Exploitation e Remediation

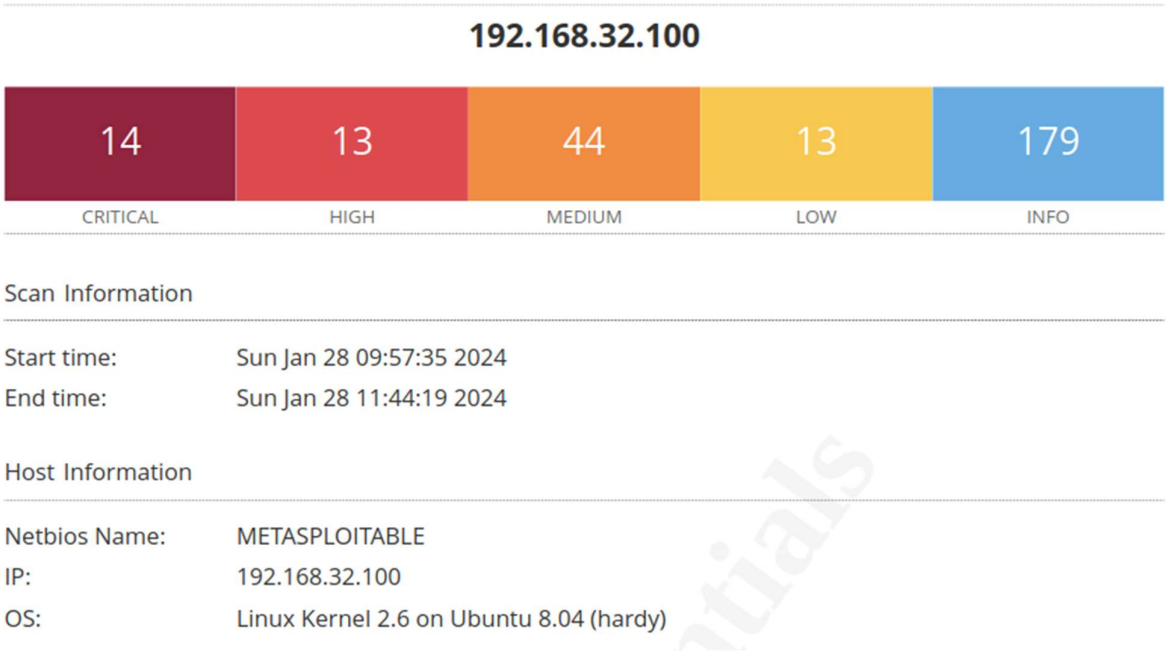
Come stabilito in fase di Ingaggio, verranno bypassate determinate fasi previste per un Penetration Test, ossia:

- Raccolta Informazioni
- Enumerazione e Scansione dei Sistemi,
- Post-Exploitation (Mantenimento Accessi)
- Scrittura della Relazione Finale

per concentrarci sulla fase di Exploitation e Remediation. La fase di Exploitation, consiste nella costruzione di una lista delle vulnerabilità presenti sui sistemi target e successiva pesatura di quest'ultima, mentre quella di Remediation consiste nella creazione di una lista di azioni da intraprendere per sanare i problemi di sicurezza. In entrambe le fasi verranno prese in considerazione, come da accordi, solo 4 vulnerabilità. Infine verrà eseguita una verifica e convalida sulla risoluzione delle vulnerabilità.

Exploitation

Per il completamento di questa fase utilizzeremo un vulnerability scanner, nel dettaglio Nessus, per analizzare il nostro target di riferimento ossia la macchina Metasploitable 2, il cui indirizzo IP è 192.168.32.100.



Lista vulnerabilità concordate

(evidenziate in azzurro)

Vulnerabilities 107

Filter | Search Vulnerabilities | 107 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1

11356 - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

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

Risk Factor

Critical

VPR Score

5.9

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

46882 - UnrealIRCd Backdoor Detection

Synopsis

The remote IRC server contains a backdoor.

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

See Also

https://seclists.org/fulldisclosure/2010/Jun/277

https://seclists.org/fulldisclosure/2010/Jun/284

http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

tcp/5900/vnc

51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

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

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

tcp/1524/wild_shell

Remediation

Per ciascuna vulnerabilità, laddove fosse necessario, verranno indicati come host autorizzati, solo gli indirizzi IP 192.168.32.101 e 192.168.32.102.

Aggiornamento della macchina Metasploitable

Per riflettere le buone pratiche di sicurezza adottate comunemente nelle organizzazioni, è consigliabile avviare le remediation con l'aggiornamento del sistema operativo della macchina Metasploitable2. Poiché questa macchina è progettata come un ambiente di prova e ha un sistema operativo obsoleto, procederemo innanzitutto con la modifica delle repository al fine di consentire un aggiornamento appropriato. Questa procedura ci permetterà di identificare e affrontare vulnerabilità più realistiche e attuali durante il corso del test di penetrazione.

Aggiunta di nuove sources list

Apriamo il file delle repository usando un editor di testo. Di solito, il file è situato in /etc/apt/sources.list. Utilizzeremo un editor di testo come ad esempio nano.

```
msfadmin@metasploitable:~$ sudo nano /etc/apt/sources.list
```

Aggiungiamo le righe relative ad repository aggiornate.

```
deb http://security.ubuntu.com/ubuntu hardy-security main restricted
deb-src http://security.ubuntu.com/ubuntu hardy-security main restricted
deb http://security.ubuntu.com/ubuntu hardy-security universe
deb-src http://security.ubuntu.com/ubuntu hardy-security universe
deb http://security.ubuntu.com/ubuntu hardy-security multiverse
deb-src http://security.ubuntu.com/ubuntu hardy-security multiverse
deb http://archive.ubuntu.com/ubuntu/ hardy main restricted universe multiverse
deb http://archive.ubuntu.com/ubuntu/ hardy-updates main restricted universe mu$
deb http://archive.ubuntu.com/ubuntu/ hardy-security main restricted universe m$
deb http://old-releases.ubuntu.com/ubuntu/ hardy main restricted universe multi$
deb http://old-releases.ubumtu.com/ubuntu/ hardy-updates main restricted univer$
deb http://old-releases.ubuntu.com/ubuntu/ hardy-security main restricted unive$
```

Infine lanciamo i comandi sudo apt-get update e sudo apt-get upgrade.

NFS Exported Share Information Disclosure

Descrizione vulnerabilitá

La configurazione NFS del server remoto consente a un host non autorizzato di montare le sue condivisioni NFS, rendendo i dati accessibili a potenziali attaccanti.

Remediation Actions

- Identificazione delle Condivisioni NFS
- Modifica delle Autorizzazioni delle Condivisioni NFS
- Aggiornare la configurazione NFS
- Riavvio del Servizio NFS

Identificazione delle Condivisioni NFS: Utilizzeremo il comando “showmount” per l’identificazione delle condivisioni NFS

```
root@metasploitable:~# showmount -e 192.168.32.100
Export list for 192.168.32.100:
/ *
root@metasploitable:~# _
```

L’output “/ *” indica che tutte le risorse del server NFS sono esposte pubblicamente. Questa è una configurazione di sicurezza molto rischiosa, poiché qualsiasi host può montare tutte le condivisioni NFS disponibili sul server.

Modifica delle Autorizzazioni delle Condivisioni NFS: Per la modifica delle autorizzazioni dovremo modificare il file di configurazione NFS, raggiungibile attraverso il path “/etc/exports”, indicando solo gli host autorizzati ossia 192.168.32.101 e 192.168.32.102.

```
  GNU nano 2.0.7             File: /etc/exports

# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
 /       192.168.32.101(rw,sync) 192.168.32.102(ro,sync)

#/      *(rw,sync,no_root_squash,no_subtree_check)
```

Come evidenziato nell'immagine, abbiamo configurato gli host abilitati e abbiamo messo in commento la riga *(rw,sync,no_root_squash,no_subtree_check). Questa riga, quando non è commentata, concede l'accesso in lettura e scrittura (rw) a qualsiasi host (*). Inoltre, consente agli utenti con privilegi di root del client di mantenere gli stessi privilegi su NFS e impedisce al server NFS di eseguire la verifica delle sottodirectory per ogni richiesta di accesso. La modifica apportata limita l'accesso solo agli host specificati, migliorando la sicurezza del sistema e fornendo un controllo più preciso sull'accesso alla condivisione NFS.

Aggiornare la configurazione NFS: Utilizzeremo il comando exportfs -a.

```
root@metasploitable:~# exportfs -a
exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree_check' specif
ied for export "192.168.32.101:/".
  Assuming default behaviour ('no_subtree_check').
  NOTE: this default has changed since nfs-utils version 1.0.x

exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree_check' specif
ied for export "192.168.32.102:/".
  Assuming default behaviour ('no_subtree_check').
  NOTE: this default has changed since nfs-utils version 1.0.x

root@metasploitable:~#
```

Riavvio del Servizio NFS: Utilizzeremo il comando sudo invoke-rc.d nfs-kernel-server restart

```
root@metasploitable:~# sudo invoke-rc.d nfs-kernel-server restart
 * Stopping NFS kernel daemon                                    [ OK ]
 * Unexporting directories for NFS kernel daemon...              [ OK ]
 * Exporting directories for NFS kernel daemon...
exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree_check' specif
ied for export "192.168.32.101:/".
  Assuming default behaviour ('no_subtree_check').
  NOTE: this default has changed since nfs-utils version 1.0.x

exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree_check' specif
ied for export "192.168.32.102:/".
  Assuming default behaviour ('no_subtree_check').
  NOTE: this default has changed since nfs-utils version 1.0.x

                                                               [ OK ]
 * Starting NFS kernel daemon                                  [ OK ]
root@metasploitable:~#
```

UnrealIRCd Backdoor Detection

Descrizione

Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un attaccante di eseguire codice arbitrario sull'host interessato.

Remediation Actions

- Trasferimento del software dalla macchina Kali
- Rimozione software con backdoor
- Estrazione e Installazione del software

Trasferimento del software dalla macchina Kali: Essendo il target una macchina obsoleta, non è possibile procedere direttamente al download del software, procederemo per cui a trasferire quest'ultimo dalla macchina kali linux, attraverso il comando presente in figura sotto.

```
┌──(kali㉿kali)-[~]
└─$ scp -oHostKeyAlgorithms=ssh-rsa unrealircd-6.1.4.tar.gz msfadmin@192.168.32.100:/tmp
msfadmin@192.168.32.100's password:
unrealircd-6.1.4.tar.gz                                       100%   10MB   6.9MB/s   00:01

┌──(kali㉿kali)-[~]
└─$
```

Rimozione del software con backdoor: Utilizzeremo il comando "which" per identificare il path del software, e tramite il comando "rm -fr" procederemo alla rimozione.

```
root@metasploitable:/tmp# which unrealircd
/usr/bin/unrealircd
root@metasploitable:/tmp# sudo rm -rf /usr/bin/unrealircd
root@metasploitable:/tmp# which unrealircd
root@metasploitable:/tmp#
```

Estrazione e Installazione del file: Per procedere all'estrazione utilizzeremo il comando "tar -zxvf".

```
msfadmin@metasploitable:/tmp$ tar -xzvf unrealircd-6.1.4.tar.gz_
```

```
unrealircd-6.1.4/extras/.indent.pro
unrealircd-6.1.4/extras/unreal.supp
unrealircd-6.1.4/extras/wrap-compiler-for-flag-check
unrealircd-6.1.4/extras/pcre2.tar.gz
unrealircd-6.1.4/extras/patches/
unrealircd-6.1.4/extras/patches/spamfilter.conf.patch
unrealircd-6.1.4/extras/patches/patch_spamfilter_conf
unrealircd-6.1.4/extras/curlinstall
unrealircd-6.1.4/unrealircd.in
unrealircd-6.1.4/README.md
unrealircd-6.1.4/Config
unrealircd-6.1.4/BSDmakefile
unrealircd-6.1.4/autoconf/
unrealircd-6.1.4/autoconf/config.guess
unrealircd-6.1.4/autoconf/m4/
unrealircd-6.1.4/autoconf/m4/ax_check_link_flag.m4
unrealircd-6.1.4/autoconf/m4/ax_pthread.m4
unrealircd-6.1.4/autoconf/m4/ax_check_compile_flag.m4
unrealircd-6.1.4/autoconf/m4/unreal.m4
unrealircd-6.1.4/autoconf/config.sub
unrealircd-6.1.4/autoconf/Makefile
unrealircd-6.1.4/autoconf/install-sh
root@metasploitable:/tmp# ls
4695.jsvc_up  unrealircd-6.1.4  unrealircd-6.1.4.tar.gz
root@metasploitable:/tmp#
```

Per l'installazione avvieremo quella guidata attraverso il comando in figura sotto.

```
root@metasploitable:/tmp# cd unrealircd-6.1.4
root@metasploitable:/tmp/unrealircd-6.1.4# ./Config
```

VNC Server 'password' Password

Descrizione

Il server VNC (Virtual Network Computing) in esecuzione sull'host remoto è protetto da una password debole. Nel caso specifico, Nessus è stato in grado di accedere utilizzando l'autenticazione VNC con la password 'password'. Questo è un problema di sicurezza significativo perché un attaccante remoto, senza autenticazione, potrebbe sfruttare questa debolezza per assumere il controllo del sistema.

Remediation Actions

- Sostituzione password debole con una robusta

Sostituzione password: Utilizzeremo il comando "vncpasswd" come in figura sotto.

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$ _
```

Bind Shell Backdoor Detection

Descrizione

È stata identificata una shell in ascolto sulla porta 1524 senza alcuna autenticazione richiesta. Questo è un potenziale problema di sicurezza, in quanto un attaccante potrebbe connettersi a quella porta e inviare comandi direttamente al sistema senza alcuna autenticazione.

Remediation Actions

- Identificazione del processo ed eliminazione di quest'ultimo
- Creazione regola firewall per bloccare l'accesso alla porta

Identificazione del processo

```
msfadmin@metasploitable:~$ sudo netstat -tulpn | grep 1524
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
4645/xinetd
msfadmin@metasploitable:~$
```

Siamo riusciti in questo modo ad identificare che il processo coinvolto è xinetd che è un daemon di sistema in grado di gestire servizi di rete su richiesta. Provvederemo ad eliminare il processo e a disabilitare xinetd.

Eliminazione processo

```
msfadmin@metasploitable:/$ sudo kill -9 4645
```

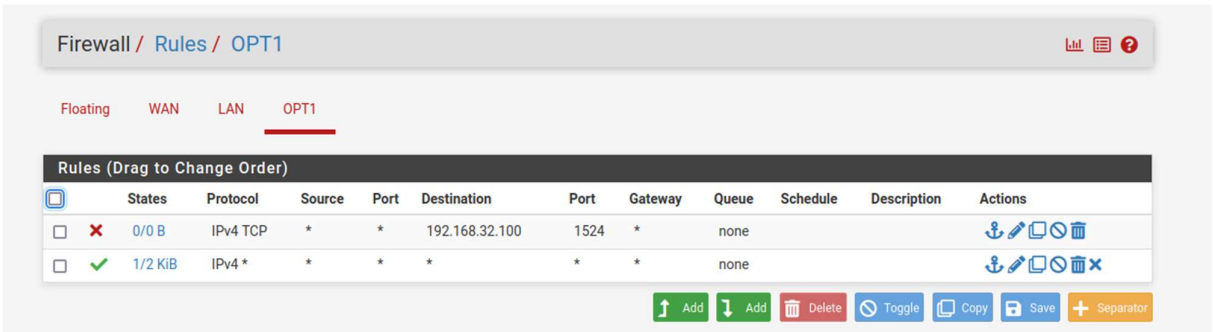
Disabilitare xinetd

```
msfadmin@metasploitable:/$ sudo update-rc.d -f xinetd remove
 Removing any system startup links for /etc/init.d/xinetd ...
   /etc/rc0.d/K20xinetd
   /etc/rc1.d/K20xinetd
   /etc/rc2.d/S20xinetd
   /etc/rc3.d/S20xinetd
   /etc/rc4.d/S20xinetd
   /etc/rc5.d/S20xinetd
   /etc/rc6.d/K20xinetd
msfadmin@metasploitable:/$ _
```

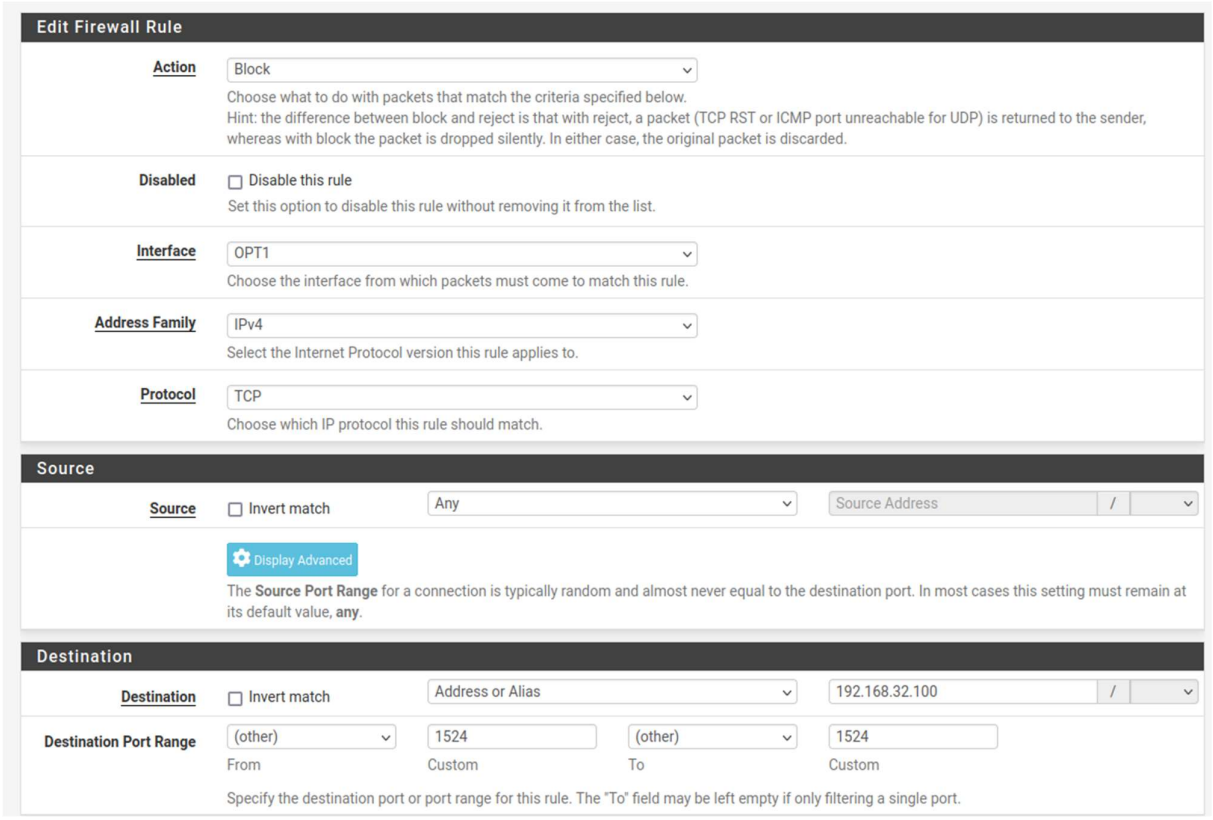
Questo comando rimuove xinetd dai servizi avviati durante il boot

Creazione regola Firewall

Per tutelarci ulteriormente provvederemo a creare una regola firewall per bloccare il traffico sulla porta 1524 della macchina metasploitable. Per fare ciò entriamo nella pagina di configurazione di pfsense, in corrispondenza delle regole firewall per l'interfaccia di metasploitable ossia OPT1.



Dettaglio regola firewall



Verifica sulla risoluzione delle vulnerabilità