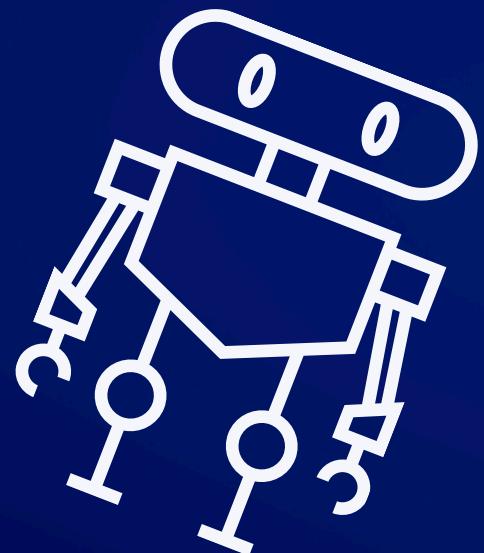
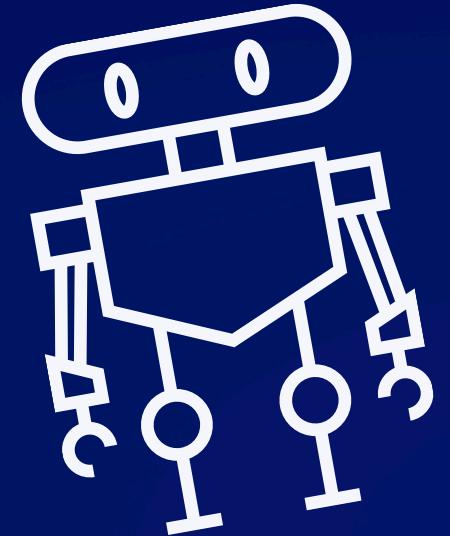




Vulnerability Assessment

55/L5

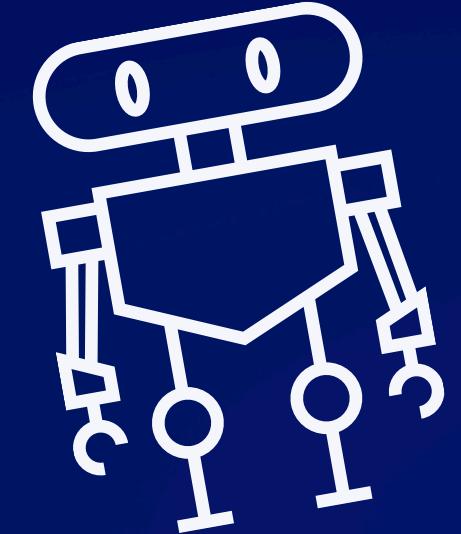
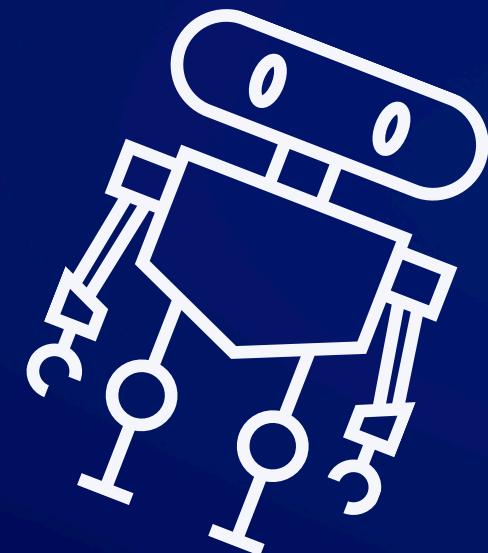


Mara Dello Russo



Vulnerability Assessment

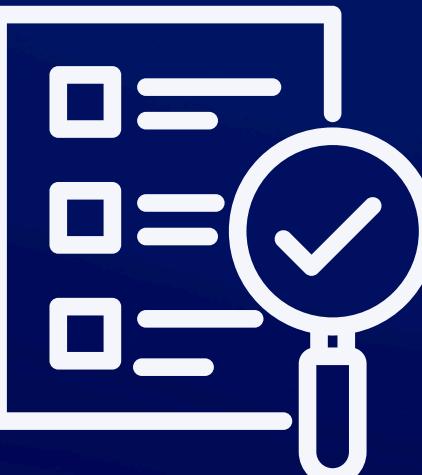
INTRODUZIONE





Cos'è un Vulnerability Assessment?

Una valutazione della vulnerabilità, Vulnerability Assessment, è un processo finalizzato a **identificare, quantificare e classificare** le vulnerabilità nei sistemi informatici, nelle reti, nelle infrastrutture o in altri asset. Questo processo può coinvolgere l'analisi delle vulnerabilità di sicurezza, dei rischi associati e delle possibili conseguenze di un'eventuale sfruttamento delle vulnerabilità. Inoltre, una valutazione delle vulnerabilità può includere raccomandazioni per mitigare o eliminare le vulnerabilità rilevate al fine di migliorare la sicurezza complessiva del sistema o dell'organizzazione. Un Vulnerability Assessment si può eseguire sia localmente che da remoto. Vista la numerosità di servizi noti, testare manualmente i sistemi per cercare le vulnerabilità sarebbe poco praticabile, quindi i penetration tester usano degli strumenti chiamati **Vulnerability Scanner** per automatizzare i test sui target. Nella scansione presentata in questo progetto utilizzeremo Nessus.



Vulnerabilità

Le vulnerabilità sono catalogate dal SANS Institute attraverso dei codici chiamati CVE (Common Vulnerabilities and Exposures). Es. “Apache Tomcat AJP Connector Request Injection”, o Ghostcat, è identificata come CVE-2020-1938.

Alcune delle principali categorie di vulnerabilità trattate dal SANS Institute includono:

- **Vulnerabilità di software:** possono includere falle di sicurezza e errori di programmazione nei sistemi operativi, nelle applicazioni software e nei servizi di rete.
- **Vulnerabilità di configurazione:** le configurazioni errate o non sicure possono creare punti deboli nei sistemi e nelle reti. Possono includere password deboli, autorizzazioni eccessive, mancata installazione di patch di sicurezza.
- **Vulnerabilità di rete:** riguardano le debolezze nelle infrastrutture di rete, come router, switch, firewall e dispositivi di sicurezza.
- **Vulnerabilità web:** le applicazioni web possono essere vulnerabili a una varietà di minacce, come ad esempio injection di codice (SQL injection, XSS), autenticazione e gestione delle sessioni non sicure, esposizione di dati sensibili e altri problemi che possono compromettere la sicurezza e la privacy degli utenti.
- **Vulnerabilità mobile:** possono includere vulnerabilità di sicurezza nel software delle app, accesso non autorizzato ai dati dell'utente e problemi legati alla gestione remota dei dispositivi

Nessus

Nessus è uno dei software più noti e utilizzati per la scansione e la valutazione della sicurezza dei sistemi informatici. Si tratta di uno **strumento di analisi delle vulnerabilità** che aiuta ad identificare e mitigare i rischi per la sicurezza nelle reti, nei sistemi e nelle applicazioni.

Nessus è in grado di eseguire scansioni automatiche dei dispositivi connessi in rete per individuare eventuali vulnerabilità note, come falle di sicurezza, configurazioni non sicure e altri problemi che potrebbero essere sfruttati da potenziali aggressori. Il software fornisce anche dettagliate relazioni sulle vulnerabilità rilevate, consentendo agli utenti di comprendere meglio i rischi e prendere misure correttive per migliorare la sicurezza del sistema.

Nessus è formato da:

- un client: viene utilizzato per configurare le scansioni: indicare i target IP, le modalità di scansione ed i test da lanciare.
- un server: si occupa di effettuare i veri e propri test sugli obiettivi specificati all'interno delle scansioni configurate dal client.

Dopo aver eseguito le scansioni il server confronta le risposte con il proprio database di vulnerabilità.

Report delle vulnerabilità rilevate da Nessus con un Basic Network Scan

→ IP Metasploitable

192.168.1.101

CRITICAL: 8 | HIGH: 4 | MEDIUM: 18 | LOW: 7 | INFO: 71

Vulnerabilities				
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	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	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability
MEDIUM	6.8	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
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
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	4.4	136808	ISC BIND Denial of Service

MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
			192.168.1.101	
MEDIUM	5.9	4.4	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	21196	AIR Connector Detection

Parametri Report

- **Severity:** La severità di una vulnerabilità indica il grado di rischio e di danno potenziale che una vulnerabilità può causare quando viene sfruttata
- **CVSS:** fornisce una valutazione numerica della gravità della vulnerabilità. il range numerico utilizzato è 0-10
- **VPR Score:** è un indice numerico che indica la priorità della minaccia, cioè aiuta a prioritizzare le azioni di mitigazione e risolvere le vulnerabilità più critiche in modo tempestivo.
- **Plugin:** sono identificatori univoci associati alle regole e ai controlli specifici eseguiti durante la scansione. ogni plugin è progettato per individuare una particolare vulnerabilità.
- **Nome:** nome della vulnerabilità rilevata.

REMEDIATION DELLE VULNERABILITA'



Nelle slide successive vedremo come
risolvere alcune delle vulnerabilità
riscontrate.

Bind Shell Backdoor Detection

Descrizione:

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione:

questaShell remota si trova in ascolto sulla porta 1524. Per interrompere questo accesso non autorizzato al sistema creiamo una **rule firewall** che blocchi il servizio su quella porta.

Possiamo effettuare un nmap sulla metasploitable per vedere effettivamente il servizio attivo sulla porta 1524.
Per una migliore visibilità lo effettuiamo dalla console msf6 su Kali Linux

```
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
[*] exec: nmap 192.168.1.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 23:48 CEST
Nmap scan report for 192.168.1.101
Host is up (0.0046s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score 9.8

Nmap done: 1 IP address (1 host up) scanned in 14.43 seconds
[*] exec: service ingreslock stop
[*] exec: service ingreslock stop
CVSS v2.0 Base Score 10.0
```

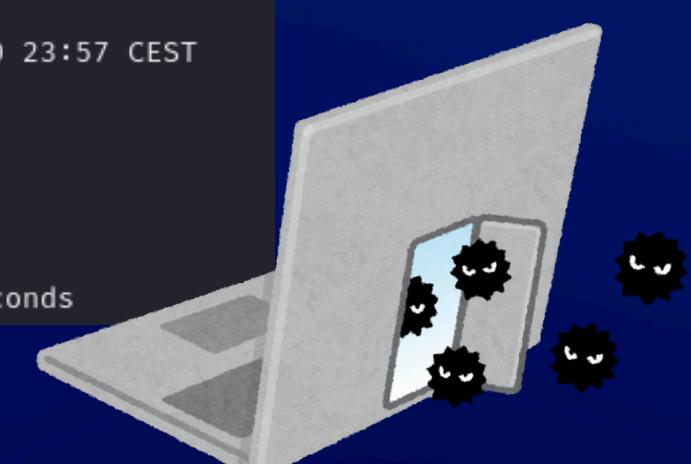
Dopo aver inserito una rule firewall su metasploitable con
sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
ricontrolliamo la porta 1524 e otterremo lo stato della porta
come "filtered". Abbiamo interrotto l'accesso.

```
msf6 > nmap 192.168.1.101 -p 1524
[*] exec: nmap 192.168.1.101 -p 1524

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 23:57 CEST
Nmap scan report for 192.168.1.101
Host is up (0.0035s latency).

PORT      STATE SERVICE
1524/tcp  filtered ingreslock

Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
```



Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Descrizione:

La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the middle.

Soluzione:

Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

```
msfadmin@metasploitable:~$ sudo rm -rf /etc/ssh/ssh_host_*
msfadmin@metasploitable:~$ sudo dpkg-reconfigure openssh-server
Creating SSH2 RSA key: this may take some time ...
Creating SSH2 DSA key: this may take some time ...
* Restarting OpenBSD Secure Shell server sshd [ OK ]
```

```
msfadmin@metasploitable:~$ sudo rm -rf /etc/apache2/ssl/*
msfadmin@metasploitable:~$ sudo mkdir /etc/apache2/ssl
msfadmin@metasploitable:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
Generating a 2048 bit RSA private key
.
.
.
writing new private key to '/etc/apache2/ssl/apache.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:
```

- **rm -rf /etc/ssh/ssh_host_***: rimuove ricorsivamente e in modo forzato tutti i file che corrispondono al pattern **/etc/ssh/ssh_host_*** nella directory **/etc/ssh/**.
- **dpkg-reconfigure openssh-server**: è un comando utilizzato per riconfigurare i pacchetti del sistema installati tramite dpkg, e openssh-server è il pacchetto che gestisce il server SSH. Verranno quindi ricreate delle nuove SSH key

- **rm -rf /etc/apache2/ssl/***: rimuove ricorsivamente e in modo forzato tutti i file e le directory all'interno della directory **/etc/apache2/ssl/**.
- **mkdir /etc/apache2/ssl**: crea una nuova directory di nome **ssl** all'interno della directory **/etc/apache2**.
- **openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt**: crea un nuovo certificato SSL auto-firmato con durata di 365 giorni e una chiave privata RSA di 2048 bit.

VNC Server 'password' Password

Descrizione:

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.

Soluzione:

• Proteggi il servizio VNC con una password complessa.

Eseguiamo il comando **vncpasswd** ed inseriamo
una password **COMPLESSA**

```
root@metasploitable:~# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:~# _
```

NFS Exported Share Information Disclosure

Descrizione:

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

Soluzione:

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

```
# /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,async)
#
/home 192.168.1.100(rw,async,no_root_squash,no_subtree_check)
```

Apriamo il file **exports** situato in **/etc/**, troveremo un'unica riga senza commento che consentirà l'ingresso a qualsiasi indirizzo ip a tutte le directory del sistema con i permessi in parentesi:

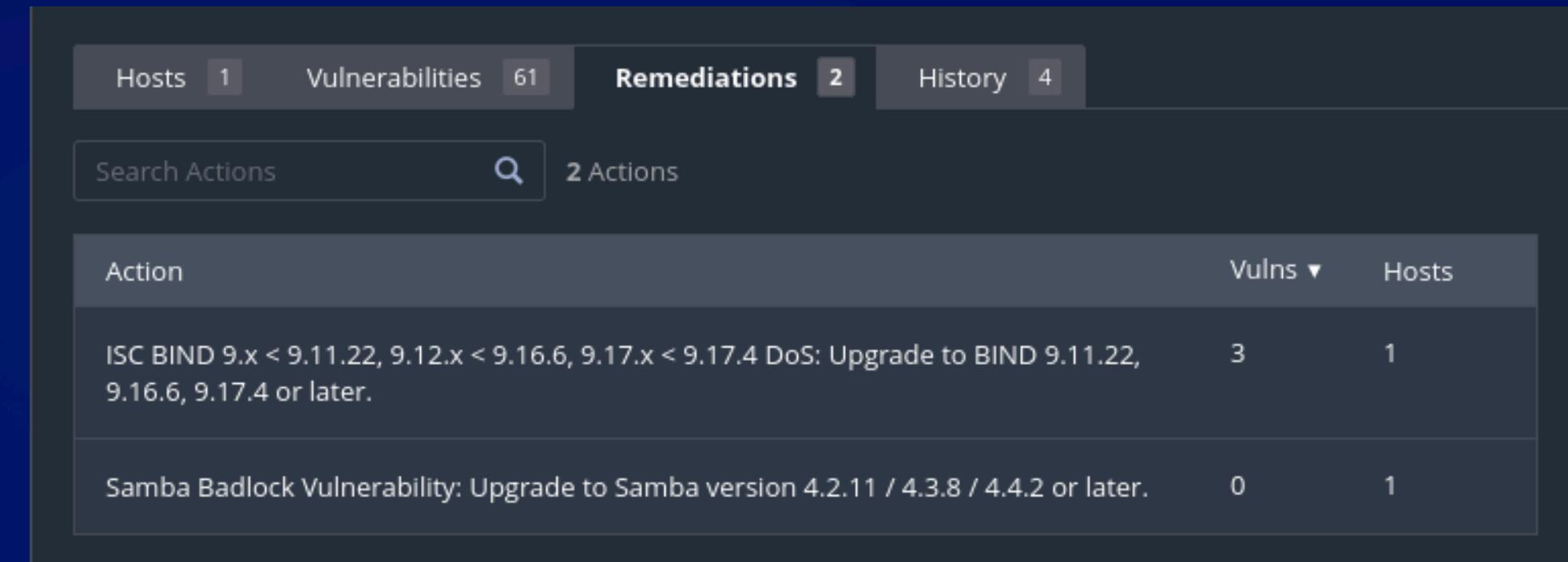
/ *(rw, sync, no_root_squash,
no_subtree_check).

Bisogna modificare questa riga inserendo il percorso della directory in cui vogliamo consentire l'accesso e l'indirizzo o gli indirizzi IP autorizzati.

```
# /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.
#
ALL: 192.168.1.100
```

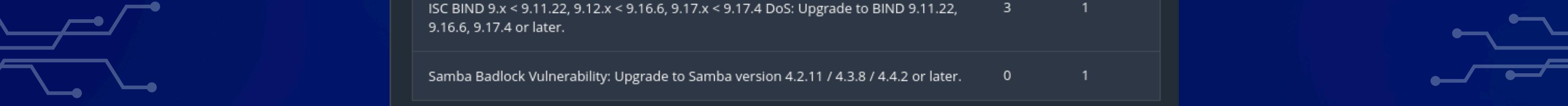
Nel file **hosts.allow** modifichiamo la riga con scritto **ALL:ALL**. Il primo ALL indica i servizi di sistema, mentre il secondo gli indirizzi IP autorizzati. Possiamo quindi scegliere quale(o quali) indirizzo IP autorizzare per quale servizio. Nell'esempio della figura sovrastante l'indirizzo IP 192.168.1.100 è autorizzato ad accedere a tutti i servizi del sistema.

Remediations Nessus



The screenshot shows the Nessus interface with the "Remediations" tab selected. There are two actions listed:

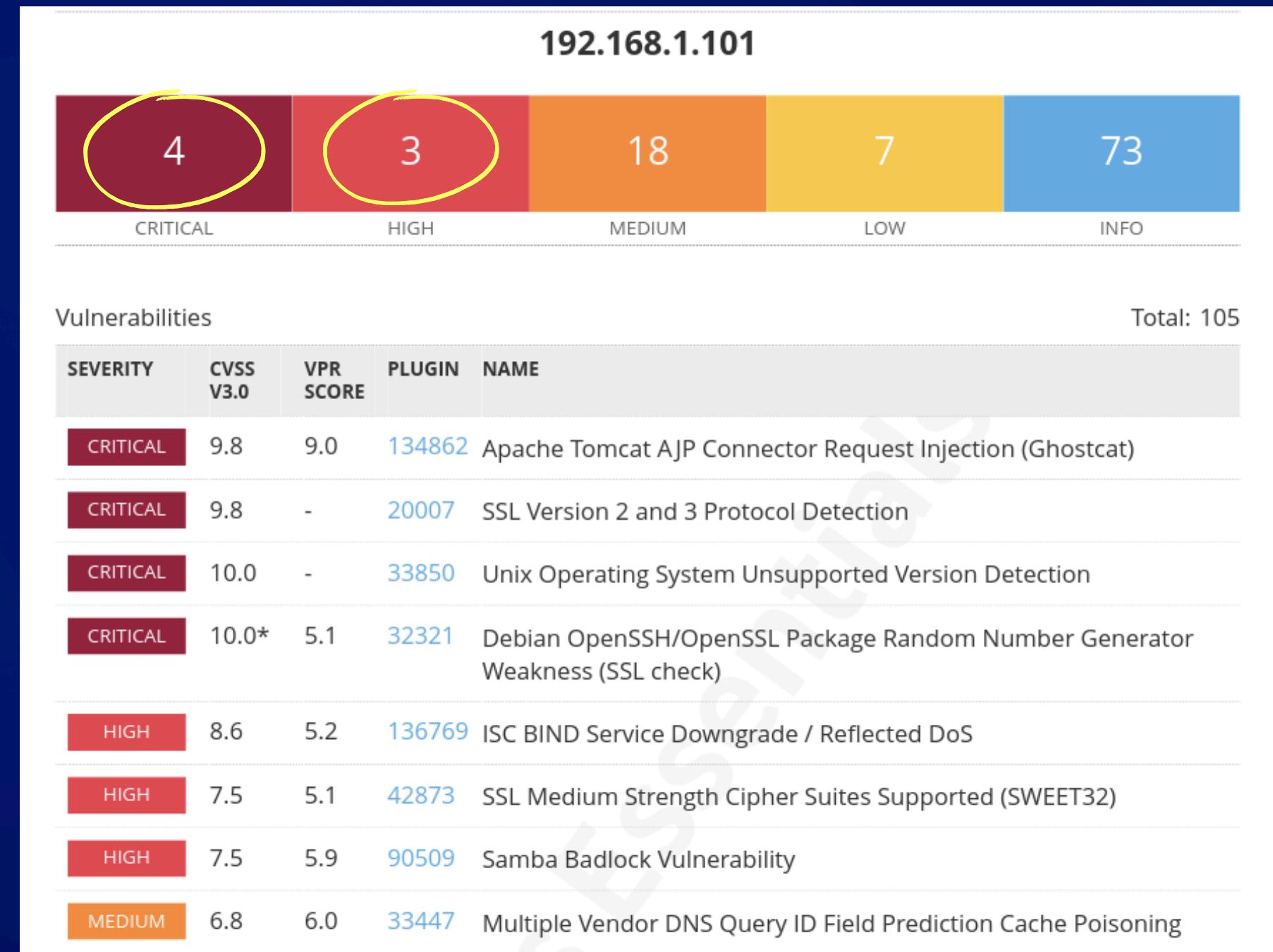
Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	0	1



Nella sezione “Remediations” Nessus ci consiglia di aggiornare BIND e Samba per risolvere due delle vulnerabilità riscontrate. Questo, essendo sempre su Metasploitable che è un ambiente di test, non è possibile a causa degli aggiornamenti non supportati. Vediamo almeno di cosa si tratta:

- ISC BIND: ISC BIND è un server DNS open source e una delle vulnerabilità più comuni e critiche associate ad esso è il "DNS cache poisoning". Questa vulnerabilità consente a un attaccante di iniettare record DNS malevoli nella cache di un server DNS, in modo che quando il server risponde a richieste DNS legittime, possa fornire risposte compromesse che dirigono il traffico verso server controllati dall'attaccante.
- Samba Badlock Vulnerability: la vulnerabilità Badlock è una vulnerabilità di tipo "man-in-the-middle" (MITM) che può consentire a un attaccante di eseguire un attacco di intercettazione sul traffico SMB (Server Message Block, protocollo utilizzato da Samba) tra client e server, permettendo potenzialmente di ottenere informazioni riservate o di alterare i dati in transito.

Scansione di Metasploitable con Nessus dopo aver risolto alcune delle vulnerabilità rilevate



GRAZIE PER
L'ATTENZIONE

