Null session e ARP Poisoning

In questo report verranno spiegati i concetti di *Null Session* e *ARP Poisoning*, per poi simulare un ARP Poisoning Attack.

Null Session Vulnerability
Questa vulnerabilità permette a un attaccante di connettersi anonimamente a un sistema Windows senza credenziali, sfruttando configurazioni errate dei servizi di rete come SMB.

Le *Null Session* sono storicamente legate a vulnerabilità nei protocolli di Microsoft.
Oggi siano considerate un rischio passato ma esistono ancora scenari in cui sono presenti:

Sistema	**Vulnerabilità**	**Stato Mercato**
Windows NT/2000	Nativa / Default	Dismessi (End of Life)
Windows Server (Moderni)	Solo se misconfigured	In commercio
Windows 10/11	Estremamente rara (manual)	In commercio
Samba / NAS	Dipende dalla config	In commercio

Mitigation/Remediation di Null Session
Per mitigare o risolvere la vulnerabilità Null Session, l'approccio principale consiste nel limitare l'accesso anonimo alle share di sistema:
- Con l'utilizzo di versioni del protocollo SMB più sicure, disabilitando SMBv1.
- File smb.conf configurato per non permettere l'enumerazione anonima.
- Utilizzo di Group Policy in ambiente Active Directory e filtraggio Firewall.
- Configurazione di Samba (se si gestisce un server Linux).

ARP Poisoning Attack
Un attaccante invia messaggi ARP (Address Resolution Protocol) falsificati all'interno di una rete locale con lo scopo di manipolare la traduzione IP – MAC e intercettare il traffico.

Non colpisce un OS in particolare, ma sfrutta una debolezza nel protocollo ARP, che lo rende "stateless" ovvero senza autenticazione, i dispositivi accettano gli aggiornamenti ARP anche se non li hanno richiesti. Qualsiasi sistema che utilizzi la suite di protocolli TCP/IP su una rete Ethernet o Wi-Fi è potenzialmente vulnerabile.

Detection: Tramite tool specializzati che tengono traccia di accoppiamenti IP-MAC, sistemi IDS/IPS e con un po' di monitoraggio della tabella ARP.

Mitigation: Tramite *Dynamic ARP Inspection,* si configura su Switch per verificare ogni pacchetto ARP rispetto a un database di indirizzi validi, oppure *Port Security* ovvero configurare lo switch per limitare il numero di MAC address permessi su una singola porta fisica, o utilizzando una VPN così da crittografare i dati, anche se spoofati saranno illeggibili.

Recovery: Cosa fare se l'attacco è in corso o è appena terminato? Svuotare la Cache ARP per rimuovere i MAC falsificati, o abilitare l'ARP statico (il computer ignorerà qualsiasi pacchetto ARP che tenti di cambiare gli indirizzi inseriti manualmente).

Simulazione ARP Poisoning con Ettercap

Prima di avviare Ettercap è consigliato vedere la tabella ARP, tramite il comando *arp -a*

```
Interfaccia: 192.168.1.60 --- 0x9
  Indirizzo Internet    Indirizzo fisico      Tipo
  192.168.1.55          32-31-48-66-b6-f6     dinamico
  192.168.1.70          08-00-27-1f-b7-23     dinamico
  192.168.1.254         f4-23-9c-98-d2-b0     dinamico
```

Si può notare come la Kali, avente IP 192.168.1.70 sia presente nella tabella ARP del target, in questo caso la macchina Host dell'ambiente virtuale (192.168.1.60).

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.70/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
```

Avviato Ettercap si procede a scansionare la rete per rilevare gli Endpoint, selezionare il target e selezionare il gateway che anch'esso è target dell'attacco. Ecco gli Endpoint rilevati:

Host List ×

IP Address	MAC Address	Description
192.168.1.60	D8:BB:C1:0C:2E:37	RAZER-CRISCU.local
2001:b07:646d:4455:30b1:274d:ff62:b039	D8:BB:C1:0C:2E:37	RAZER-CRISCU.local
2001:b07:646d:4455:f623:9cff:fe98:d2b0	F4:23:9C:98:D2:B0	
fe80::a00:27ff:fe80:4c57	08:00:27:80:4C:57	
192.168.1.61	08:00:27:80:4C:57	
fe80::f623:9cff:fe98:d2b0	F4:23:9C:98:D2:B0	
192.168.1.254	F4:23:9C:98:D2:B0	

I due target (macchina Host e Gateway), aventi IP 192.168.1.60 e 192.168.1.254, andranno aggiunti alle voci TARGET1 e TARGET2 di Ettercap.

```
Host 192.168.1.60 added to TARGET1
Host 192.168.1.254 added to TARGET2
```

Avviando l'ARP Poisoning si potrà effettuare un **MITM** (Man In The middle)

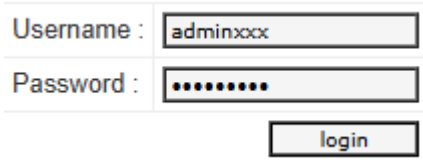
```
ARP poisoning victims:

GROUP 1 : 192.168.1.60 D8:BB:C1:0C:2E:37

GROUP 2 : 192.168.1.254 F4:23:9C:98:D2:B0
```

Per effettuare una prova di Spoofing ci si potrà avvalere di un qualsiasi sito in http, in modo da vedere il traffico in chiaro. Per questa simulazione si ha utilizzato il sito http://testphp.vulnweb.com/login.php

Provando ad effettuare il login si potranno leggere in chiaro user e password indirizzati a Kali




```
HTTP : 44.228.249.3:80 -> USER: adminxxx  PASS: pswsicura  INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=adminxxx&pass=pswsicura
```

Controllando la tabella ARP della macchina host adesso si potrà notare che il MAC del gateway ora risulta essere uguale al MAC di kali, se si facesse lo stesso controllo sulla tabella ARP del gateway si vedrebbe che la macchina host ha lo stesso MAC address di kali.

```
Interfaccia: 192.168.1.60 --- 0x9
  Indirizzo Internet    Indirizzo fisico      Tipo
  192.168.1.70          08-00-27-1f-b7-23     dinamico
  192.168.1.254         08-00-27-1f-b7-23     dinamico
```

È stato così possibile intercettare il traffico Host → Internet e Internet → Host, i pacchetti anche se indirizzati alla Kali vengono poi comunque reindirizzati al destinatario originale attraverso il forwarding che il kernel di Kali attua automaticamente.