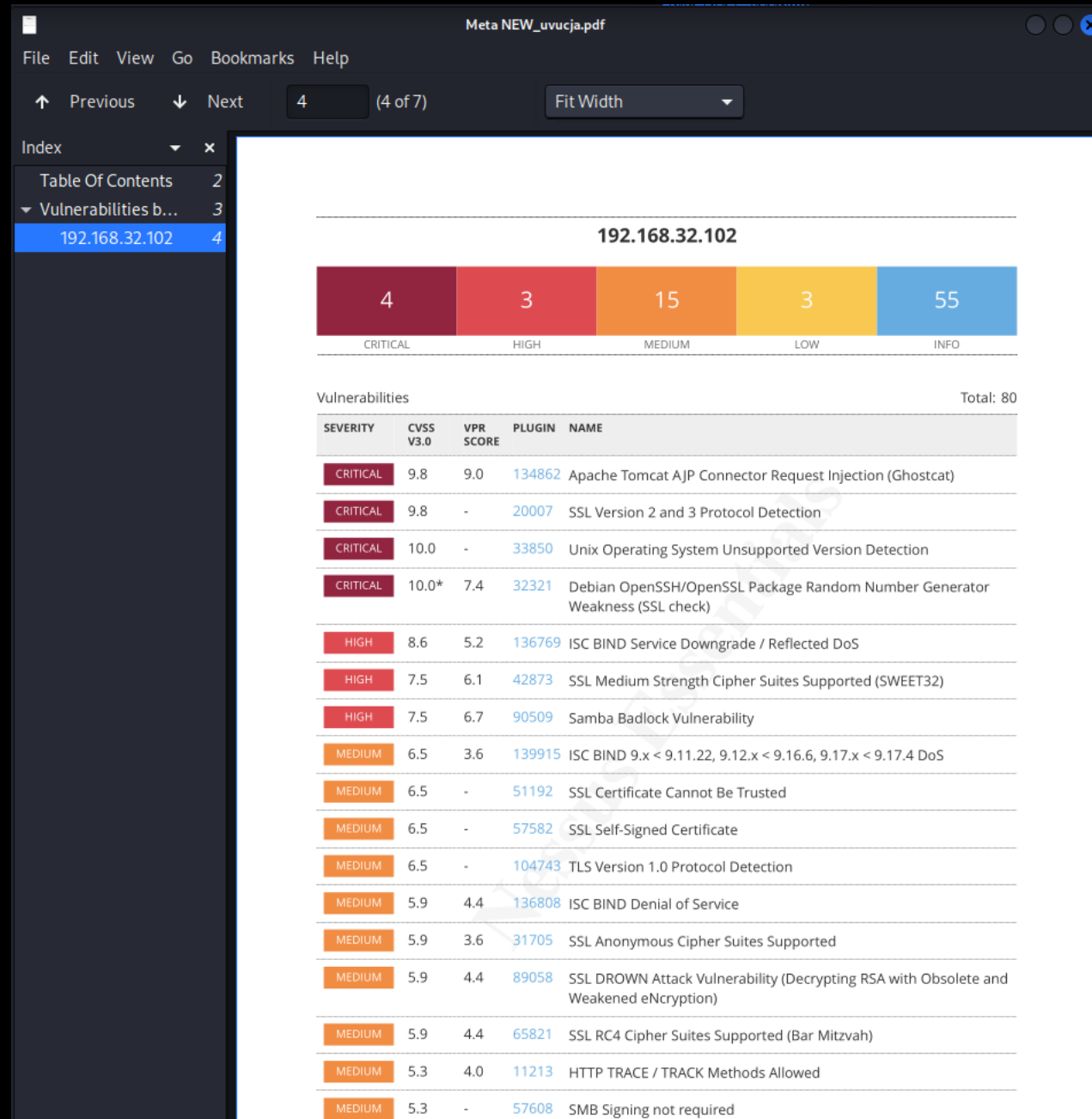
Per porre rimedio a questa vulnerabilità intervengo con una regola firewall in Meta. UFW (Uncomplicated Firewall) su Metasploitable 2 è un frontend per gestire regole di firewall su sistemi Linux. Consente di definire quali connessioni di rete sono permessi o bloccati, aiutando a proteggere il sistema da accessi indesiderati o attacchi esterni.

Dopo aver ottenuto i privilegi di root, controllo lo status del firewall che non è caricato. Lo carico («ufw enable») e inserisco la regola che nega l'accesso dalla porta 1524 («ufw deny 1524»). Da Nessus, infatti, ho potuto approfondire la vulnerabilità e notare che la backdoor interessa la porta 1524.

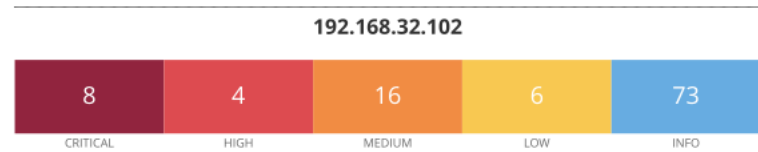
C'è un passaggio che non è esplicitato nello screenshot ma che ho dovuto implementare a posteriori: occorre impostare la regola di default di UFW in ALLOW (comando «ufw default ALLOW») altrimenti tutte le connessioni vengono bloccate perché il default è deny.

Scansione finale

Al termine delle mitigazioni, effettuiamo una nuova scansione e questo è il risultato:

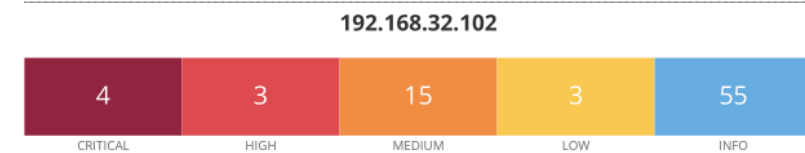


Un confronto fra le due scansioni (iniziale a destra e finale a sinistra) permette di notare come gli interventi di mitigazione abbiano sensibilmente ridotto le vulnerabilità.



Vulnerabilities Total: 107

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|----------|-----------|-----------|--------|---|
| CRITICAL | 9.8 | 9.0 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | - | 51988 | Bind Shell Backdoor Detection |
| CRITICAL | 9.8 | - | 20007 | SSL Version 2 and 3 Protocol Detection |
| CRITICAL | 10.0 | - | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0* | 7.4 | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 7.4 | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0* | 5.9 | 11356 | NFS Exported Share Information Disclosure |
| CRITICAL | 10.0* | - | 61708 | VNC Server 'password' Password |
| HIGH | 8.6 | 5.2 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | - | 42256 | NFS Shares World Readable |
| HIGH | 7.5 | 6.1 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 6.7 | 90509 | Samba Badlock Vulnerability |
| MEDIUM | 6.5 | 3.6 | 139915 | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS |
| MEDIUM | 6.5 | - | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | - | 57582 | SSL Self-Signed Certificate |
| MEDIUM | 6.5 | - | 104743 | TLS Version 1.0 Protocol Detection |
| MEDIUM | 5.9 | 4.4 | 136808 | ISC BIND Denial of Service |



Vulnerabilities Total: 80

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|----------|-----------|-----------|--------|---|
| CRITICAL | 9.8 | 9.0 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | - | 20007 | SSL Version 2 and 3 Protocol Detection |
| CRITICAL | 10.0 | - | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0* | 7.4 | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| HIGH | 8.6 | 5.2 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | 6.1 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 6.7 | 90509 | Samba Badlock Vulnerability |
| MEDIUM | 6.5 | 3.6 | 139915 | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS |
| MEDIUM | 6.5 | - | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | - | 57582 | SSL Self-Signed Certificate |
| MEDIUM | 6.5 | - | 104743 | TLS Version 1.0 Protocol Detection |
| MEDIUM | 5.9 | 4.4 | 136808 | ISC BIND Denial of Service |
| MEDIUM | 5.9 | 3.6 | 31705 | SSL Anonymous Cipher Suites Supported |
| MEDIUM | 5.9 | 4.4 | 89058 | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| MEDIUM | 5.9 | 4.4 | 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| MEDIUM | 5.3 | 4.0 | 11213 | HTTP TRACE / TRACK Methods Allowed |
| MEDIUM | 5.3 | - | 57608 | SMB Signing not required |