

CPTP0524 – W15D1

Null Session, ARP Poisoning, MITM

Prima Parte

Traccia:

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

Traccia:

Ettercap è uno strumento di analisi della rete e di attacco di tipo "Man-in-the-Middle" **MITM**.

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

Prima Parte

● Spiegare brevemente cosa vuol dire Null Session:

- La **Null Session** è un tipo di connessione anonima a un sistema Windows che non richiede credenziali di autenticazione (username e password). Questa vulnerabilità consente l'accesso a risorse di rete condivise, come l'elenco utenti, i gruppi e altre informazioni di sistema, attraverso la condivisione speciale **IPC\$** (Inter-Process Communication). Gli attaccanti possono sfruttare le Null Session per raccogliere informazioni utili a ulteriori attacchi.

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

I sistemi vulnerabili alle **Null Session** includono:

- **Windows NT 4.0**
- **Windows 2000**
- **Windows XP**
- **Windows Server 2003**

Questi sistemi non sono più ufficialmente supportati da Microsoft e non sono in commercio, ma potrebbero ancora essere presenti in ambienti legacy o sistemi industriali.

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

Per mitigare o eliminare la vulnerabilità **Null Session**, si possono adottare le seguenti misure:

1. **Disabilitare le connessioni anonime** modificando il valore del registro di sistema:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA
RestrictAnonymous = 1

2. **Aggiornare il sistema** a versioni moderne di Windows (Windows 10, Windows Server 2016/2019) che non supportano più le Null Session.

3. **Bloccare le porte SMB** (135, 139, 445) per impedire accessi non autorizzati.
4. **Implementare firewall e filtri di rete** per limitare l'accesso alle condivisioni IPC\$.

● **Spiegare brevemente come funziona l'ARP Poisoning:**

L'ARP Poisoning (Address Resolution Protocol Poisoning) è un attacco in cui un aggressore invia risposte ARP falsificate in una rete locale (LAN), facendo sì che il traffico venga reindirizzato a un dispositivo sotto il suo controllo. In questo modo, può intercettare, modificare o interrompere la comunicazione tra dispositivi.

Funzionamento dell'attacco:

1. L'attaccante invia pacchetti ARP falsificati per associare il proprio indirizzo MAC all'IP del gateway o di un host nella rete.
2. Le vittime aggiornano le proprie tabelle ARP con queste informazioni false.
3. Il traffico di rete viene dirottato attraverso l'attaccante, che può intercettarlo (Man-in-the-Middle), modificarlo o bloccarlo.

● **Elencare i sistemi che sono vulnerabili a ARP Poisoning:**

Tutti i sistemi che utilizzano ARP (Address Resolution Protocol) per la risoluzione degli indirizzi MAC-IP sono vulnerabili all'ARP Poisoning, inclusi:

- **Windows** (tutte le versioni senza protezioni avanzate)
- **Linux**
- **macOS**
- **Dispositivi IoT**
- **Switch e router di livello 2 senza protezioni ARP**

Le reti LAN senza misure di sicurezza specifiche sono particolarmente esposte a questo tipo di attacco.

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

Per mitigare e rilevare l'ARP Poisoning si possono adottare le seguenti misure:

Mitigazione:

1. Abilitare il Dynamic ARP Inspection (DAI) sugli switch di rete per filtrare pacchetti ARP sospetti.
2. Usare Static ARP Entries, configurando manualmente gli indirizzi MAC-IP nei dispositivi critici.
3. Segmentare la rete con VLAN, riducendo il raggio d'azione di un attacco.
4. Utilizzare VPN e protocolli sicuri, come HTTPS e SSH, per proteggere i dati in transito.

Rilevazione:

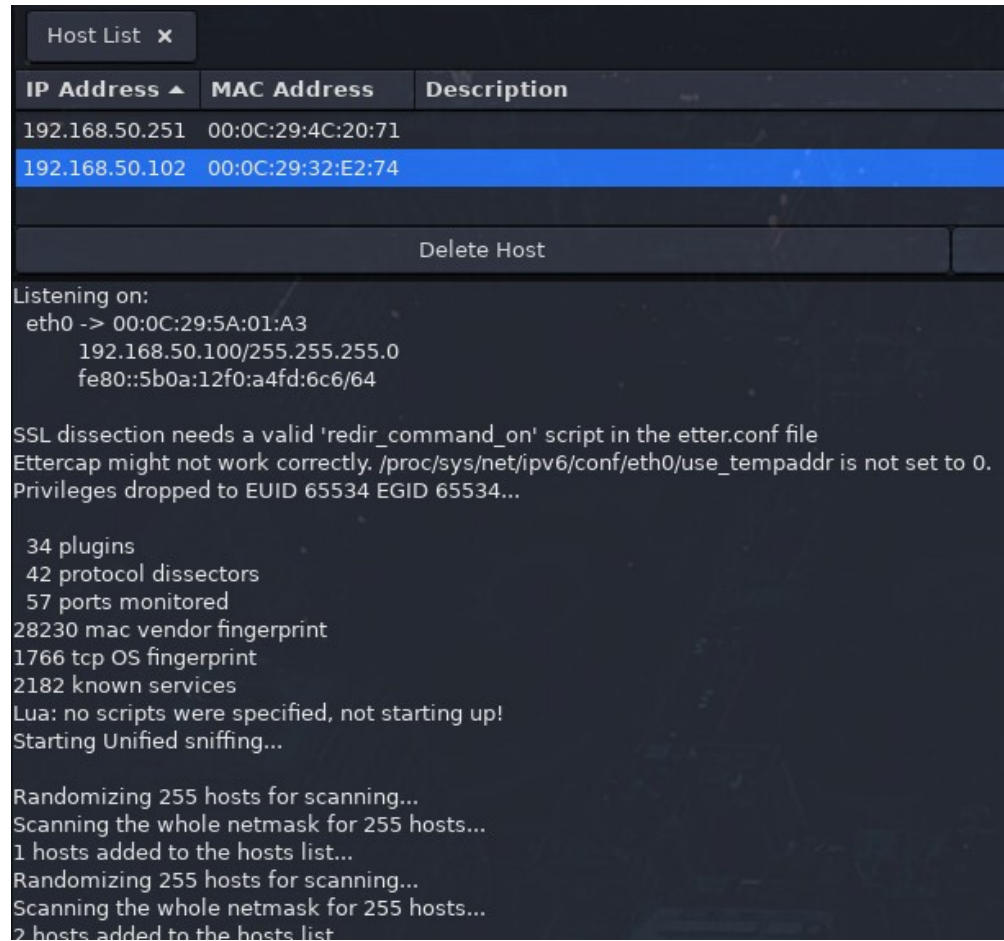
1. Utilizzare strumenti di monitoraggio come Wireshark per rilevare pacchetti ARP anomali.
2. Installare IDS/IPS (Intrusion Detection/Prevention System) come Snort per individuare attacchi ARP.
3. Verificare la tabella ARP manualmente con il comando:
 - Windows: arp -a
 - Linux/macOS: arp -n

Annullamento dell'attacco:

1. Flushare la cache ARP:
 - Windows: arp -d *
 - Linux/macOS: sudo ip -s -s neigh flush all
2. Riavviare il router e riconfigurare le assegnazioni ARP.

Seconda Parte

- Scansione Host con Ettercap



- Controllo Tabella Arp da macchina Attaccante

```
> arp -a  
epi-win10.epicode (192.168.50.102) at 00:0c:29:32:e2:74 [ether] on eth0  
? (192.168.50.251) at 00:0c:29:4c:20:71 [ether] on eth0
```

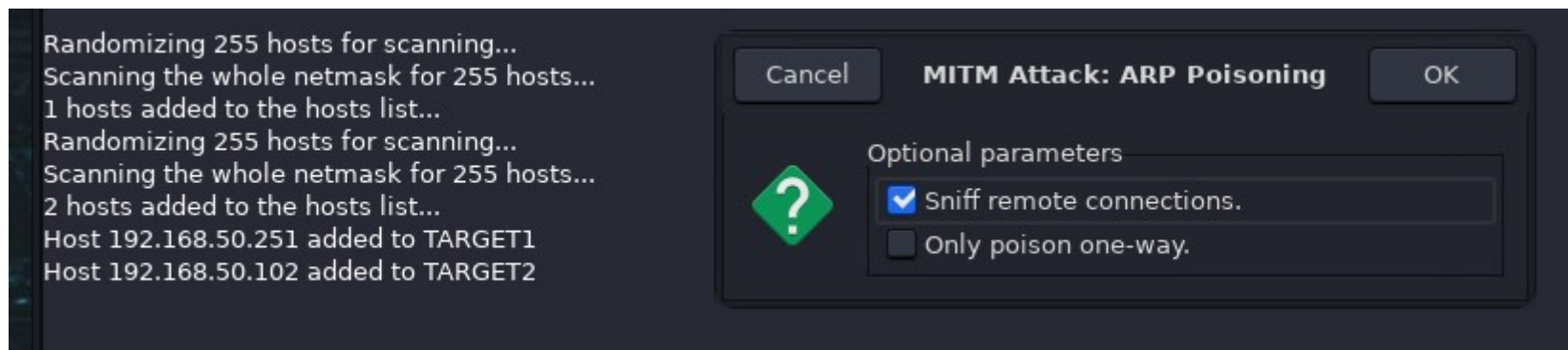
- Scansione Tabella ARP da macchina Target

```
C:\Users\user>arp -a  
  
Interfaccia: 192.168.50.102 --- 0x6  
Indirizzo Internet    Indirizzo fisico    Tipo  
192.168.50.100        00-0c-29-5a-01-a3   dinamico  
192.168.50.251        00-0c-29-4c-20-71   dinamico  
192.168.50.255        ff-ff-ff-ff-ff-ff   statico  
224.0.0.9             01-00-5e-00-00-09   statico  
224.0.0.22            01-00-5e-00-00-16   statico  
224.0.0.252           01-00-5e-00-00-fc   statico  
239.255.255.250       01-00-5e-7f-ff-fa   statico  
  
C:\Users\user>
```

- Aggiunti i dispositivi ARP come target

```
Host 192.168.50.251 added to TARGET1  
Host 192.168.50.102 added to TARGET2
```

- Avvio dell'Attacco



- Scansione Tabella ARP

Si nota perfettamente che nella seconda chiamata arp, la macchina gateway ha preso il MAC Address della Macchina Attaccante

```
C:\Users\user>arp -a

Interfaccia: 192.168.50.102 --- 0x6
   Indirizzo Internet   Indirizzo fisico   Tipo
192.168.50.100         00-0c-29-5a-01-a3   dinamico
192.168.50.251         00-0c-29-4c-20-71   dinamico
192.168.50.255         ff-ff-ff-ff-ff-ff   statico
224.0.0.9              01-00-5e-00-00-09   statico
224.0.0.22             01-00-5e-00-00-16   statico
224.0.0.252            01-00-5e-00-00-fc   statico
239.255.255.250        01-00-5e-7f-ff-fa   statico

C:\Users\user>arp -a

Interfaccia: 192.168.50.102 --- 0x6
   Indirizzo Internet   Indirizzo fisico   Tipo
192.168.50.100         00-0c-29-5a-01-a3   dinamico
192.168.50.251         00-0c-29-5a-01-a3   dinamico
192.168.50.255         ff-ff-ff-ff-ff-ff   statico
224.0.0.9              01-00-5e-00-00-09   statico
224.0.0.22             01-00-5e-00-00-16   statico
224.0.0.252            01-00-5e-00-00-fc   statico
239.255.255.250        01-00-5e-7f-ff-fa   statico
```

- Packet Sniffing con Wireshark

I target hanno il Mac di Kali (Attaccante)

```
42 Who has 192.168.50.251? Tell 192.168.50.100
60 192.168.50.251 is at 00:0c:29:4c:20:71
42 192.168.50.102 is at 00:0c:29:5a:01:a3
42 192.168.50.251 is at 00:0c:29:5a:01:a3 (duplicate use of 192.168.50.102 detected!)
84 Standard query 0xc2d8 A win10.ipv6.microsoft.com
84 Standard query 0xc2d8 A win10.ipv6.microsoft.com
42 192.168.50.102 is at 00:0c:29:5a:01:a3
42 192.168.50.251 is at 00:0c:29:5a:01:a3 (duplicate use of 192.168.50.102 detected!)
42 192.168.50.102 is at 00:0c:29:5a:01:a3
42 192.168.50.251 is at 00:0c:29:5a:01:a3 (duplicate use of 192.168.50.102 detected!)
```

Test su webapp online

<http://testphp.vulnweb.com/login.php>

- Accesso con user = test | password= test

- Output di Ettercap



```
ARP poisoning victims:  
  
GROUP 1 : 192.168.50.251 00:0C:29:4C:20:71  
  
GROUP 2 : 192.168.50.102 00:0C:29:32:E2:74  
HTTP : 44.228.249.3:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php  
CONTENT: uname=test&pass=test
```

- Sniffing con Wireshark

```
File Data: 20 bytes  
▼ HTML Form URL Encoded: application/x-www-form-urlencoded  
  ▶ Form item: "uname" = "test"  
  ▶ Form item: "pass" = "test"
```

- Aggiornamento informazioni Utente (lasciato tutto di default)

← → ↻ ⚠ Non sicuro testphp.vulnweb.com/userinfo.php

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) [Logout test](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

[Logout](#)

Links

[Security art](#)
[PHP scanner](#)
[PHP vuln help](#)
[Fractal Explorer](#)

John Smith (test)

On this page you can visualize or edit you user information.

Name:	<input type="text" value="John Smith"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="email@email.com"/>
Phone number:	<input type="text" value="2323345"/>
Address:	<input type="text" value="21 street"/>

You have 0 items in your cart. You visualize you cart [here](#).

- Sniffing con Wireshark del Inforazioni appena aggiornate

```
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "urname" = "John Smith"
  ▶ Form item: "ucc" = "1234-5678-2300-9000"
  ▶ Form item: "uemail" = "email@email.com"
  ▶ Form item: "uphone" = "2323345"
  ▶ Form item: "uaddress" = "21 street"
  ▶ Form item: "update" = "update"
```

Francesco Rinaldi