DATASHIELDS

S5-L5

WWW.DATASHIELDS.TECH

CONTENUTI

INTRODUZIONE

Partendo da uno scan iniziale eseguito con Nessus, abbiamo riscontrato diverse vulnerabilità.

Da queste criticità abbiamo testato le seguenti soluzioni:

REPORT NESSUS INIZIALE

metasploit

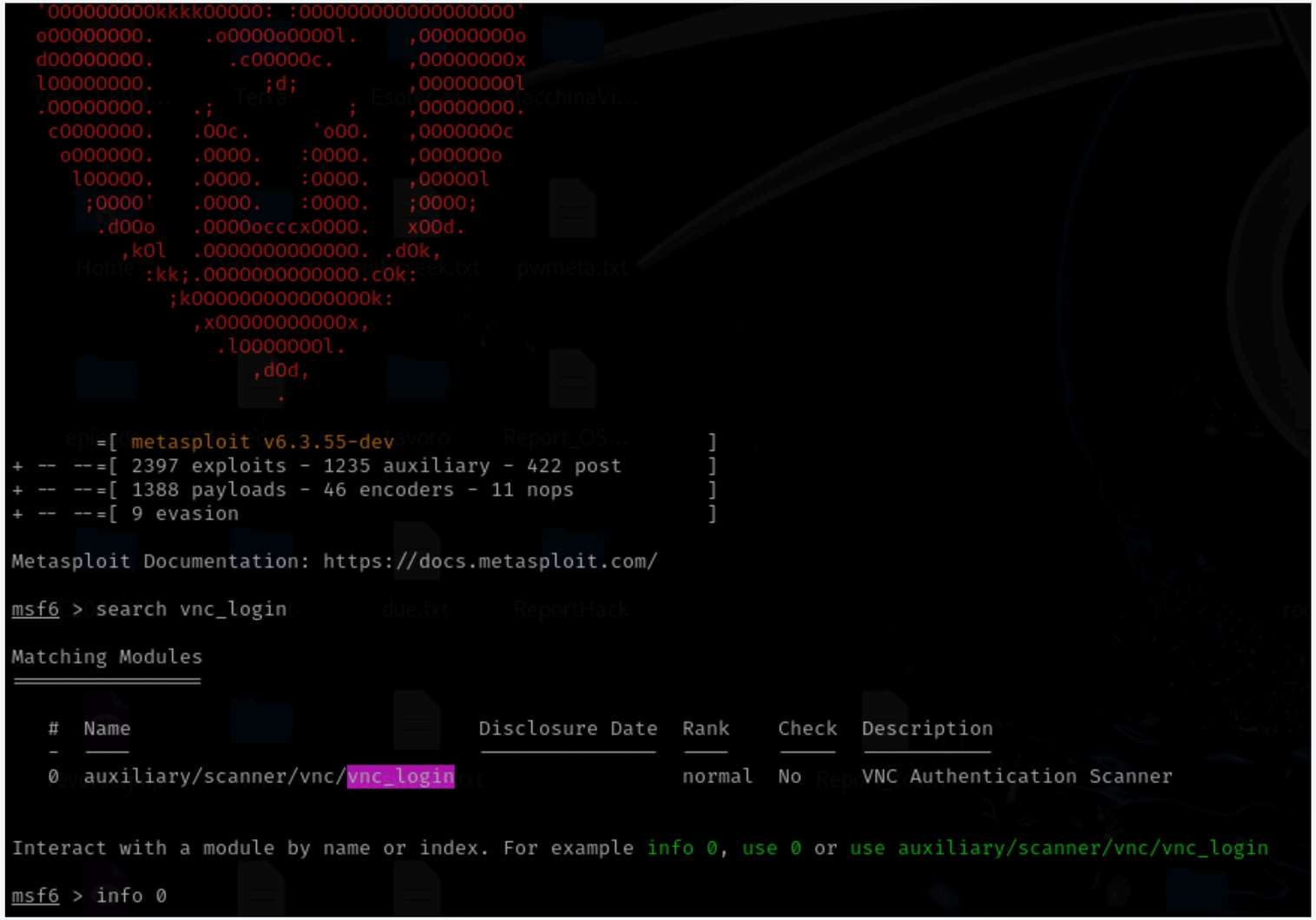
Vulnerabilities Total: 112

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	-	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*	-	61708	VNC Server 'password' Password

VNC SERVER ‘PASSWORD’ PASSWORD

- Il server VNC è protetto da una password molto debole.
- Nessus è stato in grado di accedere utilizzando come autenticazione la parola “password”.
- Il Virtual Network Computing (VNC) consente di visualizzare e controllare un computer a distanza, attraverso un altro PC o device portatile
- Un attaccante potrebbe colpire e prendere il controllo del server da remoto.
- Come soluzione proponiamo di cambiare la password mettendone una che rispetti le policy di sicurezza.

VNC SERVER



PRIMA DI AVVIARE LE NOSTRE MODIFICHE ABBIAMO VOLUTO TESTARE IL BRUTE FORCE PER COMPRENDERE IL LIVELLO DI DIFFICOLTA’

IL TOOL UTILIZZATO IN QUESTO CASO E’ IL FRAMEWORK DI METASPLOITABLE SU KALI LINUX

AVVIATO IL TOOL ABBIAMO MONTATO IL MODULO VNC_LOGIN

VNC SERVER

SUCCESSIVAMENTE ABBIAMO INSERITO LE **IMPOSTAZIONI** DEL MODULO **DEFINENDO IL TARGET** E **LA LISTA** PER IL **BRUTE FORCE**

```
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                      Required  Description
   ----              ---------------                      --------  -----------
   ANONYMOUS_LOGIN   false                                yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false                                no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                    yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                 no        Skip existing credentials stored in the current database (Acc
                                                                    epted: none, user, user&realm)
   PASSWORD                                               no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/da   no        File containing passwords, one per line
                     ta/wordlists/vnc_passwords.txt
   Proxies                                                no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                                                 yes       The target host(s), see https://docs.metasploit.com/docs/usin
                                                                    g-metasploit/basics/using-metasploit.html
   RPORT             5900                                 yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                yes       Stop guessing when a credential works for a host
   THREADS           1                                    yes       The number of concurrent threads (max one per host)
   USERNAME          <BLANK>                              no        A specific username to authenticate as
   USERPASS_FILE                                          no        File containing users and passwords separated by space, one p
                                                                    air per line
   USER_AS_PASS      false                                no        Try the username as the password for all users
   USER_FILE                                              no        File containing usernames, one per line
   VERBOSE           true                                 yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/vnc/vnc_login) > set rhost 192.168.5.101
rhost ⇒ 192.168.5.101
msf6 auxiliary(scanner/vnc/vnc_login) > show options
```

VNC SERVER

```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.5.101:5900    - 192.168.5.101:5900 - Starting VNC login sweep
[!] 192.168.5.101:5900    - No active DB -- Credential data will not be saved!
[+] 192.168.5.101:5900    - 192.168.5.101:5900 - Login Successful: :password
[*] 192.168.5.101:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

ABBIAMO LANCIATO IL BRUTE FORCE ED IN POCHI SECONDI ABBIAMO OTTENUTO LA PASSWORD

VNC SERVER RISOLUZIONE

SFRUTTANDO IL TOOL VNCVIEWER ABBIAMO APERTO LA GUI DI METASPLOITABLE E MODIFICATO LA PASSWORD CORRENTE CON UNA PIU' SICURA

```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.5.101
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  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:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

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

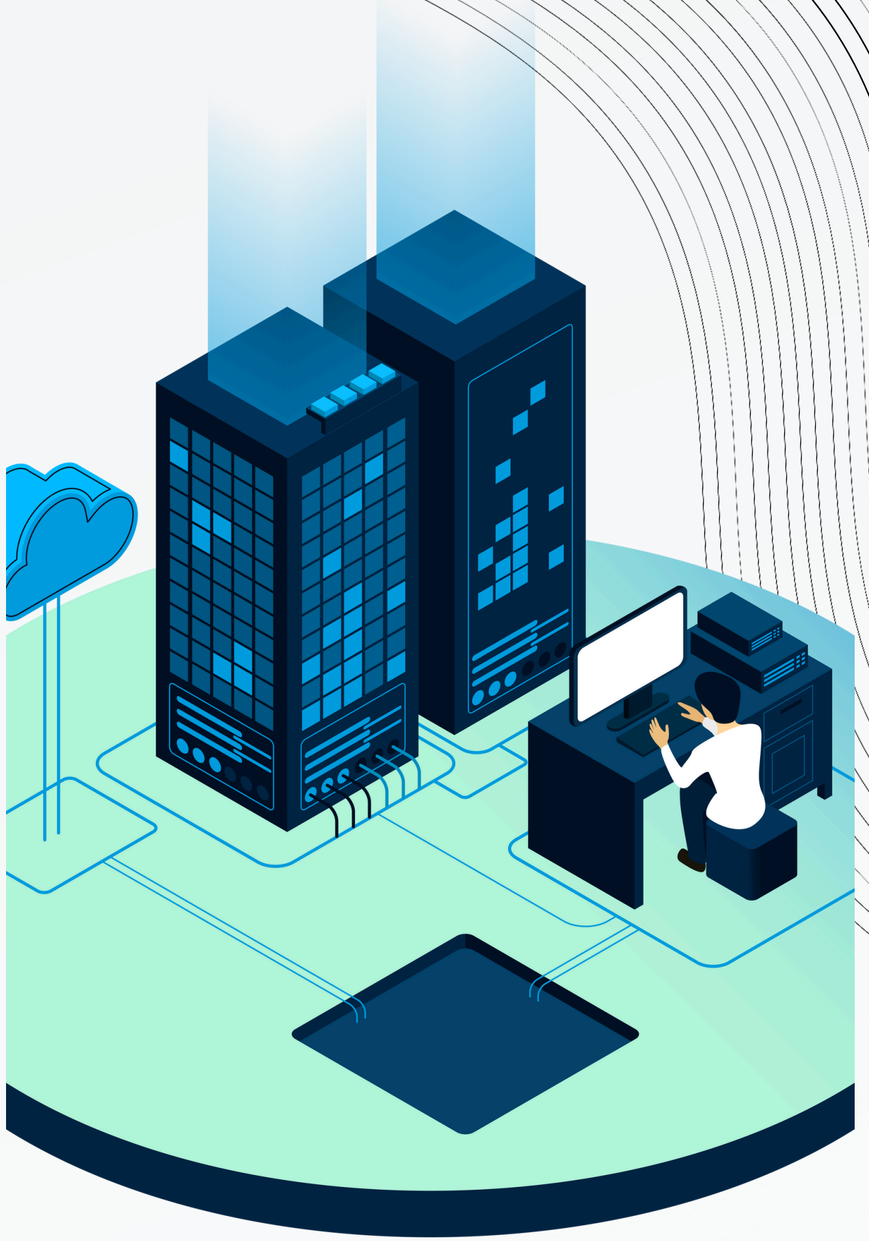
VNC SERVER RISOLUZIONE

GRAZIE ALL'ADOZIONE DI UNA PASSWORD CONFORME ALLE POLICY, ABBIAMO CONSTATO IL FALLIMENTO DEL LOGIN TRAMITE BRUTE FORCE.

```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.5.101:5900    - 192.168.5.101:5900 - Starting VNC login sweep
[!] 192.168.5.101:5900    - No active DB -- Credential data will not be saved!
[-] 192.168.5.101:5900    - 192.168.5.101:5900 - LOGIN FAILED: :password (Incorrect: Authentication failed)
[*] 192.168.5.101:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

NFS EXPORTED SHARE INFORMATION DISCLOSURE

- Con il servizio NFS, un utente (o dispositivo client) può connettersi a un server di rete e accedere ai file su di esso. Dispone di regole che consentono a più utenti di condividere lo stesso file senza conflitti di dati.
- La problematica è che almeno una delle share di NFS esportata da server remoto, può essere montata dall' host che effettua lo scan.
- Dunque, un attaccante potrebbe essere in grado di fare leva sullo scan per leggere (e scrivere) file da remoto.
- Consigliamo di configurare un NFS remoto con accesso autorizzato, in modo che solo gli host con i privilegi possano montare le sue share.



I FILE **/ETC/HOSTS.ALLOW** E **/ETC/HOSTS.DENY** VENGONO COMUNEMENTE UTILIZZATI CON I WRAPPERS SSH E TCP.

ABBIAMO DUNQUE EDITATO I DUE FILE PER NON RENDERLI ACCESSIBILI DALL'ESTERNO.

DEFINIAMO GLI HOST CHE HANNO ACCESSO AL SERVIZIO

```
 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.
#

ALL: 192.168.5.101

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

DEFINIAMO GLI HOST CHE **NON** HANNO I PRIVILEGI DI ACCESSO AL SERVIZIO

```
File  Machine  View  Input  Devices  Help
 GNU nano 2.0.7                File: /etc/hosts.deny                       Modified

# /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: PARANOID
ALL: ALL EXCEPT 192.168.5.101_

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

BIND SHELL BACKDOOR DETECTION

- PER BIND SHELL BACKDOOR DETECTION SI INDICA UNA SHELL CHE È DISPONIBILE SU UNA PORTA REMOTA SENZA RICHIEDERE ALCUNA AUTENTICAZIONE, CREANDO COSÌ UNA SIGNIFICATIVA VULNERABILITÀ DI SICUREZZA.
- QUESTO PERMETTE A UN ATTACCANTE DI CONNETTERSI A QUELLA PORTA E INVIARE COMANDI DIRETTAMENTE AL SISTEMA, METTENDOLO A RISCHIO DI COMPROMISSIONE.
- PER AFFRONTARE QUESTA SITUAZIONE, È FONDAMENTALE CONTROLLARE SE IL SISTEMA REMOTO È GIÀ STATO VIOLATO.
- QUESTO PUÒ ESSERE FATTO ANALIZZANDO I LOG E CERCANDO ATTIVITÀ SOSPETTE.
- SE SI TROVANO PROVE DI COMPROMISSIONE, È CONSIGLIABILE INSTALLARE COMPLETAMENTE IL SISTEMA OPERATIVO PER ELIMINARE EVENTUALI MINACCE E RISTABILIRE LA SICUREZZA.
- NEL CASO IN CUI NON SI VOGLIA INSTALLARE DI NUOVO L'OS, È CONSIGLIABILE OCCULTARE LA PORTA AD EVENTUALI SCANSIONI.

ABBIAMO EVIDENZIATO LA PORTA SULA QUALE E' ATTIVO IL SERVIZIO **BINDSHELL** MEDIANTE IL TOOL *NMAP*

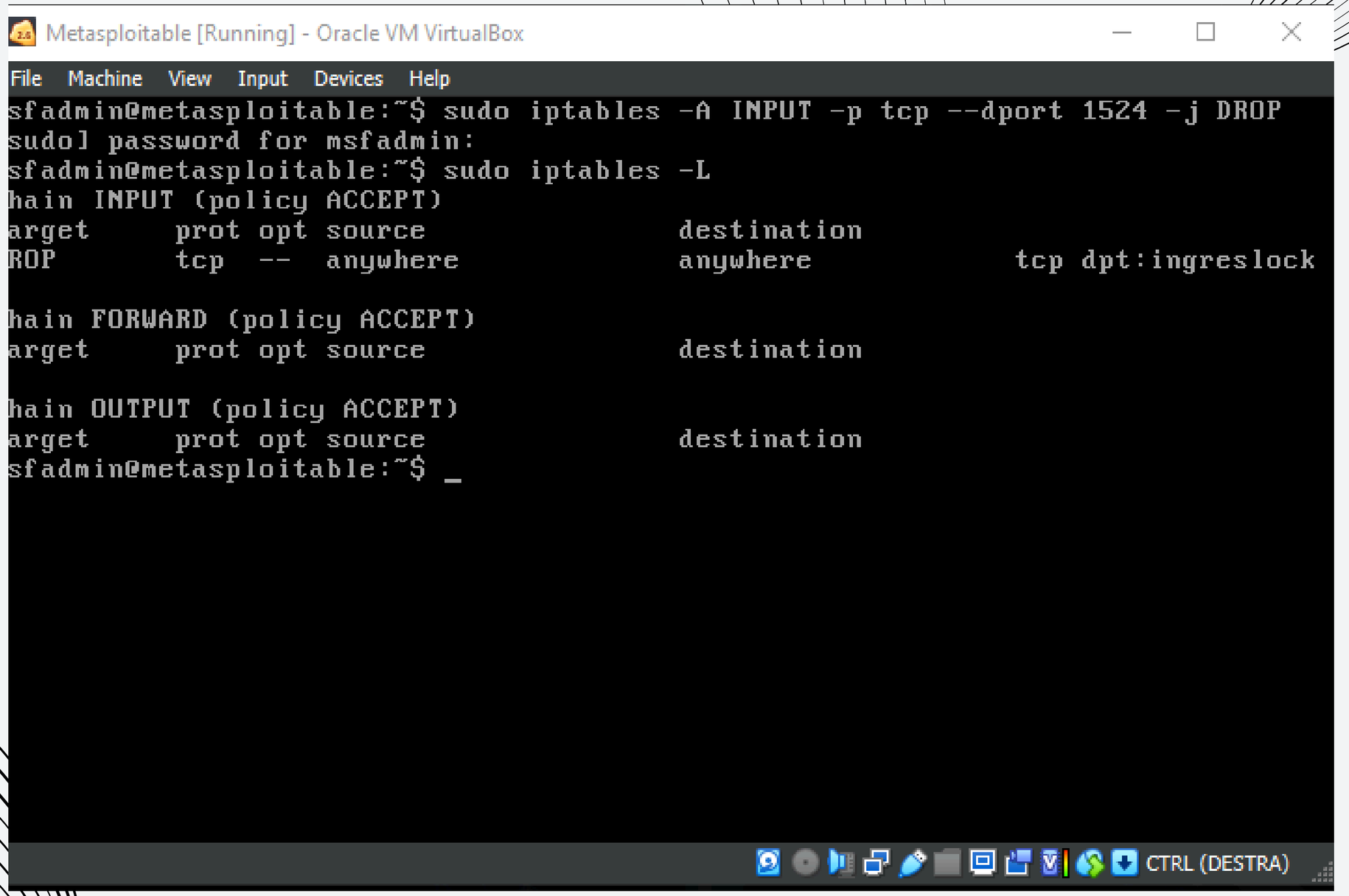
```
└─$ nmap -sV -p 1524 metasploit
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 04:51 EDT
Nmap scan report for metasploit (192.168.5.101)
Host is up (0.00055s latency).

PORT     STATE SERVICE   VERSION
1524/tcp open  bindshell Metasploitable root shell

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Your paragraph text

SFRUTTIAMO LA VULNERABILITA'
PER ENTRARE

```
└─$ nc metasploit 1524
root@metasploitable:/# cd home/
root@metasploitable:/home# ls
ftp
msfadmin
service
user
root@metasploitable:/home# cd msfadmin
root@metasploitable:/home/msfadmin# ls
vulnerable
root@metasploitable:/home/msfadmin#
```

IMPLEMENTAZIONE DELLA REGOLA DEI **FIREWALL** SU *IPTABLES*



SUCCESSIVAMENTE POSSIAMO CONSTATARE GRAZIE AD UN ULTERIORE SCAN DI NMAP CHE IN QUESTO MODO LA PORTA NON E' PIU' ACCESSIBILE

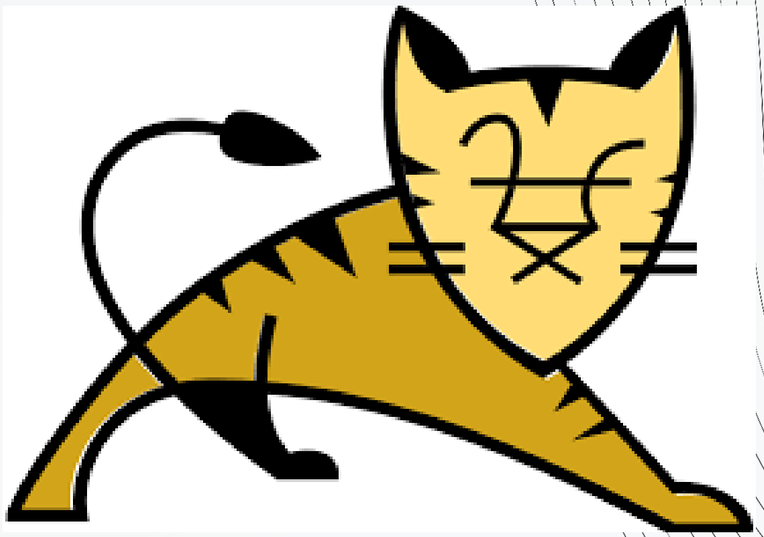
```
└─$ nmap -sV -p 1524 metasploit
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 05:06 EDT
Nmap scan report for metasploit (192.168.5.101)
Host is up (0.00059s latency).

PORT     STATE    SERVICE    VERSION
1524/tcp filtered ingreslock

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

COME AFFERMATO IN PRECEDENZA, QUESTO METODO E' UN PALLIATIVO ALLA SOLUZIONE DI RE-INSTALLARE IL SISTEMA OPERATIVO

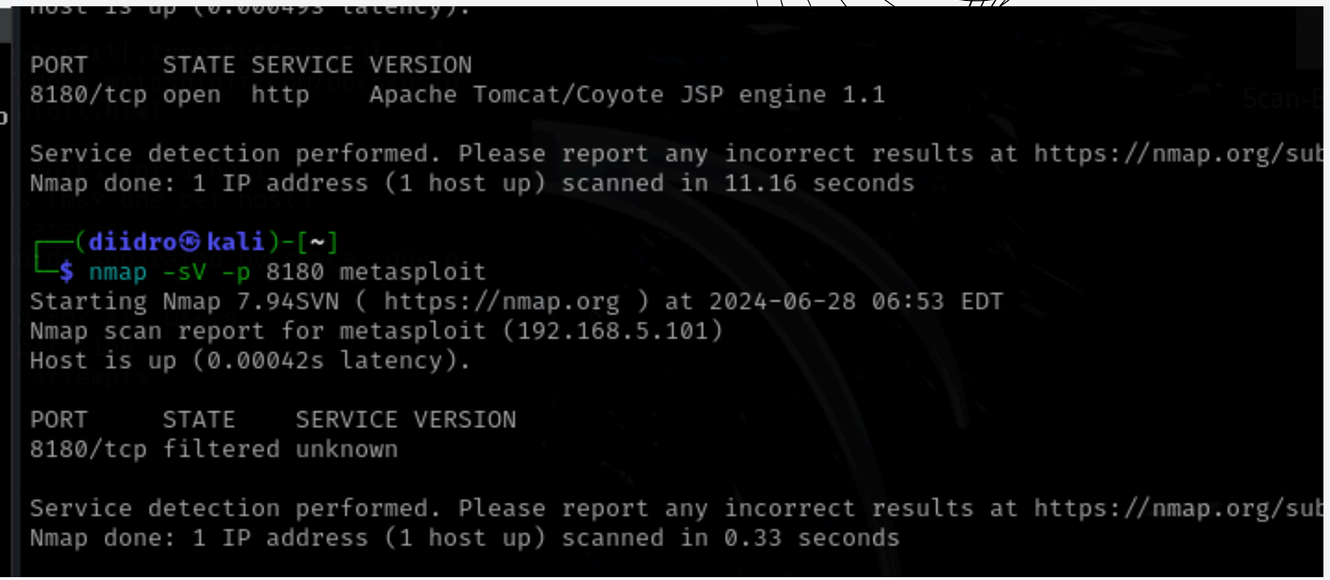
APACHE TOMCAT SEOL

- SECONDO LA SUA VERSIONE, APACHE TOMCAT È PARI O INFERIORE ALLA 5.5.X E QUINDI NON PIÙ MANTENUTO DAL FORNITORE O PROVIDER. LA MANCANZA DI SUPPORTO IMPLICA CHE NON VERRANNO RILASCIATE NUOVE PATCH DI SICUREZZA, IL CHE POTREBBE COMPORTARE VULNERABILITÀ.

- È UTILIZZATO PRINCIPALMENTE PER ESEGUIRE APPLICAZIONI WEB SCRITTE IN LINGUAGGIO JAVA. TOMCAT IMPLEMENTA LE SPECIFICHE JAVA SERVLET, JAVASERVER PAGES (JSP) E WEBSOCKET, CONSENTENDO AGLI SVILUPPATORI DI ESEGUIRE CODICE JAVA LATO SERVER PER GENERARE CONTENUTI WEB DINAMICI.



LA RISOLUZIONE IDEALE DOVREBBE ESSERE QUELLA DI AGGIORNARE APACHE ALL'ULTIMA VERSIONE SUPPORTATA.



NEL CASO IN CUI L'AZIENDA NON POSSA EFFETTUARE L'AGGIORNAMENTO SI CONSIGLIA LA SOLUZIONE SOPRASTANTE NELLA QUALE SI INSERISCONO LE IMPOSTAZIONI NEL FIREWALL IN MODO DA BLOCCARE L'ACCESSO AD ESTERNI.

REPORT NESSUS FINALE

192.168.5.101

Vulnerabilities Total: 77

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	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

COME DA IMMAGINE LE VULNERABILITA’ CHE ABBIAMO AFFRONTATO SONO STATE RISOLTE

THANKS FOR WATCHING

DATASHIELDS