Progetto fine Modulo 3

Traccia:

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità **critiche** 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.

Di seguito le vulnerabilità di grado critico evidenziate tramite la scansione con Nessus sulla macchina Metasploitable:

Vulnerabilities Total: 149

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	-	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (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*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution

---

Risoluzione della vulnerabilità **Bind Shell Backdoor Detection (51988):**

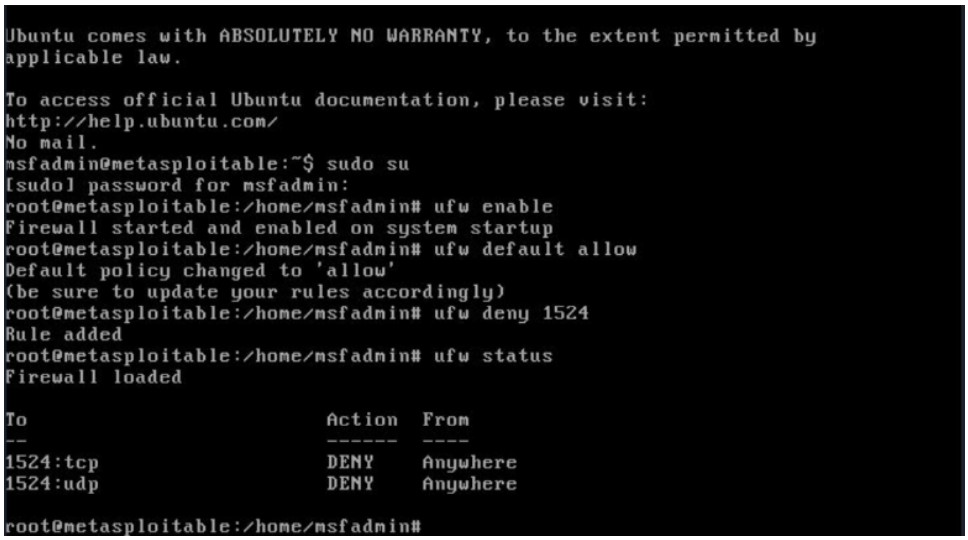
Indica la scoperta di un backdoor legato al servizio BIND (Berkeley Internet Name Domain) su un sistema. Un backdoor è un meccanismo nascosto che consente l'accesso non autorizzato al sistema da parte di un utente malintenzionato.

Se questa vulnerabilità venisse sfruttata, un attaccante potrebbe potenzialmente ottenere un accesso non autorizzato al sistema compromesso attraverso il backdoor associato al servizio BIND.

Per la risoluzione di questa vulnerabilità abbiamo impostato una regola firewall che blocca la connessione alla porta 1524, sulla quale è attiva una backdoor.

Tramite i privilegi –root utilizziamo i seguenti comandi:

- ufw enable
- ufw default allow
- ufw deny 1524



Risoluzione della vulnerabilità **VNC Server 'Password' Password (61708):**

Indica una debolezza nella configurazione di un server VNC (Virtual Network Computing) che utilizza una password predefinita o facilmente indovinabile per l'accesso remoto.

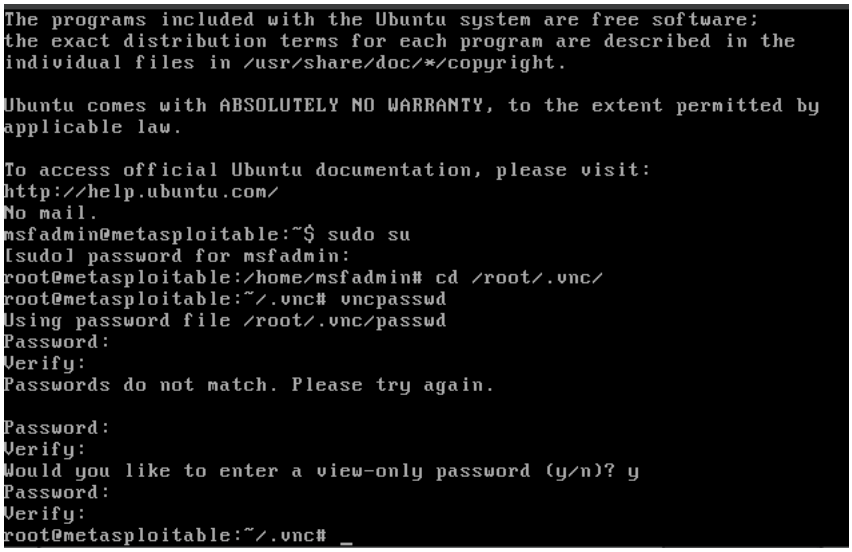
VNC è un sistema di controllo desktop remoto che consente agli utenti di controllare un computer da un'altra posizione tramite una connessione di rete. Se il server VNC è

configurato con una password debole o predefinita come "password", "admin", o simili, ciò costituisce una grave vulnerabilità di sicurezza.

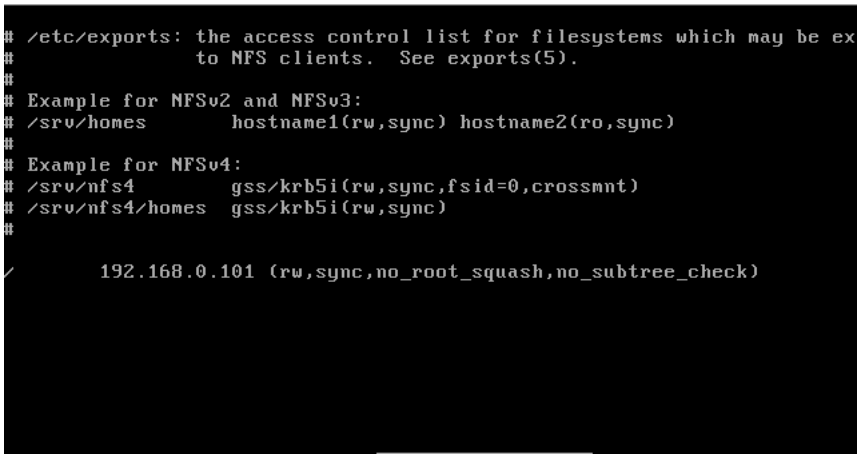
Per questa vulnerabilità è sufficiente modificare la password di VNC, in quanto è letteralmente “password” e corrisponde a quella predefinita e, quindi, accessibile a chiunque.

Dal terminale di Metasploitable basterà, con i privilegi di –root, entrare nella directory di VNC, cambiare la password seguendo le indicazioni e riavviare.

- cd.vnc
- vncpasswd
- sudo reboot



Risoluzione della vulnerabilità **NFS Exported Share Information Disclosure (11356):**



Si riferisce a una debolezza nella configurazione del servizio NFS (Network File System) che espone informazioni sensibili o riservate sui dati condivisi tramite NFS.

NFS è un protocollo di condivisione file di rete che consente agli utenti di accedere e condividere file e directory tra sistemi informatici su una rete. Se il servizio NFS è configurato in modo errato e le condivisioni NFS sono esposte senza adeguati controlli di accesso, ciò potrebbe consentire a un utente non autorizzato di accedere e visualizzare i dati sensibili o riservati contenuti in queste condivisioni.

Per risolvere questa vulnerabilità eseguiamo il comando:

- sudo nano /etc/exports

Nell'ultima riga, inseriamo l'indirizzo IP corrispondente a Metasploitable al posto dell'asterisco, in modo da impedire l'accesso dall'esterno alla macchina.

Risoluzione della vulnerabilità **UnrealIRCd Backdoor Detection (46882):**

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.0.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 14:27 EDT
Nmap scan report for 192.168.0.101
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         vsftpd 2.3.4
22/tcp   open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet      Linux telnetd
25/tcp   open     smtp        Postfix smtpd
53/tcp   open     domain      ISC BIND 9.4.2
80/tcp   open     http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open     rpcbind     2 (RPC #100000)
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open     exec        netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     shell       Netkit rshd
1099/tcp open     java-rmi    GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs         2-4 (RPC #100003)
2121/tcp open     ftp         ProFTPD 1.3.1
3306/tcp open     mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc         VNC (protocol 3.3)
6000/tcp open     X11         (access denied)
6667/tcp open     irc         UnrealIRCd
8009/tcp open     ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
```

Si riferisce alla scoperta di un backdoor nel software UnrealIRCd, un'applicazione utilizzata per creare server di chat IRC (Internet Relay Chat). Un backdoor è una porta segreta o una vulnerabilità deliberatamente inserita nel software che consente a un utente non autorizzato di ottenere un accesso non autorizzato al sistema.

```
Use the ``-h'' option to get more help information.
root@metasploitable:/home/msfadmin# kill lsof -i 6667
bash: kill: lsof: arguments must be process or job IDs
bash: kill: -i: arguments must be process or job IDs
bash: kill: (6667) - No such process
root@metasploitable:/home/msfadmin# lsof -i :6667
COMMAND    PID USER   FD   TYPE DEVICE SIZE NODE NAME
unrealirc 4637 root    2u  IPv4  12242       TCP *:ircd (LISTEN)
root@metasploitable:/home/msfadmin# kill 4637
root@metasploitable:/home/msfadmin# _
```

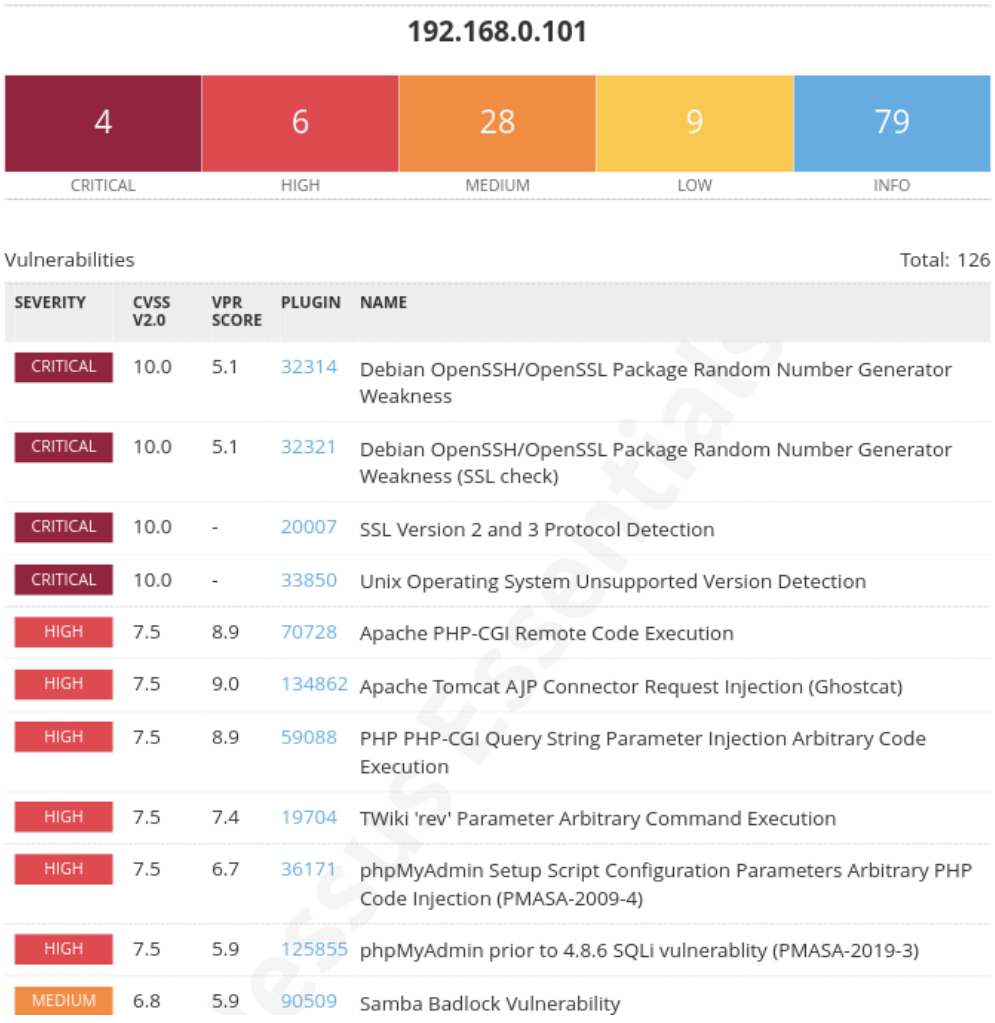
Per risolvere la vulnerabilità legata a questa backdoor, tramite i privilegi di –root, identifichiamo quali processi sono attivi sulla porta 6667 e ne forziamo l'arresto, successivamente andremo a rimuovere "unrealircd service". Eseguiamo questi comandi da terminale, sulla macchina Metasploitable:

- lsof -i :6667
- kill (numero del processo attivo) 4637 (in questo caso)
- rm unrealircd.conf (dalla directory /etc/unreal)

```
root@metasploitable:/etc/unreal# ls
aliases               dccallow.conf  ircd.pid   spamfilter.conf
badwords.channel.conf doc            ircd.tune  tmp
badwords.message.conf Donation       LICENSE    unreal
badwords.quit.conf    help.conf      modules    unrealircd.conf
curl-ca-bundle.crt    ircd.log       networks
root@metasploitable:/etc/unreal# rm unrealircd.conf
root@metasploitable:/etc/unreal#
```

Quindi riavviare la macchina.

A questo punto, ripetiamo lo scanning con Nessus, per verificare che tutte le vulnerabilità siano state sanate correttamente.



192.168.0.101

4	6	28	9	79
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 126

SEVERITY	CVSS V2.0	VPR SCORE	PLUGIN	NAME
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	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
HIGH	7.5	8.9	70728	Apache PHP-CGI Remote Code Execution
HIGH	7.5	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
HIGH	7.5	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	7.5	6.7	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
HIGH	7.5	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
MEDIUM	6.8	5.9	90509	Samba Badlock Vulnerability

Come possiamo vedere, non sono più presenti nelle vulnerabilità CRITICAL o HIGH.

E nemmeno, come negli screen successivi, nelle vulnerabilità medie.

MEDIUM	6.4	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	-	57582	SSL Self-Signed Certificate
MEDIUM	6.1	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.8	-	42263	Unencrypted Telnet Server
MEDIUM	5.0	-	11411	Backup Files Disclosure
MEDIUM	5.0	-	40984	Browsable Web Directories

MEDIUM	5.0	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
MEDIUM	5.0	-	46803	PHP expose_php Information Disclosure
MEDIUM	5.0	-	57608	SMB Signing not required
MEDIUM	5.0	-	15901	SSL Certificate Expiry
MEDIUM	5.0	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	5.0	-	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	5.0	-	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)
MEDIUM	4.3	4.4	136808	ISC BIND Denial of Service
MEDIUM	4.3	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	4.3	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	3.7	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3	3.8	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	4.3	3.0	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)
MEDIUM	4.0	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	4.0	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
LOW	2.6	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	-	153953	SSH Weak Key Exchange Algorithms Enabled