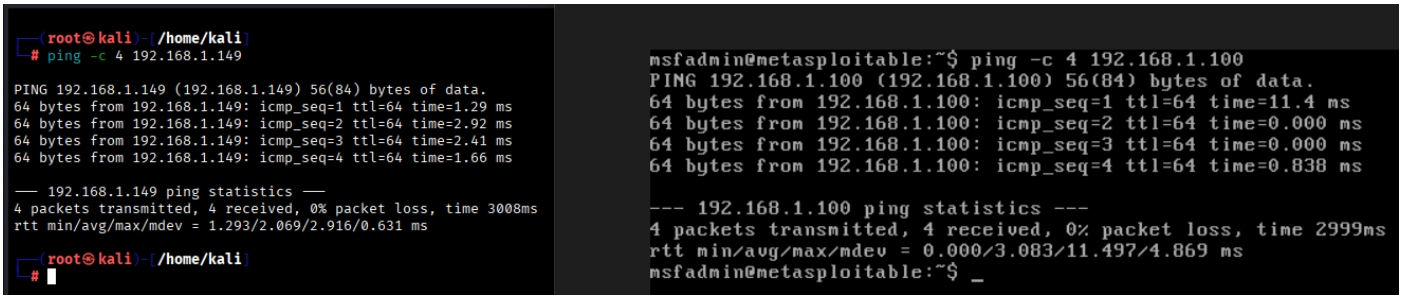
INDICE

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: il laboratorio analizza la sicurezza del servizio Telnet esposto su un sistema target, concentrandosi sulle implicazioni derivanti dall'uso di protocolli legacy e da configurazioni non adeguatamente protette.
L'attività è orientata alla comprensione delle modalità con cui un servizio di rete non correttamente configurato possa rivelare informazioni sensibili e consentire l'accesso non autorizzato a un sistema remoto.
L'analisi viene condotta attraverso strumenti comunemente impiegati nei processi di vulnerability assessment, integrando fasi di rilevazione automatizzata e verifica manuale dei risultati ottenuti.

OBIETTIVO: dentificare e confermare la presenza di una vulnerabilità sul servizio Telnet della macchina Metasploitable, verificando l'esposizione del servizio e l'eventuale utilizzo di credenziali di default.



Il laboratorio ha inizio con una fase preliminare di verifica della connettività di rete tra la macchina di analisi e il sistema target; la comunicazione bidirezionale correttamente stabilita tra i due sistemi conferma che essi sono inseriti nella stessa rete e possono scambiarsi traffico senza restrizioni a livello infrastrutturale.
Questa fase è fondamentale in quanto consente di escludere problemi di rete, di configurazione o di isolamento dei sistemi, garantendo che le successive attività di analisi e accesso ai servizi esposti siano attribuibili esclusivamente alle configurazioni di sicurezza del sistema target e non a limitazioni di connettività.

È stata avviata una fase di analisi strutturata finalizzata all'identificazione dei servizi di rete attivi sul sistema target, utilizzando una piattaforma professionale impiegata nei processi di vulnerability assessment; questa attività consente di individuare servizi potenzialmente critici esposti sulla rete e di valutarne le caratteristiche di base, come la disponibilità e le

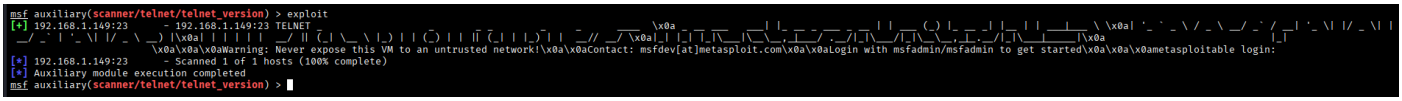
informazioni restituite in fase di connessione.
In particolare, l'analisi ha permesso di verificare la presenza del servizio Telnet, un protocollo di comunicazione remota considerato obsoleto e intrinsecamente insicuro, in quanto non prevede meccanismi di cifratura per la protezione delle credenziali e dei dati trasmessi.
La rilevazione del servizio rappresenta un primo indicatore di rischio, poiché l'esposizione di Telnet su un sistema accessibile in rete può costituire un vettore di accesso non autorizzato se non adeguatamente protetto o disabilitato.

```
[*] Using auxiliary/scanner/telnet/telnet_version
msf auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


View the full module info with the info, or info -d command.

msf auxiliary(scanner/telnet/telnet_version) >
```

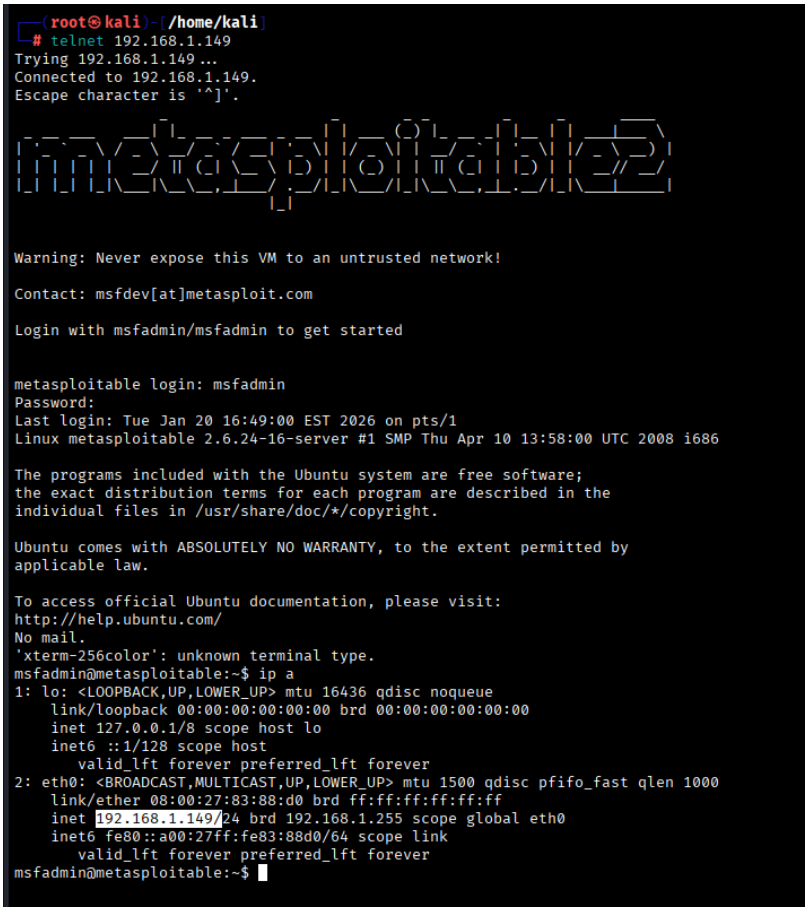
Nel corso dell'attività è emerso che l'analisi iniziale del servizio Telnet non poteva essere eseguita in modo efficace in quanto mancava l'indicazione esplicita del sistema target da sottoporre a valutazione.
In assenza di tale informazione, la procedura di analisi non disponeva di un perimetro definito e non era in grado di produrre risultati significativi.

```
msf auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


View the full module info with the info, or info -d command.

msf auxiliary(scanner/telnet/telnet_version) >
```

Per risolvere questa condizione, è stata effettuata una configurazione mirata dell'ambiente di analisi, specificando il sistema oggetto della verifica e rendendo così possibile l'avvio corretto dell'attività di valutazione.
Questo adeguamento ha consentito di delimitare con precisione l'ambito dell'analisi, garantendo che le evidenze raccolte fossero direttamente riferibili al sistema esaminato e coerenti con gli obiettivi dell'esercizio.



A seguito della corretta definizione del perimetro di analisi, è stata eseguita la verifica del servizio Telnet esposto dal sistema target e l'attività ha confermato che il servizio risponde attivamente alle richieste di connessione e fornisce informazioni identificative durante la fase iniziale di comunicazione.
In particolare, il servizio Telnet espone un banner informativo che rivela la presenza di credenziali di accesso predefinite, indicando esplicitamente la possibilità di autenticarsi utilizzando account standard; questo comportamento costituisce una vulnerabilità rilevante, in quanto consente a un soggetto non autorizzato di ottenere informazioni sensibili e potenzialmente accedere al sistema senza la necessità di tecniche di attacco avanzate.
La presenza di credenziali di default associate a un servizio di accesso remoto non cifrato rappresenta un rischio elevato per la sicurezza del sistema, poiché abbassa drasticamente la soglia di accesso e aumenta la probabilità di compromissione in scenari reali.



L'attività di verifica ha confermato che il servizio Telnet esposto consente l'accesso diretto al sistema target utilizzando credenziali predefinite, senza l'adozione di meccanismi di protezione aggiuntivi e quindi l'autenticazione è avvenuta con successo, permettendo l'ottenimento di una sessione interattiva sul sistema remoto.
Questo risultato dimostra in modo inequivocabile che un utente non autorizzato, una volta

individuato il servizio esposto, è in grado di accedere al sistema senza dover ricorrere a tecniche di attacco avanzate.
La possibilità di stabilire una sessione remota interattiva implica il completo superamento dei controlli di accesso di base e rappresenta una compromissione effettiva del sistema. L'accesso non autorizzato ottenuto evidenzia un rischio significativo per la sicurezza dell'infrastruttura, in quanto consente potenzialmente l'esecuzione di comandi, la consultazione di informazioni sensibili e l'escalation dei privilegi.

CONCLUSIONE

L’attività di analisi ha evidenziato come l’esposizione di servizi di rete obsoleti e non adeguatamente protetti possa rappresentare un rischio significativo per la sicurezza di un sistema informatico.
La presenza del servizio Telnet, unita all’utilizzo di credenziali predefinite, ha consentito l’accesso non autorizzato al sistema target, dimostrando in modo concreto l’impatto di configurazioni di sicurezza non conformi alle best practice attuali.
Il laboratorio ha mostrato come una corretta sequenza di analisi, che include la verifica della connettività, l’identificazione dei servizi esposti e la validazione dell’accesso, permetta di individuare vulnerabilità critiche anche in assenza di tecniche di attacco avanzate.
In un contesto aziendale reale, condizioni analoghe potrebbero essere sfruttate per compromettere la riservatezza dei dati, alterare la configurazione dei sistemi o interrompere la continuità operativa.
La conclusione dell’attività sottolinea l’importanza di una gestione consapevole dei servizi di rete, della dismissione dei protocolli obsoleti e dell’adozione di politiche di sicurezza rigorose, al fine di ridurre la superficie di attacco e prevenire accessi non autorizzati; infine il laboratorio conferma il valore delle attività di vulnerability assessment come strumento essenziale per l’individuazione preventiva delle debolezze e per il miglioramento continuo del livello di sicurezza dei sistemi informativi.