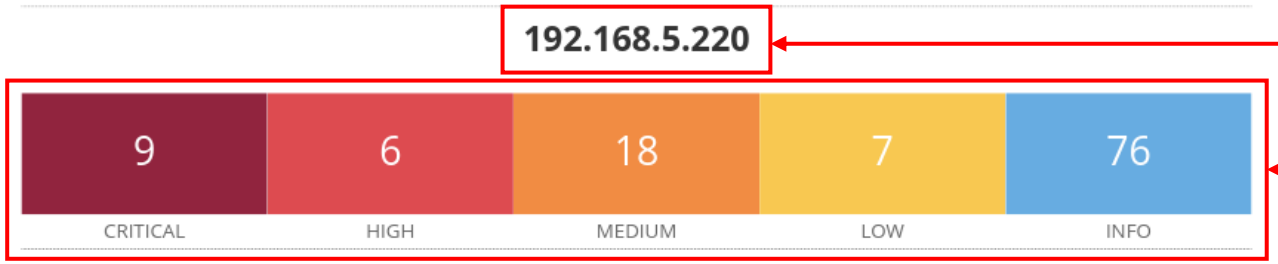
CONSEGNA SETTIMANA 5 LEZIONE 5

Scansione e risoluzione delle vulnerabilità

La richiesta di oggi prevede la scansione della macchina metasploitable tramite il software Nessus e la risoluzione di 4 vulnerabilità di livello critico/alto.
Prendiamo in esame la seguente schermata recuperata dal report di Nessus:



Vulnerabilities — Total: 116

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	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	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
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*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Indirizzo IP della macchina target

Numero delle vulnerabilità differenziato per livello di importanza (da *critical* a *low* + *INFO*)

Vulnerabilità totali di livello critico con relativo punteggio CVSS (sistema di valutazione del rischio informatico)

Da questa schermata possiamo notare che la macchina metasploitable porta con sè un elevato numero di vulnerabilità che potrebbero essere utilizzate da un ipotetico individuo malintenzionato per un attacco.
Da questo elenco ho selezionato 3 vulnerabilità da prendere in esame e risolvere:

- *Bind Shell Backdoor Detection*
- *Debian OpenSSH/OpenSSL Package Random Number Generator Weakness*
- *VNC Server "password" Password*

CONSEGNA SETTIMANA 5 LEZIONE 5

Scansione e risoluzione delle vulnerabilità

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -T5 -p 1524 192.168.5.220
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 05:24 EST
Nmap scan report for 192.168.5.220
Host is up (0.00032s latency).

PORT     STATE SERVICE   VERSION
1524/tcp open  bindshell Metasploitable root shell
MAC Address: 08:00:27:BB:C6:4D (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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

TRACEROUTE
HOP RTT     ADDRESS
1   0.32 ms 192.168.5.220

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
```

DESCRIZIONE DELLA VULNERABILITA'

La vulnerabilità *Bind Shell Backdoor Detection* fa riferimento ad una porta aperta dove la macchina è in ascolto e può ricevere comandi di root.
Per poter trovare la porta corretta possiamo usare **nmap** tramite una scansione aggressiva e trovare il servizio associato
(nel nostro caso bindshell).
Un malintenzionato potrebbe tramite il comando **netcat** [IP] [PORT] collegarsi a metasploitable e istruire comandi di root.

RISOLUZIONE

Una possibile risoluzione è quella di bloccare l'accesso alla porta tramite il firewall (nel nostro caso **PfSense**) oppure tramite le **IpTables** interne alla macchina.

CONCLUSIONE

A questo punto non sarà più possibile connettersi alla porta e la vulnerabilità è stata risolta.

CONSEGNA SETTIMANA 5 LEZIONE 5

Scansione e risoluzione delle vulnerabilità

CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

DESCRIZIONE DELLA VULNERABILITA'

La vulnerabilità *Debian OpenSSH/OpenSSL Package Random Number Generator Weakness* fa riferimento ad un errore nelle chiavi di crittazione di OpenSSH. In questo caso particolare, la versione che genera le chiavi produce delle sequenze numeriche facilmente prevedibili e pertanto facili da poter aggirare.

RISOLUZIONE

Un ipotetico metodo di risoluzione è quello di eliminare le chiavi di crittazione all'interno della macchina (presenti nella sottocartella */etc/ssh/ssh_host_**) con il comando **rm**, per poi rigenerarle tramite il comando **dpkg-reconfigure openssh-server**. In questo modo le chiavi di crittazione verranno rigenerate con un sistema parzialmente aggiornato (tramite il comando **sudo apt-get update** e **sudo apt-get upgrade**).

CONCLUSIONE

A questo punto le chiavi di crittazione non saranno più facilmente prevedibili e la vulnerabilità è stata risolta.

CONSEGNA SETTIMANA 5 LEZIONE 5

Scansione e risoluzione delle vulnerabilità

CRITICAL	10.0*	-	61708	VNC Server 'password' Password

DESCRIZIONE DELLA VULNERABILITA'

La vulnerabilità *VNC Server 'password' Password* fa riferimento alla password di default del Server VNC (le vnc sono applicazioni per l'accesso da remoto al proprio computer, pertanto una possibile via facilitata per eventuali malintenzionati se non configurate a dovere).

In questo caso la password di default è 'password' ,facilmente prevedibile e quindi un grande rischio per la sicurezza della macchina.

RISOLUZIONE

Una possibile soluzione, per mantenere attivo il servizio di accesso da remoto, è quella di entrare nella macchina metasploitable come amministratore (con il comando **sudo su**) e modificare la password tramite il comando **vncpasswd**.

CONCLUSIONE

A questo punto non sarà più possibile accedere da remoto con la password di default e la vulnerabilità è stata risolta.

CONSEGNA SETTIMANA 5 LEZIONE 5

Scansione e risoluzione delle vulnerabilità

192.168.5.220

8	6	19	7	78
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 118

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	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

IN CONCLUSIONE

Possiamo notare che le 3 vulnerabilità presenti all'interno della macchina sono sparite dal report di Nessus.
Allo stesso tempo però ne sono state rilevate ulteriori che richiederanno diversi metodi di risoluzione per poterle eliminare o quanto meno ridurre il loro impatto sulla sicurezza informatica.

ULTERIORI CONSIDERAZIONI

Alcune ulteriori soluzioni possibili riguarderanno sicuramente regole da impostare nel firewall e l'aggiornamento della macchina target, in quanto gli aggiornamenti spesso sono utili a ridurre le vulnerabilità del sistema.
Inoltre, sarebbe consigliabile la disabilitazione dei protocolli SSL v.2 e v.3 (in quanto ormai datati e con vulnerabilità evidenti) e la sostituzione con protocolli più recenti come il TLS v.1.2