

Report Vulnerability Assessment

Indice

1. Vulnerability Scanning; identificazione delle vulnerabilità.
2. Risoluzione delle vulnerabilità
3. Rivalutazione

Vulnerability Scanning; identificazione delle vulnerabilità

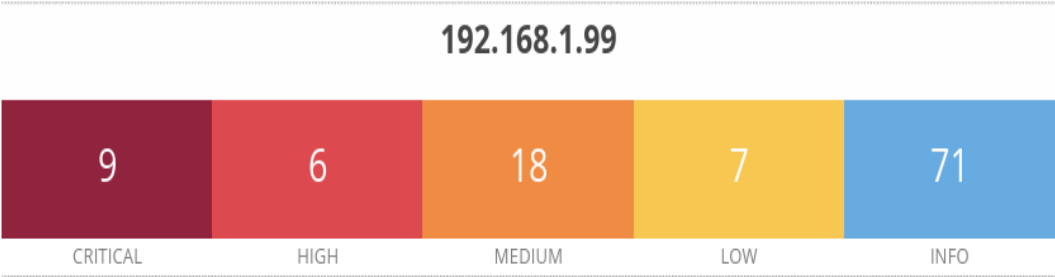
Nell'ambito della computer security Nessus è un software proprietario di tipo client-server di scansione di tutti i tipi di vulnerabilità. Costituito da nessusd, il demone, che effettua la scansione, e da nessus, il client, il quale fornisce all'utente i risultati della scansione, tramite lo scan e l'abilitazione di plugin appositamente configurabili a seconda della tipologia di host e vulnerabilità che si andrà ad analizzare, rileva le vulnerabilità presenti suggerendo le possibili soluzioni attraverso report di facile analisi in vari formati. Tuttora Nessus con le sue tante opzioni per la scansione, la possibilità di scrivere plugin e per il tipo di reportistica prodotta rimane uno dei migliori strumenti per vulnerability assessment.

Tipicamente, Nessus inizialmente effettua una port scan con il suo portscanner interno (oppure talvolta utilizza Nmap[4]) per determinare quali porte sono aperte sull'obiettivo e poi tenta diversi exploit sulle porte aperte. I test di vulnerabilità, disponibili sotto forma di corposi plugin, sono scritti in NASL (Nessus Attack Scripting Language), un linguaggio di programmazione ottimizzato per l'interazione tra reti differenti.

La scansione effettuata ha avuto come target Metaspitable (IP 192.168.1.99).

Ai fini del report sono state prese in considerazione solo le vulnerabilità con un livello di severity "critical". Secondo il Common Vulnerability Scoring System (CVSS), che fornisce un modo per catturare le principali caratteristiche di una vulnerabilità e produrre un punteggio numerico che ne riflette la gravità, le vulnerabilità classificate come critiche sono quelle ricomprese tra un punteggio di 9.1 e 10.0.

Di seguito l'elenco delle vulnerabilità scansionate:



Vulnerabilities Total: 111

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	-	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Sono state prese in esame tre tipologie di vulnerabilità: Bind Shell Backdoor Detection, NFS Exported Share Information Disclosure e VCN Server 'password' Password.

- BPFdoor

The screenshot displays the Metasploit interface for the 'Bind Shell Backdoor Detection' vulnerability (Plugin #51988). The interface is in dark mode. At the top, there are tabs for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below the tabs, the vulnerability is listed as 'CRITICAL Bind Shell Backdoor Detection'. The 'Description' section states: '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.' The 'Solution' section says: 'Verify if the remote host has been compromised, and reinstall the system if necessary.' The 'Output' section shows a command prompt where 'Nessus was able to execute the command "id" using the following request :'. The output is truncated to 10 lines, showing 'root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)'. The 'Plugin Details' section on the right lists: Severity: Critical, ID: 51988, Version: 1.10, Type: remote, Family: Backdoors, Published: February 15, 2011, Modified: April 11, 2022. The 'Risk Information' section shows: Risk Factor: Critical, CVSS v3.0 Base Score: 9.8, CVSS v3.0 Vector: 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, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C. At the bottom, there is a table with columns 'Port' and 'Hosts'. The first row shows '1524/tcp/wild_shell' and '192.168.1.99'.

BPFdoor è un malware che bypassa i firewall per connettersi da remoto a una shell di Linux. Ha l'obiettivo di prendere il controllo completo del sistema sotto attacco, in maniera passiva e mettendosi in ascolto.

Sfruttando una funzione di sniffing, che opera nell'interfaccia al livello di rete, BPFdoor non è soggetto alle regole del firewall e resta in "ascolto" di pacchetti dalle porte ICMP, UDP e TCP. Tramite il rilevamento di specifici pacchetti, dotati di valori ben precisi e, nel caso di UDP/TDP, di una password, la backdoor si attiva eseguendo uno dei comandi supportati, ad esempio attivando una Reverse Shell.

- NFS Exported Share Information Disclosure

The screenshot displays the Metasploit interface for the 'NFS Exported Share Information Disclosure' vulnerability (Plugin #11356). The interface is in dark mode. At the top, there are tabs for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below the tabs, the vulnerability is listed as 'CRITICAL NFS Exported Share Information Disclosure'. The 'Description' section states: '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.' The 'Solution' section says: 'Configure NFS on the remote host so that only authorized hosts can mount its remote shares.' The 'Output' section shows a command prompt where 'The following NFS shares could be mounted :'. The output is a list of shares: '+ /', '+ Contents of /:', '+ ..', '+ bin', '+ boot', '+ more...'. The 'Plugin Details' section on the right lists: Severity: Critical, ID: 11356, Version: 1.21, Type: remote, Family: RPC, Published: March 12, 2003, Modified: August 30, 2023. The 'Risk Information' section shows: Risk Factor: Critical, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C. The 'Vulnerability Information' section shows: Exploit Available: true, Exploit Ease: Exploits are available, Vulnerability Pub Date: January 1, 1985. The 'Exploitable With' section shows: Metasploit (NFS Mount Scanner). At the bottom, there is a table with columns 'Port' and 'Hosts'. The first row shows '2049/udp/rpc-rfs' and '192.168.1.99'.

NFS è un protocollo di rete inizialmente sviluppato da Sun Microsystems nel 1984 che facilita la condivisione dei contenuti sulla rete. Le cartelle condivise risulteranno accessibile, anche in modalità remota, dai sistemi client così come se fossero disponibili in ambito locale.

Il protocollo NFS viene spesso utilizzato nelle reti in cui sono presenti sia sistemi Linux che Windows così da semplificare l'accesso alle risorse.

Supportando a sua volta il protocollo TCP, NFS può essere utilizzato per condividere file e cartelle tra sedi remote attraverso la rete Internet.

In presenza di un NFS Exported Share Information Disclosure si presuppone che almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

- VCN Server 'password' Password

The screenshot displays the Nessus interface for a specific vulnerability. At the top, it shows 'Scan1 / Plugin #61708' and navigation buttons like 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below this, a 'Vulnerabilities' section highlights the 'VNC Server 'password' Password' vulnerability as 'CRITICAL'. The 'Description' states that the VNC server is secured with a weak password, allowing Nessus to login using VNC authentication and a password of 'password'. The 'Solution' advises securing the VNC service with a strong password. The 'Output' section shows a log entry: 'Nessus logged in using a password of "password"'. To the right, 'Plugin Details' provide metadata: Severity: Critical, ID: 61708, Version: \$Revision: 1.2 \$, Type: remote, Family: Gain a shell remotely, Published: August 29, 2012, and Modified: September 24, 2015. Below this, 'Risk Information' lists the Risk Factor as Critical, CVSS v2.0 Base Score as 10.0, and CVSS v2.0 Vector as CVSS2#AV:N/AC:L/Au:N/C:C/I:L/C:A/C. Finally, 'Vulnerability Information' shows 'Default Account: true' and 'Exploited by Nessus: true'.

VCN è un servizio attivabile per fare in modo che il personal computer sul quale viene installato il server VNC sia sempre accessibile da remoto. Solitamente è necessario soltanto specificare una password. Tale password vi consentirà di amministrare, da remoto, il computer sul quale avete installato il server di VNC.

Attraverso questa finestra è possibile, eventualmente, attivare funzionalità avanzate, come la disabilitazione di tastiera/mouse locali/remoti.

Risoluzione delle vulnerabilità

La risoluzione delle vulnerabilità si riferisce al processo di identificazione e correzione delle vulnerabilità o dei punti deboli della sicurezza in software, sistemi o reti. Comporta l'analisi e la definizione delle priorità dei rischi per la sicurezza, l'applicazione di patch e aggiornamenti di sicurezza, l'implementazione di controlli di sicurezza e la verifica dell'efficacia delle misure di sicurezza.

L'obiettivo del processo di risoluzione delle vulnerabilità è ridurre il rischio di attacchi informatici, proteggere le risorse digitali e mantenere la riservatezza, l'integrità e la disponibilità delle informazioni.

Si è proceduto con la risoluzione della prima vulnerabilità 'Bind Shell Backdoor Detection'.

Vulnerabilities

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)

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

Plugin Output

tcp/1524/wild_shell

Nessus was able to execute the command "id" using the following request :

This produced the following truncated output (limited to 10 lines) :
..... snip
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
..... snip

Nessus ha rilevato una backdoor (remote shell) sulla porta 1524.

Con il comando *sudo ufw enable* è stato attivato il firewall e, successivamente, con *sudo ufw deny 1524* è stata applicata una regola che negasse qualsiasi azione sulla porta 1524.

```
# 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:192.168.1.60
```

[Wrote 19 lines]

```
msfadmin@metasploitable:~$ sudo ufw enable
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw deny 1524
Rule added
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded
```

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

```
msfadmin@metasploitable:~$
```

La seconda vulnerabilità NFS Exported Share Information Disclosure è dovuta alla configurazione su Metasploitable che consente l'accesso a tutte le share condivisibili. Tramite il comando `/etc/exports` è possibile visualizzare la lista delle cartelle condivisibili, mentre con `sudo nano /etc/hosts.allow` si può specificare quali computer sulla rete posso accedere alle directory condivise e con `sudo nano /etc/hosts.deny` quali, invece, non possono.

Con il comando allow è stata decommentata la riga ALL:ALL

```
GNU nano 2.0.7      File: /etc/hosts.allow

# /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.
#
ALL:ALL

[ Smooth scrolling enabled ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

Con il comando deny è stata modificata la riga ALL:192.168.1.60, quindi inserendo l'IP di Kali.

```
GNU nano 2.0.7      File: /etc/hosts.deny

# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:         ALL: some.host.name, .some.domain
#                   ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# 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.
#
# 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:192.168.1.60

[ Smooth scrolling enabled ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

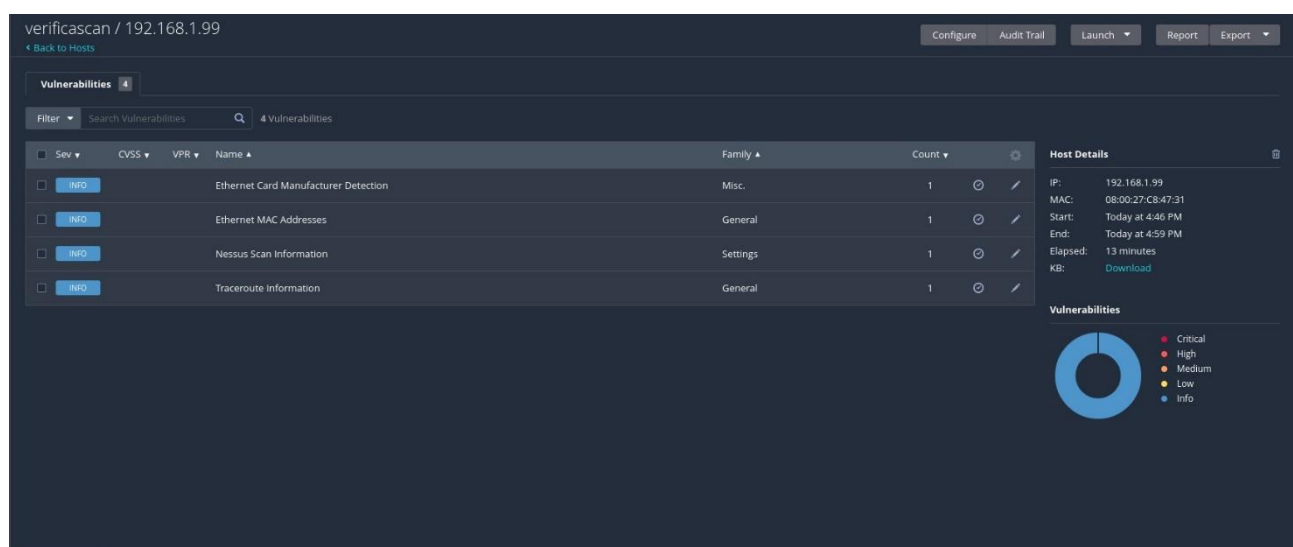
Infine, la terza vulnerabilità, VCN Server 'password' Password, è stata risolta inserendo una password che rispecchi criteri tali da garantire un alto livello di sicurezza, difficile da scoprire con attacchi come Brute Force.

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Warning: password truncated to the length of 8.
Verify:
msfadmin@metasploitable:~$
```

[Switched to password]

Rivalutazione

Quando le vulnerabilità vengono risolte, viene sempre eseguita una nuova valutazione delle vulnerabilità per assicurarsi che le attività di correzione abbiano funzionato e che non abbiano introdotto nuove vulnerabilità.



La posizione di sicurezza complessiva risulta, ora, ottimale.