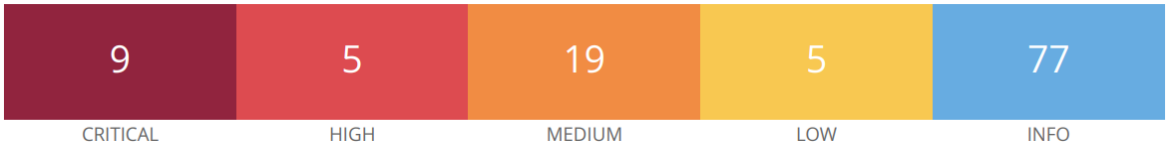
Prova pratica 2-24-23

Vulnerability Remediation sul target Metasploitable192.168.30.200



Come possiamo vedere dall'immagine sopra, la macchina presenta varie criticità (115) sfruttabili da un attaccante mettendo a rischio l'integrità e la sicurezza dei dati che contiene.

In particolare in questo esercizio ci concentreremo sul rimedio delle vulnerabilità più pericolose indicate come "critical", questo tipo in particolare rappresenta una famiglia di debolezze note, facilmente sfruttabili e potenzialmente molto dannose, una volta risolte quelle gravi anche alcune di quelle di livello inferiore dovrebbero risolversi a cascata (es. risolvendo un problema critico legato all'alta visibilità anche tutte le info che dipendono da quella breccia verranno risolte di conseguenza).

Nonostante le vulnerabilità di livello alto vadano risolte tempestivamente non bisogna tralasciare quelle di livello più basso che, seppur non rappresentino un potenziale danno diretto, potrebbero dare informazioni circa i nostri sistemi quindi facilitare l'adattamento dei tool di attacco verticalizzando la minaccia su una falla di cui l'attaccante ha molte informazioni ponendo a serio rischio la sicurezza del sistema stesso.

CRITICAL

É possibile accedere alle condivisioni del Network File System dell host.
Con questa falla un attaccante potrebbe accedere al sistema quindi leggere e modificare file direttamente sull'host remoto.

```
  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.
#

IP:192.168.50.30_
```

```
  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: ALL
```

Per la risoluzione di questo problema ho optato per la configurazione manuale del servizio NFS, nello specifico sono andato a modificare il file hosts.deny bloccando tutte le connessioni in entrata, successivamente ho scritto nel file hosts.allow una regola per cui solo gli ip specificati sono autorizzati a compiere azioni di file sharing.

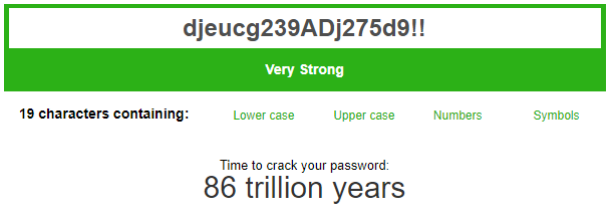
CRITICAL

La password del servizio Virtual Network Computing non è sicura.
Dato che la password è "password" un attaccante potrebbe facilmente scoprirla ed usarla per prendere il controllo remoto della macchina.

```
  GNU nano 2.0.7            File: passwd                  Modified

djeucg239ADj275d9!!
```

Per eliminare il rischio di bruteforce sul VNC ho impostato una password superiore ai 12 caratteri contenente anche simboli, maiuscole e numeri.



Affidandoci a questo servizio online possiamo constatare che una password del genere richiederebbe un tempo a dir poco eccessivo per essere scoperta da un comune programma di bruteforce, l'unico modo per compromettere questa sequenza sarebbe un errore umano da parte del proprietario o eventualmente uno spyware installato nella macchina. (si consiglia l'uso di un password manager per immagazzinare la stringa)

CRITICAL

Una Bind Shell è in ascolto su una porta, questa vulnerabilità potrebbe essere sfruttata da un attaccante per lanciare comandi bash da remoto andando ad intaccare in maniera diretta sul sistema.

```
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  tcpwrapped
22/tcp   open  ssh?
23/tcp   open  telnet?
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?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  tcpwrapped
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix
```

Questa immagine porta in evidenza il fatto che la porta 1524 è in ascolto con il servizio attivo di root bindshell, è bastato uno scan nmap -sV per ottenere questa informazione e rappresenta sicuramente un vettore di attacco critico da risolvere.

Perciò ho deciso di chiudere la porta e abbattere il servizio, un'alternativa sarebbe stata di fare port filtering aggiungendo una regola al firewall.

```
msfadmin@metasploitable:~$ sudo fuser -k 1524/tcp
[sudo] password for msfadmin:
1524/tcp:             4415
msfadmin@metasploitable:~$ _
```

```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh?
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)
1099/tcp open  java-rmi    GNU Classpath grmiregistry
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  tcpwrapped
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)
```

Questa evidenza riporta il risultato di una seconda scansione nmap, quindi notiamo la mancanza della porta con il servizio in causa.

CRITICAL

Il servizio rexecd serve per l'esecuzione di comandi da remoto da parte di utenti della stessa rete, ma al contempo non fornisce un grado di sicurezza sufficiente, appunto un attaccante potrebbe sfruttarlo a suo favore per lanciare comandi nella shell.

```
  GNU nano 2.0.7            File: /etc/inetd.conf                      Modified

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
#exec           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i
```

La soluzione più sicura sarebbe togliere il servizio direttamente dai file di configurazione, ma se lo si ritiene necessario, basta inserire una regola nel firewall filtrando il traffico in entrata da quella porta autorizzando solo ip noti.

CRITICAL

Per le ultime tre criticità (sistema operativo non supportato, servizio SSL obsoleto e server Tomcat deprecato) si consiglia un aggiornamento alle ultime versioni seguendo le norme e consigli del distributore ponderandoci sulla nostra disponibilità economica e tecnica.

Lasciare sistemi obsoleti sulla macchina pone l'integrità della stessa in serio pericolo dato che finito il supporto da parte della casa produttrice tutti gli exploit scoperti successivamente, accessibili da chiunque online, non verranno mai corretti ponendoci in una lampante situazione di vulnerabilità considerando il fatto che facendo una scansione attiva sul sistema chiunque può capire quale tipo di software gira sulla nostra macchina.

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-02-24T08:58:32-05:00

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.88 seconds
```

Appunto gli sviluppatori di questo sistema operativo hanno terminato il suo supporto oltre 12 anni fa, e facendo una semplice ricerca su internet si possono trovare più di 200 vulnerabilità note più o meno pericolose.

CONCLUSIONI

Di seguito riporto l'evidenza di come le azioni di remediation siano state efficaci ad eliminare almeno in parte i rischi maggiori per la sicurezza del sistema (tralasciando le vulnerabilità che richiedono aggiornamenti), e come prima accennato possiamo notare la risoluzione a cascata di vulnerabilità di livello più basso che si basavano su una o più falle nei punti critici.

prima

9	5	19	5	77
CRITICAL	HIGH	MEDIUM	LOW	INFO

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	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*	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*	61708	VNC Server 'password' Password
CRITICAL	10.0*	10203	rexecd Service Detection
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	42256	NFS Shares World Readable
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability
HIGH	7.5*	10205	rlogin Service Detection
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	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

dopo

4	3	17	2	60
CRITICAL	HIGH	MEDIUM	LOW	INFO

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	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*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	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	136808	ISC BIND Denial of Service
MEDIUM	5.9	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	12085	Apache Tomcat Default Files