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.

ATTENZIONE !!!

SVOLGIMENTO PRIMA PARTE:

risposte null session:

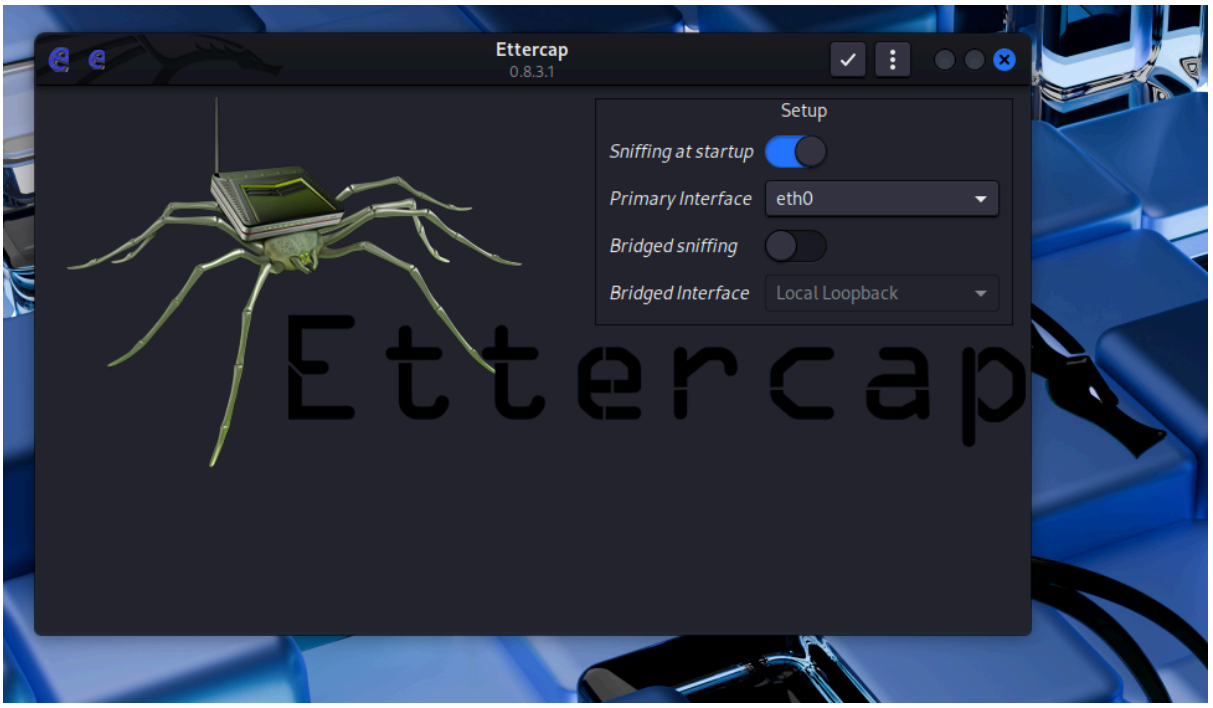
1. La Null Session è una sessione che permette di interagire con un sistema Windows senza dover effettuare l'autenticazione. Tramite la Null Session è possibile ottenere informazioni sul sistema, come l'elenco delle condivisioni e l'elenco degli utenti. questa vulnerabilità di verifica quando un client windows si connette ad un server windows utilizzando una identità vuota/anonima ovvero senza specificare le credenziali di accesso.
2. Sistemi vulnerabili sono: windows NT 2000, windows XP/2003, windows server 2003 windows NT molto vulnerabili sono rari e sono presenti solo in vecchie infrastrutture, windows XP 2003 vulnerabili se non aggiornati sono ancora presenti anche se obsoleti perchè critici per le operazioni aziendali o perché la loro sostituzione comporterebbe costi e sforzi troppo elevati, windows server 2003 sono vulnerabili e ancora presenti in vecchie infrastrutture
3. La prima azione per mitigare è aggiornare questi sistemi obsoleti poiché microsoft rilascia aggiornamenti di sicurezza del sistema operativo così facendo si mitigano i rischi di vulnerabilità.
   Configurare le autorizzazioni nelle condivisioni di file limitando l'accesso alle risorse solo agli utenti che hanno bisogno di questi file, questo limita gli accessi non autorizzati.

Limitare gli accessi attraverso la configurazione di regole di firewall che bloccano gli accessi da connessione remota e non autorizzati filtrando le connessioni in entrata sulla base della porta che tentano di utilizzare.
Disabilitare l'account guest che consente l'accesso alle risorse della rete senza richiedere alcuna credenziale.
Disabilitare il supporto NETbios su TCP/IP: netbios è un vecchio servizio che permette ai computer windows di trovarsi e condividere risorse di rete, quando viene eseguito "su TCP/IP" apre porte e servizi (tipicamente 137–139) che permettono le operazioni di condivisione e in reti non aggiornate, anche connessioni anonime.
Utilizzare software specifici di sicurezza sistemi che possono monitorare e prevenire gli accessi non autorizzati.
Disabilitare la condivisione file e stampanti windows proprio perché la null session sfrutta proprio i servizi di condivisione SMB anche se questa è una soluzione drastica al problema non è molto pratica perchè in sistemi aziendali le persone per lavorare condividono file cartelle o stampanti tra pc.

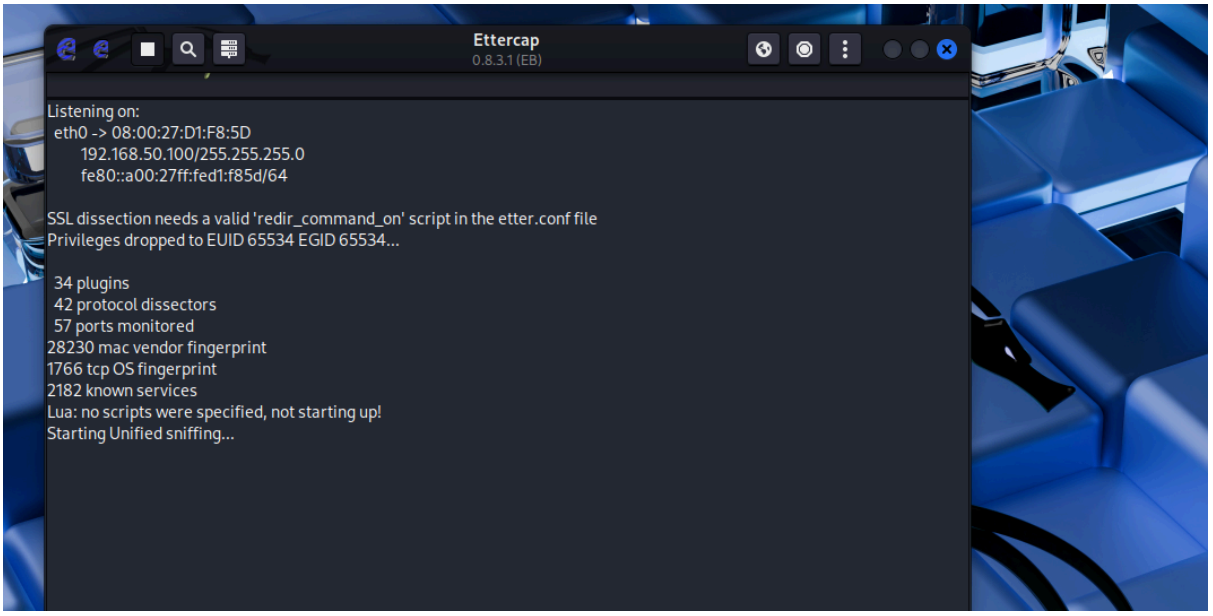
risposte ARP poisoning:

1. ARP poisoning è un attacco in cui un malintenzionato intercetta analizza e manipola il traffico di rete all'interno di una LAN, questo tipo di attacco utilizza il protocollo ARP (address resolution protocol) per inviare pacchetti arp falsi sulla LAN, l'attaccante fa credere che il proprio indirizzo MAC sia associato ad un IP legittimo ciò consente all'attaccante di intercettare il traffico di rete tra le macchine e il router o di dirottare questo traffico ogni volta che una macchina invia un pacchetto al gateway o al router, il traffico destinato al gateway/host passando dall'attaccante gli permette di: modificarlo, intercettarlo o bloccarlo. ARP poisoning colpisce solo i sistemi che fanno parte di una LAN che utilizzano lo stesso gateway e lo stesso indirizzo IP
2. Sono vulnerabili tutti i sistemi che utilizzano ARP non autenticato quindi ogni rete IPv4 locale
3. mitigare rilevare o annullare l'ARP poisoning: utilizzare protocolli sicuri come: HTTPS, SSL, TLS o VPN (virtual private network) crittografando i dati in transito impediscono all'attaccante di leggerli o manipolarli.
   Utilizzare switch di livello 3 costosi ma in questo modo si divide la rete in sottoreti
   Monitoraggio costante, utilizzo di software di sicurezza.
4. Per il monitoraggio esistono in commercio diversi programmi per l'arp poisoning: arpwatch è uno strumento gratuito e open source su sistemi unix/linux, monitora l'attività ARP di una rete LAN, registrando in un database le associazioni tra indirizzi IP e MAC.
   Segnala eventuali cambiamenti, come l'aggiunta di un nuovo host o la modifica di un indirizzo MAC, che possono indicare un tentativo di attacco.Può inviare avvisi via email quando rileva attività anomale.
   Xarp: una utility disponibile per diversi sistemi operativi che aiuta a rilevare e bloccare gli attacchi ARP.
   wireshark: strumento molto utile che analizza i protocolli e può essere utilizzato per rilevare gli attacchi arp attraverso l'analisi del traffico dei pacchetti catturati può mostrare pacchetti arp sospetti.

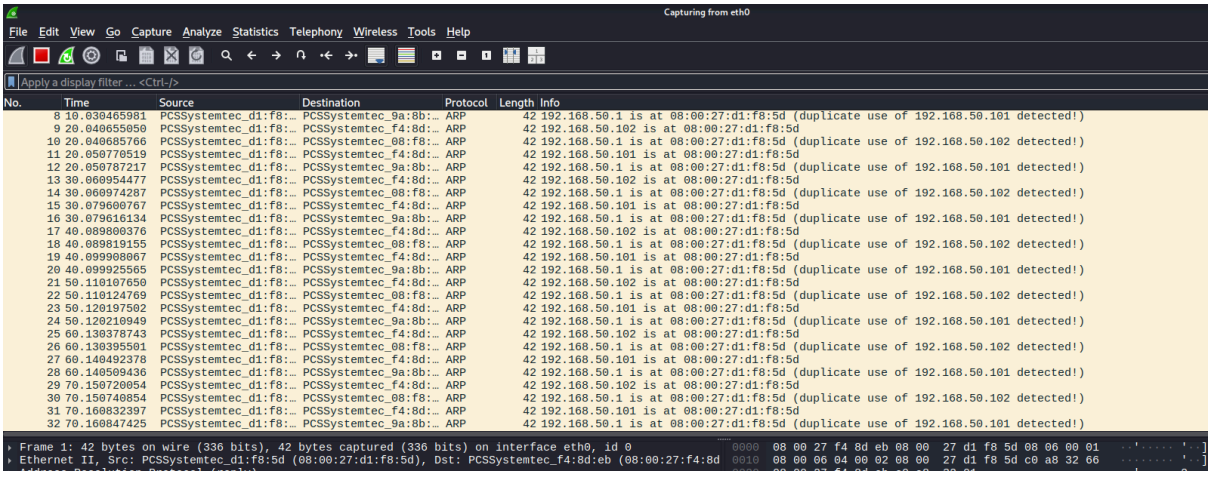
SVOLGIMENTO SECONDA PARTE:



ho avviato il servizio di ettercap



ho cliccato su host poi scan host e ho trovato le macchine



```
ARP poisoning victims:

GROUP 1 : 192.168.50.1 08:00:27:F4:8D:EB

GROUP 2 : 192.168.50.101 08:00:27:9A:8B:1E
GROUP 2 : 192.168.50.102 08:00:27:08:F8:35
Host 192.168.50.1 added to TARGET1
Host 192.168.50.102 added to TARGET2
```

ho aggiunto i target nel primo il gateway e l'host vittima in questo caso la macchina windows

```
┌──(kali㉿kali)-[~]
└─$ arp -a
? (192.168.50.101) at 08:00:27:9a:8b:1e [ether] on eth0
? (192.168.50.1) at 08:00:27:f4:8d:eb [ether] on eth0
? (192.168.50.102) at 08:00:27:08:f8:35 [ether] on eth0

┌──(kali㉿kali)-[~]
└─$ █
```

qui ho avuto un problema nelle slide diceva che il mac address della macchina kali doveva cambiare dopo l'esecuzione di vari comandi arp - a ifconfig non notavo nessuna differenza dopo aver perso molto tempo ho deciso di verificare se l'attacco di arp poisoning era comunque stato eseguito

```
No.   Time          Source                 Destination            Protocol  Length Info
    8 10.030465981  PCSSystemtec_d1:f8:…  PCSSystemtec_9a:8b:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.101 detected!)
    9 20.040655050  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.102 is at 08:00:27:d1:f8:5d
   10 20.040685766  PCSSystemtec_d1:f8:…  PCSSystemtec_08:f8:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.102 detected!)
   11 20.050770519  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.101 is at 08:00:27:d1:f8:5d
   12 20.050787217  PCSSystemtec_d1:f8:…  PCSSystemtec_9a:8b:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.101 detected!)
   13 30.060954477  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.102 is at 08:00:27:d1:f8:5d
   14 30.060974287  PCSSystemtec_d1:f8:…  PCSSystemtec_08:f8:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.102 detected!)
   15 30.079600767  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.101 is at 08:00:27:d1:f8:5d
   16 30.079616134  PCSSystemtec_d1:f8:…  PCSSystemtec_9a:8b:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.101 detected!)
   17 40.089800376  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.102 is at 08:00:27:d1:f8:5d
   18 40.089819155  PCSSystemtec_d1:f8:…  PCSSystemtec_08:f8:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.102 detected!)
   19 40.099908067  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.101 is at 08:00:27:d1:f8:5d
   20 40.099925565  PCSSystemtec_d1:f8:…  PCSSystemtec_9a:8b:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.101 detected!)
   21 50.110107650  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.102 is at 08:00:27:d1:f8:5d
   22 50.110124769  PCSSystemtec_d1:f8:…  PCSSystemtec_08:f8:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.102 detected!)
   23 50.120197502  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.101 is at 08:00:27:d1:f8:5d
   24 50.120210949  PCSSystemtec_d1:f8:…  PCSSystemtec_9a:8b:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.101 detected!)
   25 60.130378743  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.102 is at 08:00:27:d1:f8:5d
   26 60.130395501  PCSSystemtec_d1:f8:…  PCSSystemtec_08:f8:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.102 detected!)
   27 60.140492378  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.101 is at 08:00:27:d1:f8:5d
   28 60.140509436  PCSSystemtec_d1:f8:…  PCSSystemtec_9a:8b:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.101 detected!)
   29 70.150720054  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.102 is at 08:00:27:d1:f8:5d
   30 70.150740854  PCSSystemtec_d1:f8:…  PCSSystemtec_08:f8:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.102 detected!)
   31 70.160832397  PCSSystemtec_d1:f8:…  PCSSystemtec_f4:8d:…  ARP           42 192.168.50.101 is at 08:00:27:d1:f8:5d
   32 70.160847425  PCSSystemtec_d1:f8:…  PCSSystemtec_9a:8b:…  ARP           42 192.168.50.1 is at 08:00:27:d1:f8:5d (duplicate use of 192.168.50.101 detected!)

▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0          0000  08 00 27 f4 8d eb 08 00  27 d1 f8 5d 08 06 00 01
▸ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: PCSSystemtec_f4:8d:eb (08:00:27:f4:8d  0010  08 00 06 04 00 02 08 00  27 d1 f8 5d c0 a8 32 66
```

ho aperto wireshark e ho notato i vari pacchetti arp inviati.

```
HTTP : 192.168.50.1:80 -> USER: Sign+In  PASS:   INFO: http://192.168.50.1/
CONTENT: __csrf_magic=sid%3A7ab5e5e3aef1521929c3f69a91782ef019945284%2C1761334092&usernamefld=adminpfsense&passwordfld=&login=Sign+In

HTTP : 192.168.50.1:80 -> USER: Sign+In  PASS:   INFO: http://192.168.50.1/
CONTENT: __csrf_magic=sid%3A7ab5e5e3aef1521929c3f69a91782ef019945284%2C1761334092&usernamefld=adminpfsense&passwordfld=&login=Sign+In

HTTP : 192.168.50.1:80 -> USER: Sign+In  PASS:   INFO: http://192.168.50.1/
CONTENT: __csrf_magic=sid%3A7ab5e5e3aef1521929c3f69a91782ef019945284%2C1761334092&usernamefld=adminpfsense&passwordfld=&login=Sign+In

HTTP : 192.168.50.1:80 -> USER: Sign+In  PASS:   INFO: http://192.168.50.1/
CONTENT: __csrf_magic=sid%3A7ab5e5e3aef1521929c3f69a91782ef019945284%2C1761334092&usernamefld=adminpfsense&passwordfld=&login=Sign+In

HTTP : 192.168.50.1:80 -> USER: Sign+In  PASS:   INFO: http://192.168.50.1/
CONTENT: __csrf_magic=sid%3A7ab5e5e3aef1521929c3f69a91782ef019945284%2C1761334092&usernamefld=adminpfsense&passwordfld=&login=Sign+In
```

volevo fare il test su vulnweb dalla macchina windows ma non mi apriva il sito ho pensato che ci fosse un problema con qualche regola di firewall impostata ho provato ad accedere al firewall e l’ettercap ha intercettato la ricerca quindi ho pensato di lasciarlo così e di mettere gli screenshot.