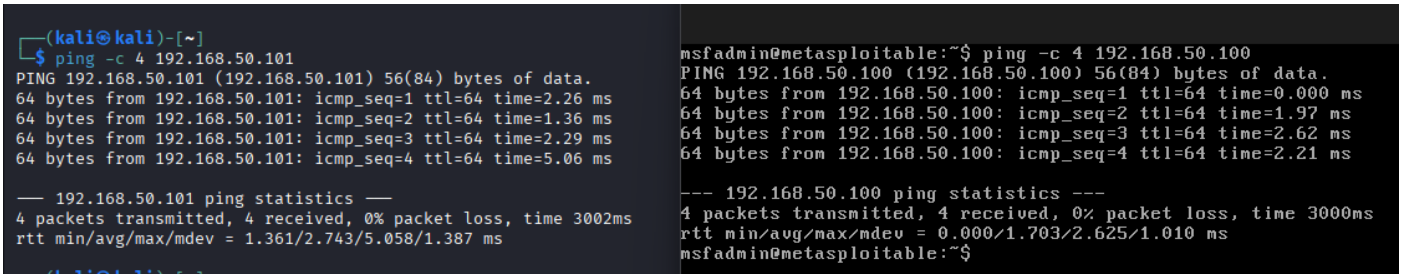
INDICE

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: il laboratorio è stato progettato per analizzare in modo strutturato il comportamento di alcuni servizi di accesso remoto esposti su un sistema di test, osservando come la scelta delle credenziali e delle configurazioni influisca direttamente sulla possibilità di ottenere un accesso valido.
L'attività si concentra sull'utilizzo controllato di strumenti di autenticazione automatizzata, applicati a servizi differenti, al fine di comprendere le dinamiche operative che portano all'individuazione di credenziali corrette quando queste risultano deboli, prevedibili o incluse in insiemi di valori comunemente utilizzati.

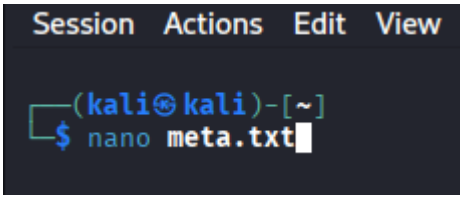
OBIETTIVO: verificare la possibilità di individuare credenziali valide su più servizi di accesso remoto utilizzando dizionari di password mirati, valutando l'efficacia del processo e le differenze di comportamento tra i servizi analizzati.

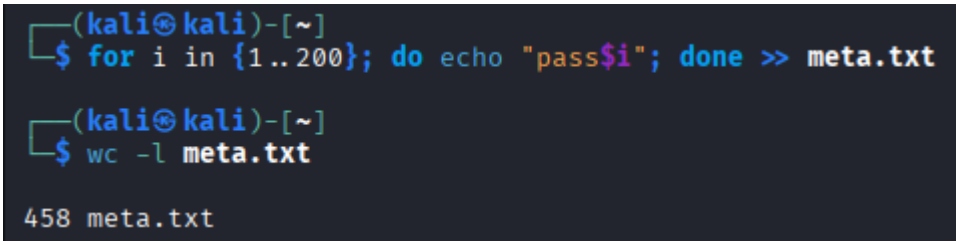


Prima di procedere con le attività operative, è stata verificata la corretta comunicazione tra i sistemi coinvolti; la connettività bidirezionale è stata testata attraverso l'invio di pacchetti di rete tra le macchine, confermando che entrambe risultano raggiungibili e rispondono correttamente alle richieste.
Questa fase è fondamentale perché garantisce che l'infrastruttura di rete sia configurata in modo coerente e che non vi siano problemi di isolamento, instradamento o filtraggio del traffico.
Solo in presenza di una comunicazione stabile e continua tra i sistemi è possibile eseguire in modo affidabile le successive attività sui servizi di accesso remoto, evitando risultati falsati o errori dovuti a problemi di rete piuttosto che al comportamento effettivo dei servizi analizzati.

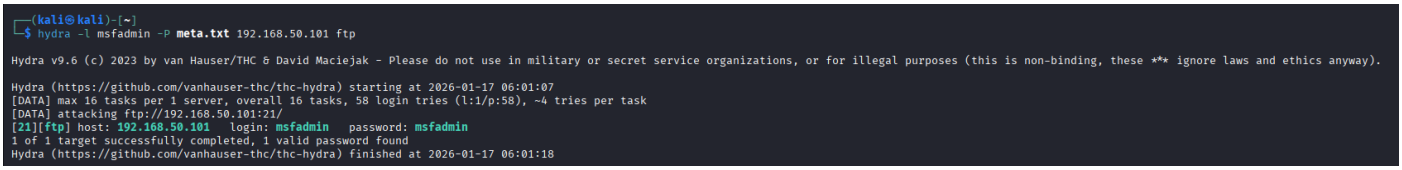
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV 192.168.50.101

Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-15 11:19 EST
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 979 closed tcp ports (reset)
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?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
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
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
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:83:88:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.23 seconds
```

Una volta confermata la comunicazione tra le macchine, l'attività è proseguita con l'analisi dei servizi esposti dal sistema di destinazione.
A questo scopo è stata eseguita una scansione delle porte e dei servizi attivi che ha permesso di individuare quali componenti risultano in ascolto sulla rete e quindi potenzialmente accessibili.
Questa fase ha un ruolo centrale nell'esercizio perché consente di costruire una visione completa della superficie di accesso del sistema: vengono infatti identificati i protocolli disponibili, le porte utilizzate e le versioni dei servizi in esecuzione; le informazioni ottenute permettono di selezionare in modo consapevole i servizi su cui concentrarsi nelle fasi successive, evitando tentativi casuali e indirizzando l'analisi solo verso i punti effettivamente esposti.
L'esito della scansione ha evidenziato la presenza di diversi servizi di accesso remoto e di rete, tra cui FTP, SSH e Telnet, che rappresentano canali di autenticazione diretta.
Sulla base di questi risultati è stato quindi possibile definire con precisione quali servizi sottoporre alle attività successive, assicurando coerenza tra la fase di analisi preliminare e le operazioni operative svolte in seguito.



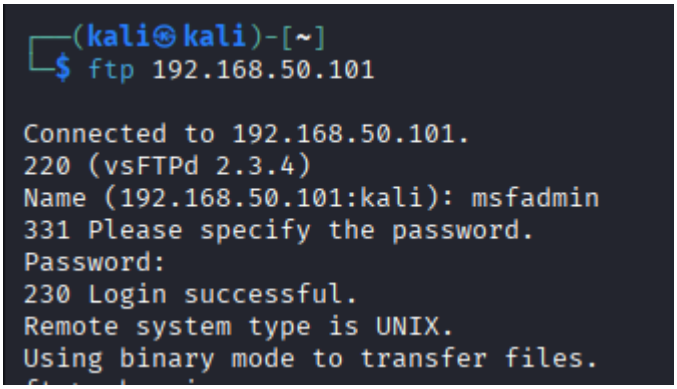


Per rendere l'attività più veloce, prima di avviare le operazioni di autenticazione è stata effettuata una fase di preparazione mirata delle credenziali da testare.
Invece di utilizzare dizionari estesi e generici, è stato creato un file di testo dedicato, contenente un insieme selezionato di password plausibili, in linea con scenari reali e con l'obiettivo di ridurre sensibilmente i tempi di esecuzione.
Il dizionario è stato costruito localmente e popolato in modo automatico con un numero significativo di stringhe, arrivando a diverse centinaia di possibili password.
Questa scelta consente di simulare un approccio più strategico, basato su tentativi mirati piuttosto che su un'esplorazione indiscriminata, mantenendo comunque una varietà sufficiente di combinazioni da testare.
La verifica finale del file ha confermato la corretta creazione del dizionario e il numero di voci disponibili, rendendolo immediatamente utilizzabile nelle successive fasi di autenticazione sui servizi individuati.



Successivamente il laboratorio è proseguito con la verifica delle credenziali sul servizio FTP individuato in precedenza.
È stato avviato un processo di autenticazione automatizzata utilizzando come nome utente un account noto presente sul sistema e come insieme di password il dizionario creato nella fase precedente.
L'operazione ha previsto l'esecuzione di tentativi paralleli, consentendo di testare in modo efficiente le diverse combinazioni disponibili.
Il servizio ha risposto positivamente a una delle credenziali presenti nel dizionario, permettendo di individuare una coppia utente-password valida; il risultato conferma che il servizio accetta autenticazioni basate su credenziali deboli o facilmente prevedibili e dimostra l'efficacia di un dizionario mirato rispetto a liste generiche molto più ampie.

Il completamento dell'operazione ha fornito un accesso valido al servizio FTP, rendendo possibile l'interazione diretta con il sistema remoto e aprendo la strada alle successive verifiche sugli altri servizi esposti.



A seguito dell'individuazione delle credenziali valide, è stato effettuato un tentativo di accesso diretto al servizio FTP esposto dal sistema remoto.
La connessione è stata stabilita correttamente e il servizio ha risposto accettando l'autenticazione con le credenziali precedentemente individuate.
Una volta completata la fase di login, il sistema remoto ha confermato l'accesso consentendo l'interazione con il file system attraverso il protocollo FTP.
Il servizio si è presentato come pienamente operativo e configurato per l'utilizzo di autenticazione basata su username e password, senza ulteriori meccanismi di restrizione o controllo aggiuntivi.
Il risultato ottenuto dimostra che le credenziali individuate non solo risultano valide dal punto di vista teorico, ma permettono un accesso reale e funzionale al servizio, confermando l'effettiva esposizione del sistema e la possibilità di operare direttamente sulle risorse messe a disposizione dal server FTP.

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l msfadmin -P meta.txt -t 4 192.168.50.101 ssh

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-17 06:19:42
[DATA] max 4 tasks per 1 server, overall 4 tasks, 61 login tries (l:1/p:61), ~16 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[22][ssh] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-17 06:20:37
```

Successivamente, l'analisi è stata estesa al servizio SSH, configurato per consentire l'accesso remoto tramite autenticazione basata su credenziali.
Utilizzando il dizionario personalizzato precedentemente costruito, è stata avviata un'attività di verifica automatizzata delle combinazioni di accesso sull'account individuato come potenzialmente valido.
Il processo ha effettuato tentativi controllati e paralleli, fino a individuare una corrispondenza corretta tra nome utente e password.
Il risultato ha confermato la validità delle stesse credenziali già emerse in precedenza, dimostrando che l'account risulta riutilizzato su più servizi esposti dal sistema.
L'esito positivo dell'operazione indica che il servizio SSH accetta autenticazioni basate su password senza ulteriori restrizioni, rendendo possibile l'accesso remoto completo al sistema attraverso un canale cifrato; questo conferma la coerenza della configurazione dei servizi e l'effettiva possibilità di ottenere una sessione interattiva utilizzando credenziali deboli o facilmente individuabili.

```
[23][telnet] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-17 06:32:32
```

L'analisi è stata infine estesa al servizio Telnet, presente sul sistema come ulteriore canale di accesso remoto basato su autenticazione testuale; utilizzando lo stesso dizionario personalizzato già impiegato nelle fasi precedenti, è stata avviata una procedura di verifica automatizzata delle credenziali sull'account individuato.
Il processo ha eseguito una serie di tentativi sequenziali fino a identificare una combinazione valida di nome utente e password, confermando nuovamente l'utilizzo delle stesse credenziali già riscontrate sugli altri servizi.
L'esito positivo dimostra che il servizio Telnet accetta autenticazioni senza meccanismi di protezione aggiuntivi e senza differenziazione delle credenziali rispetto agli altri servizi esposti.
Questo risultato evidenzia come l'accesso remoto tramite Telnet consenta l'ingresso completo al sistema utilizzando credenziali deboli e riutilizzate, aumentando significativamente la superficie di accesso e la possibilità di compromissione attraverso servizi legacy privi di adeguate misure di controllo.

CONCLUSIONE

L’attività svolta ha dimostrato come la presenza di servizi di accesso remoto configurati con credenziali deboli e condivise rappresenti un fattore critico di esposizione per un sistema. L’analisi ha evidenziato che più servizi distinti, pur utilizzando protocolli differenti, accettano le stesse credenziali di autenticazione, rendendo possibile l’accesso completo al sistema attraverso canali alternativi e riducendo drasticamente le barriere di protezione.
L’utilizzo di un dizionario mirato e realistico ha permesso di ottenere risultati concreti in tempi contenuti, mostrando come la prevedibilità delle credenziali influisca direttamente sull’efficacia dei meccanismi di autenticazione; la possibilità di accedere al sistema tramite FTP, SSH e Telnet con le medesime credenziali evidenzia inoltre l’assenza di una separazione logica tra i servizi e una gestione non differenziata degli accessi.
Nel complesso, l’esercizio mette in luce l’importanza di una gestione rigorosa delle credenziali e della configurazione dei servizi di rete, sottolineando come la combinazione di account predefiniti, password riutilizzate e servizi legacy possa compromettere l’integrità e il controllo di un sistema anche in assenza di vulnerabilità software avanzate.