13 DICEMBRE 2026

AUDIT DI SICUREZZA RETE E SERVIZI

INDICE

INTRODUZIONE

Questa relazione descrive il processo di analisi di rete, valutando le rotte configurate, i servizi esposti e la sicurezza delle applicazioni coinvolte. Sono stati utilizzati strumenti e tecniche standard del settore per raccogliere informazioni utili a identificare vulnerabilità e suggerire mitigazioni. Ogni passaggio dell’analisi è stato condotto con l'obiettivo di comprendere a fondo lo stato di sicurezza della rete esaminata e proporre miglioramenti concreti.

CONTESTO DELLA RETE

L'analisi delle rotte attive e delle configurazioni di rete è stata effettuata utilizzando il comando netstat -r.
Questo strumento consente di visualizzare le tabelle di routing attive e le rotte configurate per ogni interfaccia.

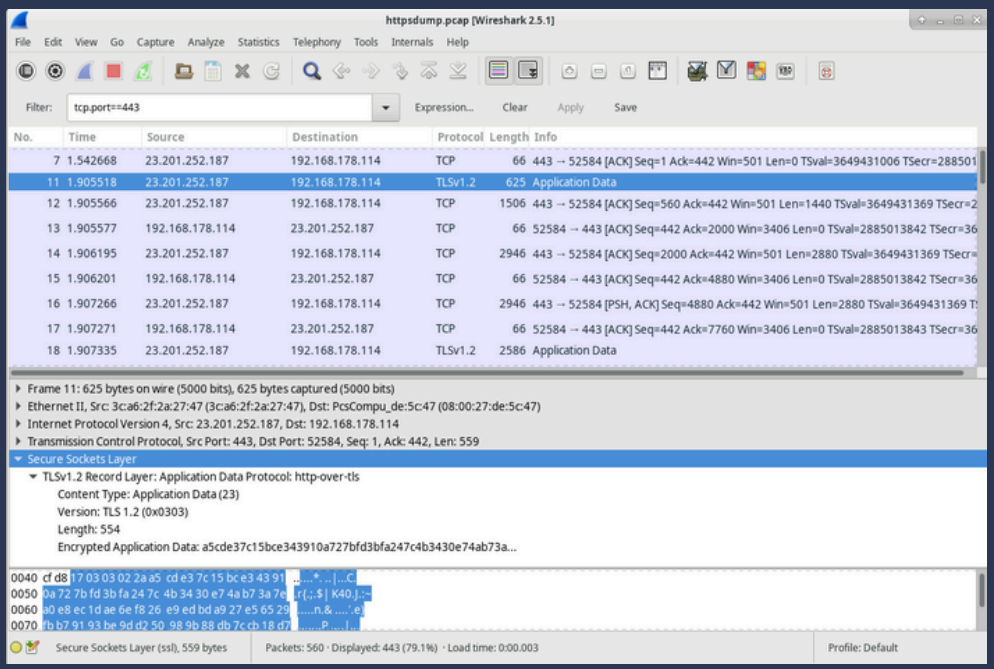
- OUTPUT NETSTAT -R (IPV4 E IPV6):
- IPV4:
  - IL GATEWAY PREDEFINITO È 192.168.178.1 E L'INTERFACCIA ASSOCIATA È 192.168.178.113.
  - SONO PRESENTI ROTTE LOCALI, COME 127.0.0.1, UTILIZZATE PER COMUNICAZIONI INTERNE.
  - LA METRICA PER LA ROTTA PRINCIPALE È 10, INDICANDO CHE È PRIORITIZZATA RISPETTO AD ALTRE.
- IPV6:
  - CONFIGURAZIONI DI INDIRIZZAMENTO AVANZATE, COME INDIRIZZI LINK-LOCAL E GATEWAY IPV6 (ES. FE80::3EA6:2FFF:FE2A:2747), SONO PRESENTI. QUESTE CONFIGURAZIONI NECESSITANO DI CONTROLLI PER EVITARE FALLE DI SICUREZZA.

```
PS C:\Users\user> netstat -r
===========================================================================
Elenco interfacce
  4...08 00 27 60 10 db ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
  6...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
  5...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete            Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0    192.168.178.1  192.168.178.113     10
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
    192.168.178.0    255.255.255.0         On-link   192.168.178.113    266
  192.168.178.113  255.255.255.255         On-link   192.168.178.113    266
  192.168.178.255  255.255.255.255         On-link   192.168.178.113    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link   192.168.178.113    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link   192.168.178.113    266
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  4    266 ::/0                     fe80::3ea6:2fff:fe2a:2747
  1    306 ::1/128                  On-link
  4    266 2a05:5800:5e5:9400::/56  fe80::3ea6:2fff:fe2a:2747
  4    266 2a05:5800:5e5:9400::/64  On-link
  4    266 2a05:5800:5e5:9400:3c3c:13de:c82a:774d/128
                                    On-link
  4    266 2a05:5800:5e5:9400:81f3:e962:d982:ff52/128
                                    On-link
  4    266 fe80::/64                On-link
  4    266 fe80::3c3c:13de:c82a:774d/128
                                    On-link
  1    306 ff00::/8                 On-link
  4    266 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna
PS C:\Users\user>
```

ANALISI DEL TRAFFICO (WIRESHARK)

Per comprendere il traffico di rete, è stata effettuata una cattura di pacchetti usando Wireshark.

- TRAFFICO HTTPS (TLS 1.2):
- LA COMUNICAZIONE È AVVENUTA TRA 23.201.252.187 E 192.168.178.114 SULLA PORTA 443.
- L'USO DI TLS 1.2 GARANTISCE CHE I DATI TRASMESSI SIANO CIFRATI, PROTEGGENDO LA CONFIDENZIALITÀ.
- LA SEQUENZA DI PACCHETTI INCLUDE SEGMENTI PSH E ACK, CHE SUGGERISCONO UN TRAFFICO LEGITTIMO, MA RICHIEDONO ATTENZIONE PER IDENTIFICARE POTENZIALI ATTACCHI BASATI SU ANOMALIE NEL TRAFFICO (ES. FLOODING O MITM).



SCANSIONE DI RETE (NMAP)

Con l'utilizzo di Nmap, sono stati analizzati i servizi esposti sulla rete, in particolare sull'host 192.168.178.114.

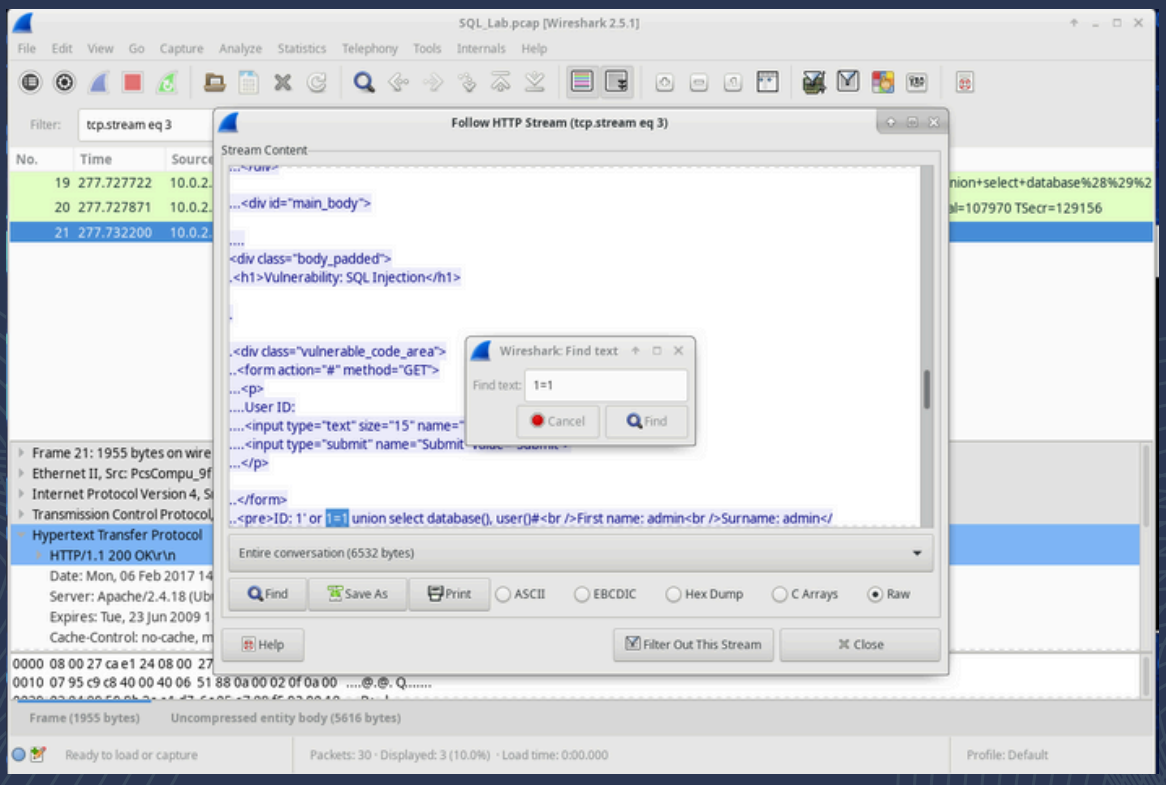
- SERVIZI RILEVATI: (RIFERIMENTO:
- PORTA 21 (FTP): IL SERVER VSFTPD 3.0.3 CONSENTE ACCESSO ANONIMO. QUESTO RAPPRESENTA UN RISCHIO SIGNIFICATIVO, POICHÉ UTENTI NON AUTENTICATI POSSONO ACCEDERE A DIRECTORY POTENZIALMENTE CRITICHE.
- PORTA 22 (SSH): IL SERVIZIO OPENSSH 7.7 È CONFIGURATO IN MODO STANDARD, MA DEVONO ESSERE IMPLEMENTATE MISURE AGGIUNTIVE PER PREVENIRE ATTACCHI BRUTE-FORCE.

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.178.114
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 05:00 EST
Nmap scan report for secOps.fritz.box (192.168.178.114)
Host is up (0.00073s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.178.112
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
|_  256 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.58 seconds
```

SQL INJECTION

Un test di sicurezza ha simulato un attacco SQL Injection su un database vulnerabile.

- ATTACCO SIMULATO:
- PAYLOAD UTILIZZATO: 1=1. QUESTO È STATO INSERITO IN UNA QUERY DINAMICA NON PROTETTA, CAUSANDO LA DIVULGAZIONE DI INFORMAZIONI SENSIBILI COME IL NOME DEL DATABASE E L'UTENTE CORRENTE.
- PROBLEMA IDENTIFICATO: MANCANZA DI VALIDAZIONE DELLE INPUT E UTILIZZO DI QUERY NON PARAMETRIZZATE.



RISCHI E MITIGAZIONI

- Rischio: Accesso anonimo che potrebbe essere sfruttato per accedere a file sensibili.
- Mitigazione: Disabilitare l'accesso anonimo o limitarlo a directory non critiche.

01 Servizio FTP

- Rischio: Attacchi brute-force per compromettere credenziali.
- Mitigazione: Configurare strumenti come fail2ban, utilizzare chiavi SSH sicure e disabilitare l'accesso root.

02 Servizio SSH

- Rischio: Compromissione totale del database tramite query non sicure.
- Mitigazione: Implementare query parametrizzate e validare ogni input utente.

03 SQL Injection

- Rischio: Potenziali vulnerabilità nei gateway link-local.
- Mitigazione: Audit periodici delle configurazioni di routing e applicazione di ACL su interfacce critiche.

04 Configurazione IPv6

CONCLUSIONI

L’analisi effettuata ha evidenziato diverse criticità nella configurazione della rete e nei servizi esposti. In particolare, il servizio FTP rappresenta un punto debole significativo, così come la presenza di vulnerabilità legate a SQL Injection. Le mitigazioni proposte devono essere implementate con urgenza per ridurre il rischio complessivo.

L’utilizzo di strumenti come Wireshark e Nmap si è rivelato fondamentale per identificare problemi di sicurezza e migliorare la resilienza della rete. Si raccomanda inoltre di effettuare test di sicurezza regolari per mantenere un elevato livello di protezione.