Esercizio W15D1

Redatto da: Pandolfi Luciano

Data: 15/12/24

Indice

Traccia

L’esercizio è diviso in due parti.

Prima parte

Rispondere ai seguenti quesiti:

● Spiegare brevemente cosa vuol dire Null Session

● Elencare i sistemi che sono vulnerabili a Null Session e se sono ancora in commercio

● Elencare le modalità per mitigare o risolvere la vulnerabilità Null Session

● Spiegare brevemente come funziona l'ARP Poisoning

● Elencare i sistemi che sono vulnerabili a ARP Poisoning

● Elencare le modalità per mitigare, rilevare o annullare l'ARP Poisoning

Seconda parte

Esercizio guidato su Ettercap:

Ettercap è uno strumento di analisi della rete e di attacco di tipo "Man-in-the-Middle" MITM. Ettercap può essere utilizzato per diverse finalità, inclusa la cattura e l'analisi del traffico di rete, il rilevamento di host nella rete, e l'esecuzione di attacchi MITM per intercettare le comunicazioni. Può anche essere configurato per eseguire attacchi di spoofing, come ARP spoofing, per indirizzare il traffico attraverso l'attaccante.

1. PRIMA PARTE (Null Session)

1.1 Cosa vuol dire Null Session?

Una Null Session è una connessione anonima che viene stabilita su un computer o server, in cui non vengono fornite le credenziali di autenticazione (username e password).

Questa connessione è solitamente utilizzata da un processo di rete in cui l'utente non è autenticato, ma il sistema consente comunque di ottenere informazioni pubbliche.

La vulnerabilità Null Session su Windows è una vulnerabilità di sicurezza che consente a un attaccante di accedere a informazioni sensibili sui sistemi Windows, come nomi di account utente, password e informazioni di condivisione delle risorse.

E' importante mettere in evidenza che la vulnerabilità è stata risolta in versioni successive dei sistemi operativi Windows e che molti amministratori di sistema Windows hanno adottato misure di sicurezza per mitigare questa vulnerabilità.

1.2 Sistemi vulnerabili a Null Session e se sono ancora in commercio

I sistemi vulnerabili a Null Session sono principalmente le versioni più vecchie dei sistemi operativi Microsoft Windows, in particolare:

- Windows Server 2003
- Windows 98
- Windows NT

- Windows 2000
- Windows XP (in alcune configurazioni)

Anche se queste versioni di Windows non sono più in commercio, versioni più moderne di Windows, come Windows 7, 8, 10 e 11, potrebbero essere vulnerabili a Null Session in ambienti mal configurati, specialmente se le politiche di sicurezza non sono correttamente impostate.

1.3 Modalità per mitigare o risolvere la vulnerabilità Null Session

Le seguenti misure possono essere adottate per mitigare o risolvere la vulnerabilità Null Session:

- Disabilitare il protocollo NetBIOS: Bloccare le comunicazioni di rete via NetBIOS, che spesso permettono le Null Session.
- Modificare le politiche di sicurezza: Configurare correttamente le politiche di sicurezza di Windows per impedire l'autenticazione anonima.
- Limitare le condivisioni di rete: Proteggere le condivisioni di rete sensibili con password robuste e disabilitare la condivisione anonima.
- Aggiornare i sistemi: Assicurarsi che il sistema operativo e le applicazioni siano aggiornati con le ultime patch di sicurezza.

1.4 Come funziona l'ARP Poisoning?

L'ARP Poisoning (o ARP Spoofing) è un attacco in cui un attaccante invia risposte ARP false sulla rete, associando il proprio indirizzo MAC a un indirizzo IP che appartiene a un altro dispositivo (come un router o un altro host). In questo modo, l'attaccante può intercettare, modificare o reindirizzare il traffico di rete destinato all'indirizzo IP compromesso, causando un attacco Man-in-the-Middle. L'attaccante inganna la rete facendole credere che l'indirizzo MAC del dispositivo di destinazione sia associato all'indirizzo IP di un altro dispositivo, consentendo la manipolazione del traffico.

1.5 Sistemi vulnerabili a ARP Poisoning

I sistemi vulnerabili all'ARP Poisoning sono quelli che utilizzano il protocollo ARP (Address Resolution Protocol) per risolvere gli indirizzi IP in indirizzi MAC, quindi la maggior parte delle reti che operano su tecnologie Ethernet sono vulnerabili. Questi includono:

- Sistemi operativi Windows, Linux, macOS: Tutti questi sistemi sono vulnerabili se non vengono adottate contromisure adeguate.

- Dispositivi di rete come switch e router: Se non configurati correttamente, possono essere vulnerabili all'ARP Poisoning.
- Sistemi in ambienti di rete locali (LAN) che utilizzano il protocollo ARP per la risoluzione degli indirizzi.

1.6 Modalità per mitigare, rilevare o annullare l'ARP Poisoning

Le seguenti misure possono essere adottate per mitigare e rilevare l'ARP Poisoning:

- Utilizzare ARP Statico: Configurare manualmente le tabelle ARP per assegnare indirizzi IP a indirizzi MAC specifici. Questo impedisce che l'attaccante possa inviare risposte ARP false.
- Implementare sistemi di rilevamento delle intrusioni (IDS/IPS): Questi sistemi possono rilevare attività sospette, come risposte ARP non verificate.
- Utilizzare crittografia: La crittografia delle comunicazioni di rete, come l'uso di HTTPS, può ridurre l'impatto di un attacco Man-in-the-Middle derivante da ARP Poisoning.
- Monitorare il traffico di rete: Utilizzare software come Wireshark per monitorare la rete alla ricerca di risposte ARP sospette.

Queste soluzioni aiuteranno a ridurre i rischi legati a Null Session e ARP Poisoning, migliorando la sicurezza complessiva della rete.

2. SECONDA PARTE (Ettercap)

2.1 Dettagli dell'Ambiente:

- **Localhost**: Kali Linux
  - **Indirizzo IP**: 192.168.1.18 - 127.0.0.1

Avviamo ETTERCAP, esso ha sia un interfaccia grafica che da riga di comando.

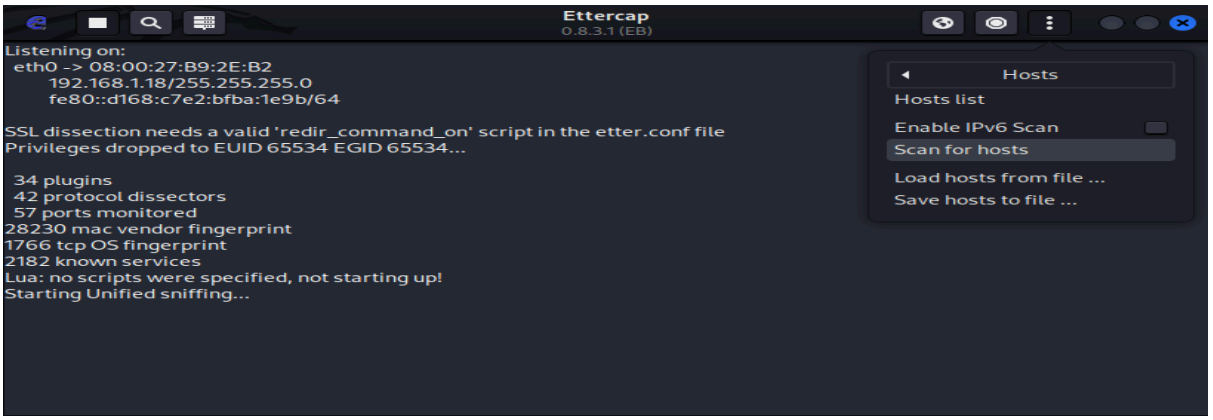
- Screen:

Una volta avviato andiamo a scansionare i nostri target.

Lo scopo di questo attacco è quello di mettersi in mezzo e intercettare tutti i dati non criptati che passano tra due host vittima.

In questo caso ci metteremo in mezzo ad un PC vittima e al nostro Router-Gateway del nostro provider.

- Screen:



2.2 Scansione degli host

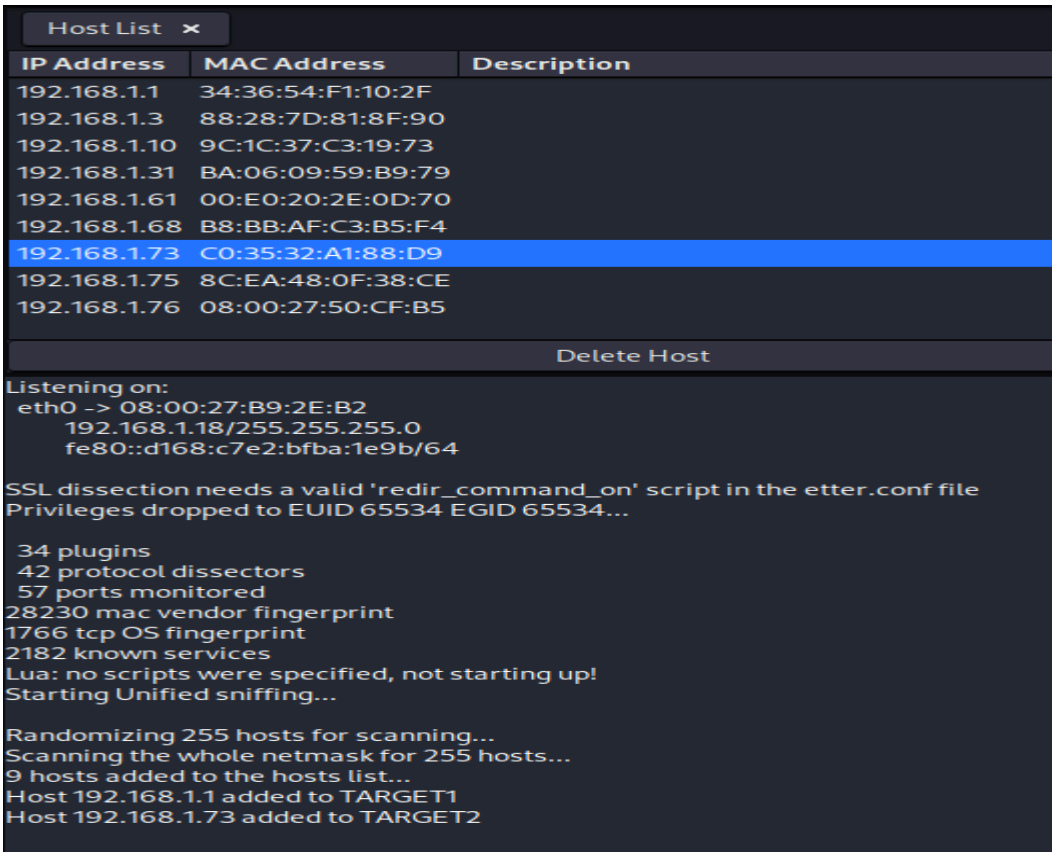
Facciamo click su **Scan for host** e facciamo partire la scansione degli host che abbiamo nella nostra rete. Dopo aver finito la scansione della nostra rete avremmo un risultato simile.

2.3 Assegnazione dei target

I nostri target sono: il gateway del provider (192.168.1.1) e un host vittima, in questo caso il nostro PC (192.168.1.73).

Assegniamo ai due dispositivi ADD TARGET 1 (gateway provider) e ADD TARGET 2 al nostro PC.

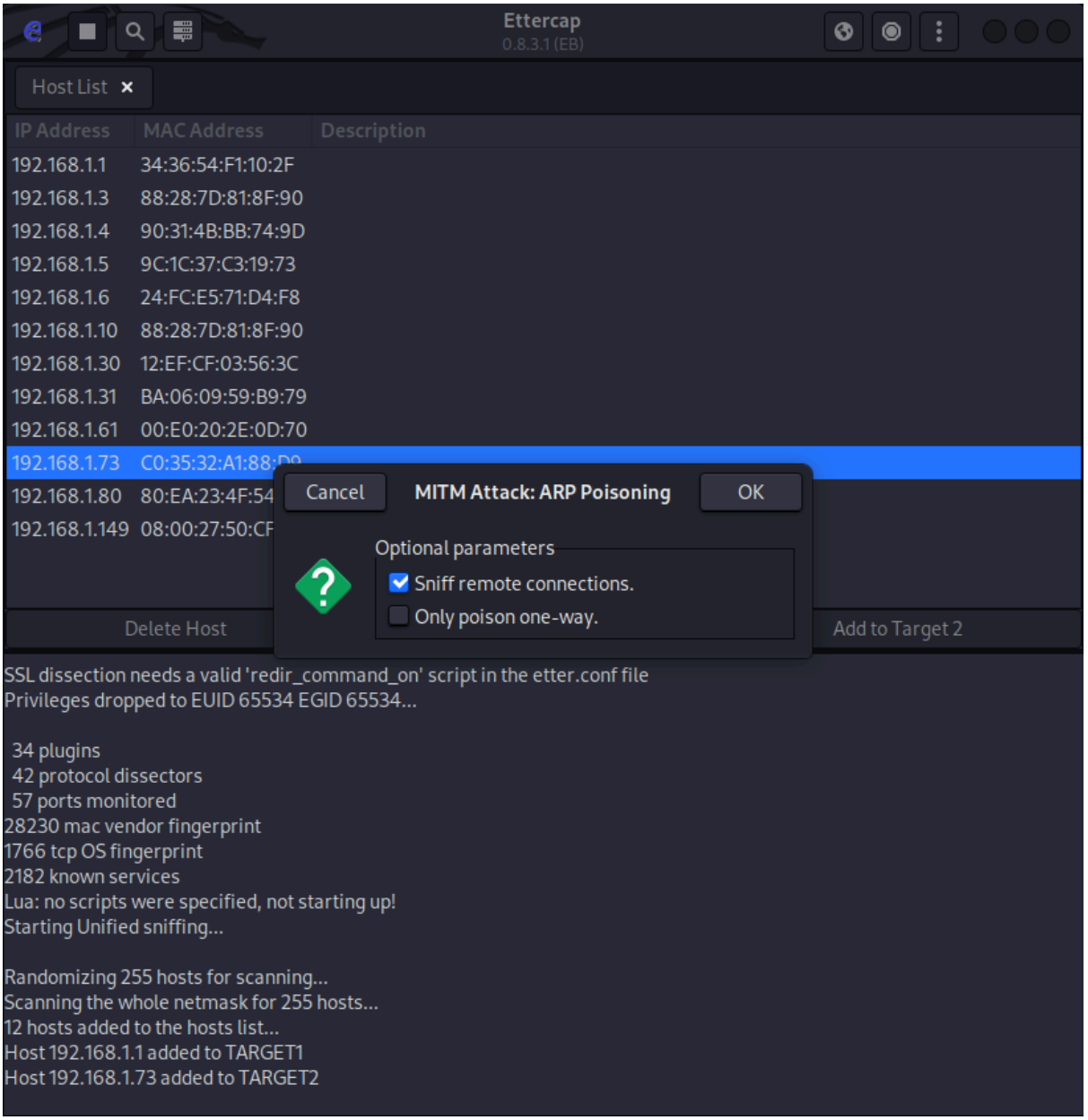
- Screen:



2.4 ARP Poisoning e Intercettazione del Traffico

Andiamo sull'icona del mondo e poi su ARP poisoning, facciamo partire quindi l’attacco.

- Screen:



Notiamo che l' associazione IP - Mac è cambiata da prima. Ora il 192.168.1.1 ha il Mac di Kali.

- Screen:

```
Scheda LAN wireless Wi-Fi:

   Suffisso DNS specifico per connessione: homenet.telecomitalia.it
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::bf7e:ca9f:24ce:cab2%11
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.1.73
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : 192.168.1.1
```

```
Interfaccia: 192.168.1.73 --- 0xb
  Indirizzo Internet    Indirizzo fisico      Tipo
  192.168.1.1           34-36-54-f1-10-2f     dinamico
  192.168.1.18          08-00-27-b9-2e-b2     dinamico
  192.168.1.255         ff-ff-ff-ff-ff-ff     statico
  224.0.0.22            01-00-5e-00-00-16     statico
  224.0.0.251           01-00-5e-00-00-fb     statico
  224.0.0.252           01-00-5e-00-00-fc     statico
  239.255.255.250       01-00-5e-7f-ff-fa     statico
  255.255.255.255       ff-ff-ff-ff-ff-ff     statico
```

```
Interfaccia: 192.168.1.73 --- 0xb
  Indirizzo Internet    Indirizzo fisico      Tipo
  192.168.1.1           08-00-27-b9-2e-b2     dinamico
  192.168.1.18          08-00-27-b9-2e-b2     dinamico
  192.168.1.255         ff-ff-ff-ff-ff-ff     statico
  224.0.0.22            01-00-5e-00-00-16     statico
  224.0.0.251           01-00-5e-00-00-fb     statico
  224.0.0.252           01-00-5e-00-00-fc     statico
  239.255.255.250       01-00-5e-7f-ff-fa     statico
  255.255.255.255       ff-ff-ff-ff-ff-ff     statico
```

2.5 Monitoraggio dei Pacchetti con Wireshark

Vediamo i pacchetti con Wireshark

- Screen: