

Benchmark M3

esercitazione finale modulo 3

Ignazio Saba

INTRODUZIONE

In questo benchmark dovremmo effettuare delle scansioni, tramite Nessus, verso una macchina target “meta” da una macchina attaccante “Kali” passando attraverso un firewall gestito da “pfsense”

fatte le scansioni valutare le vulnerabilità trovate e risolverne alcune

configurazioni

pfsense farà da firewall è configurato con una porta WAN e due LAN
la WAN è lasciata in dhcp in modo di avere libero accesso a internet

LAN kali IP: 192.168.32.1

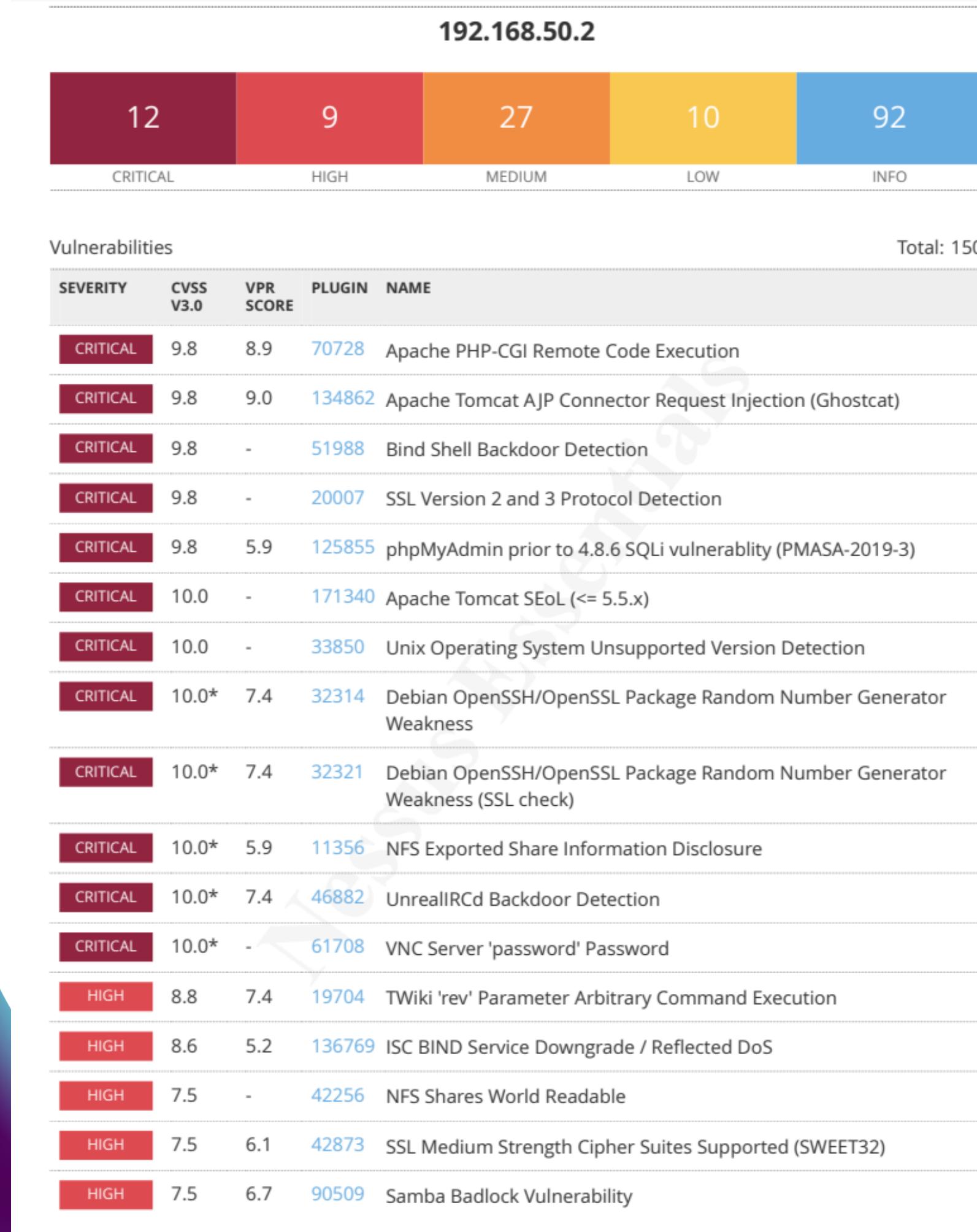
LAN METASPLOIT IP: 192.168.50.1

kali e meta saranno anch'essi in dhcp ma su lan differenti gestite da PFsense

IP KALI: 192.168.32.10

IP META: 192.168.50.2

tutte le macchine si vedono in rete e hanno accesso a internet



SCANSIONE NESSUS

lista compatta delle vulnerabilità trovate
le vulnerabilità riguardanti tomcat
sono state risolte con il comando
“ apt-get install update e apt-get
upgrade”
di cui purtroppo non ho screen a
causa delle ridotte righe di comando
visibili su metasploit

Modifica password VNC

```
msf6 > use 0
[!] (kali㉿kali)-[~] iured, defaulting to windows/meterpreter/reverse_tcp
└─$ vncviewer 192.168.50.2:5900 [cclient] > use 1
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication -h" for more information
Password:ary(scanner/vnc/vnc_login) > show options
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel. [rent Setting] Required Description
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format: o Try blank pass
 32 bits per pixel. [SPEED 5] yes How fast to bring up the screen
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
vncviewer: VNC server closed connection
DB_SKIP_EXISTING none
[!] (kali㉿kali)-[~]
└─$ vncviewer 192.168.50.2:5900 [loit-framework/data/wordlists/vnc_pass]

TX packets:3876 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:299097 (292.0 KB) TX bytes:834066 (814.5 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:4167 errors:0 dropped:0 overruns:0 frame:0
TX packets:4167 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2002913 (1.9 MB) TX bytes:2002913 (1.9 MB)

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)? n
root@metasploitable:/home/msfadmin# _
```

NFS

```
GNU nano 2.0.7           File: exports

# /etc/exports: the access control list for filesystems which
#                 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,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
# *(rw,sync,no_root_squash,no_subtree_check)

[ Wrote 12 lines ]

root@metasploitable:/etc#
```

rinominato il file exports originale e
ricreato vuoto

Bind Shell backdoor

sulla macchina meta veniva esposta una porta la 1524 si procede con iptables a creare una regola che blocca il traffico su quella porta dall'indirizzo di kali

```
vmlinuz Modules
whoami=====
root
# Name          Disclosure Date Rank Check Description
└─(kali㉿ kali)-[~/Documents/test]─
└─$ nmap -sV 192.168.50.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-28 04:36 EST
Nmap scan report for 192.168.50.2
Host is up (0.00081s 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/vnc/vnc_login:
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)      yes  Attempt to login with a blank username and password
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   fanetkit-rsh rexecd  no   Try each user/password couple stored in the current database
513/tcp   open  login  OpenBSD or Solaris rlogind no   Add all passwords in the current database to the list
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry no   Skip existing credentials stored in the current database (Accepts connections from Java RMI)
1524/tcp  open  bindshell Metasploitable root shell  The password to test
2049/tcp  open  nfs    /s 2-4 (RPC #100003) mework/data/wordlists/vnc_passwords.txt no   File containing passwords, one per line
2121/tcp  open  ftp    ProFTPD 1.3.1      no   A proxy chain of format type:host:port[,type:host:port][...]
3306/tcp  open  mysql  MySQL 5.0.51a-3ubuntu5  The target host(s), see https://docs.metasploit.com/docs/using-metasploit
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7  The target port (TCP)
5900/tcp  open  vnc    VNC (protocol 3.3)  yes  Stop guessing when a credential works for a host
6000/tcp  open  X11   (access denied)      yes  The number of concurrent threads (max one per host)
6667/tcp  open  irc    UnrealIRCd      no   A specific username to authenticate as
8009/tcp  open  ajp13?
8180/tcp  open  unknown
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
VERBOSE: true
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 188.95 seconds
View the full module info with the info or info command
```

Bind Shell backdoor

```
root@metasploitable:~#  
root@metasploitable:~# iptable -L  
bash: iptable: command not found  
root@metasploitable:~# iptables -L  
Chain INPUT (policy ACCEPT)  
target     prot opt source          destination  
  
Chain FORWARD (policy ACCEPT)  
target     prot opt source          destination  
  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source          destination  
root@metasploitable:~# iptables -A INPUT -p tcp -s 192.168.32.10 --dport 1524 -j  
    DROP  
root@metasploitable:~# iptables -L  
Chain INPUT (policy ACCEPT)  
target     prot opt source          destination  
DROP      tcp   --  192.168.32.10      anywhere            tcp  dpt:ingreslock  
  
Chain FORWARD (policy ACCEPT)  
target     prot opt source          destination  
  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source          destination  
root@metasploitable:~#
```

creata regola sulle
iptables che impedisce
all'indirizzo di kali
192.168.32.10 di
raggiungere la porta
1524

Bind Shell backdoor

una nuova scansione di
nmap mostra come la
porta ora sia filtrata

```
(kali㉿kali)-[~/Documents/test] normal No VNC Authentication Scanner
$ nmap -sV 192.168.50.2 nmap_http_get 2001-01-29 average No WinVNC Web Server GET Overflow
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-28 05:06 EST
Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.91% done; ETC: 05:08 (0:00:07 remaining) exploit/windows/vnc/winvnc_http_get
Stats: 0:02:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.48% done; ETC: 05:09 (0:00:00 remaining)
Nmap scan report for 192.168.50.2
Host is up (0.00076s latency). (at port 22)
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  vsftpd  3.4.2
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 rexec
513/tcp   open  login  nis
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  /nfs share 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   ircd UnrealIRCd
8009/tcp  open  ajp13?
8180/tcp  open  unknown
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
VERBOSE: true
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 190.01 seconds
View the full module info with the info, or info -d command.
```



Vulnerabilities

Total: 136

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
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	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	6.7	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

nuova scansione nessus

come s può vedere dalla nuova scansione le vulnerabilità sono diminuite, non solo quelle critiche ma anche quelle di minore importanza sicuramente dipendenti da quelle con un cvss più alto