

W15D1 – NULL SESSION (anonymous logon)

Le *null session* sono vulnerabilità dello share di Windows (cartelle, file) e che sono ancora presenti in numerosi contesti aziendali. Tramite gli attacchi *null session* si possono recuperare informazioni dal target come ad esempio: password, programmi aperti, nomi utente di sistema ecc... perchè il sistema non richiede credenziali di autenticazione. Sfruttando questa vulnerabilità l'attaccante può connettersi da remoto utilizzando una condivisione amministrativa locale o remota.

Possiamo ancora trovare sistemi vulnerabili a questo attacco che sono:

windows explorer.exe;

windows xp 2003;

Samba linux/unix;

Le azioni di rimedio per questo tipo di vulnerabilità possono essere la rimozione del protocollo SMBV1 ovvero un protocollo obsoleto che permetteva ad un client di scrivere e leggere file su un server e non supporta la crittografia dei dati oppure l'utilizzo di chiavi LSA per impedire l'enumerazione delle share e l'enumerazione degli account.

Sono ovviamente necessarie anche attività di aggiornamento dei sistemi oppure blocco definitivo di utilizzo di attrezzature ormai obsolete.

ARP POISONING

Attacco che consiste nella manipolazione della tabella Arp cache che traduce i Mac address in indirizzi IP. Tramite questo attacco si possono inviare pacchetti ARP manipolati cosicché il traffico destinato ad un indirizzo MAC venga fatto deviare sull'indirizzo dell'attaccante. In questo modo l'attaccante intercetta, modifica, legge, il traffico di rete tra due host. (man in the middle)

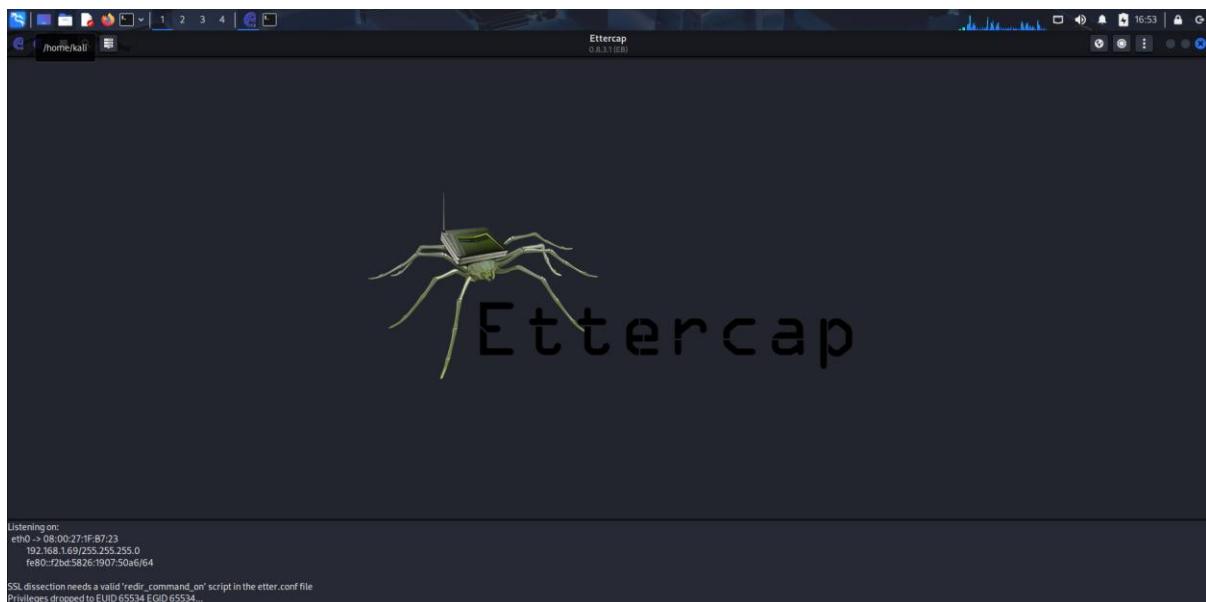
Le azioni di rimedio per evitare attacchi di questo comprendono: pulizia della cache, utilizzo di port security che imita il numero di indirizzi MAC che possono connettersi a una singola porta dello switch impedendo a un attaccante di inviare tante richieste; utilizzo di firewall per rilevare gli attacchi, utilizzo di protocollo https.

Esercizio con il tool ETTERCAP

Si utilizza il tool ettercap come strumento di attacco di tipo Man in the middle per intercettare comunicazioni, analisi di rete o attacchi di spoofing.

Per l'esercizio facciamo partire una scansione degli hosts sulla nostra rete

Indirizzo ip kali



Risultato scansione

A screenshot of a Windows command prompt window titled "Prompt dei comandi". The window shows the results of a ping scan and an ARP dump. The ping results show responses from 192.168.1.69 and 192.168.1.156. The ARP dump shows a list of MAC addresses and their types. At the bottom, there is a taskbar with icons for File Explorer, Google Chrome, and others, along with system status information like battery level and date/time.

```
C:\Users\user>ping 192.168.1.69

Indirizzi. Se non è presente, verrà utilizzata la prima
interfaccia utilizzabile.

Esempio:
> arp -s 192.168.1.222 00:aa:00:62:c6:09 ....Aggiunge una voce statica.
> arp -a .....Visualizza la tabella ARP.

C:\Users\user>ping 192.168.1.69

Esecuzione di Ping per 192.168.1.69 con 32 byte di dati:
Risposta da 192.168.1.69: bytes=32 durata=2ms TTL=64

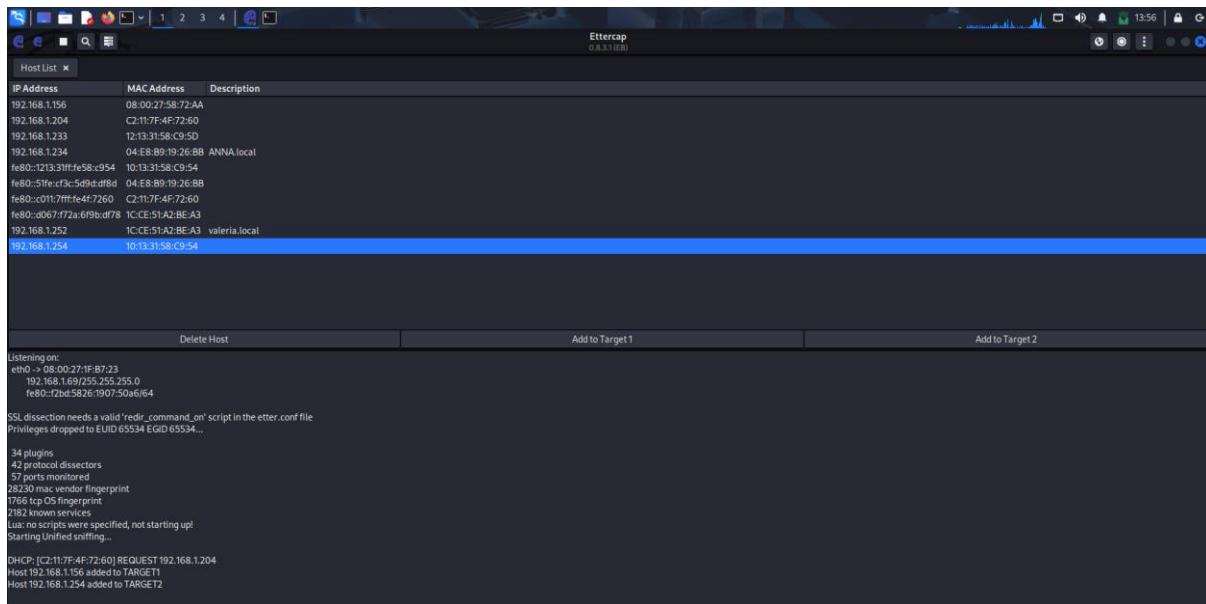
Statistiche Ping per 192.168.1.69:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Percentuale di perdite (0% persi),
Tempo approssimativo di ritorno minimo/medio/massimo in millisecondi:
Minimo = 1ms, Massimo = 2ms, Medio = 1ms

C:\Users\user>arp -a

Interfaccia: 192.168.1.156 --- 0x4
Indirizzo Internet Indirizzo fisico Tipo
192.168.1.156 00:00:00:00:00:00 dinamico
192.168.1.254 10:13:31:58:c9:54 dinamico
192.168.1.255 ff:ff:ff:ff:ff:ff statico
224.0.0.1 01:00:5e:00:00:01 statico
224.0.0.9 01:00:5e:00:00:09 statico
224.0.0.22 01:00:5e:00:00:16 statico
224.0.0.251 01:00:5e:00:00:f1 statico
239.255.255.252 01:00:5e:7f:ff:ff statico
239.255.255.250 01:00:5e:7f:ff:fa statico
255.255.255.255 ff:ff:ff:ff:ff:ff statico

C:\Users\user>
```

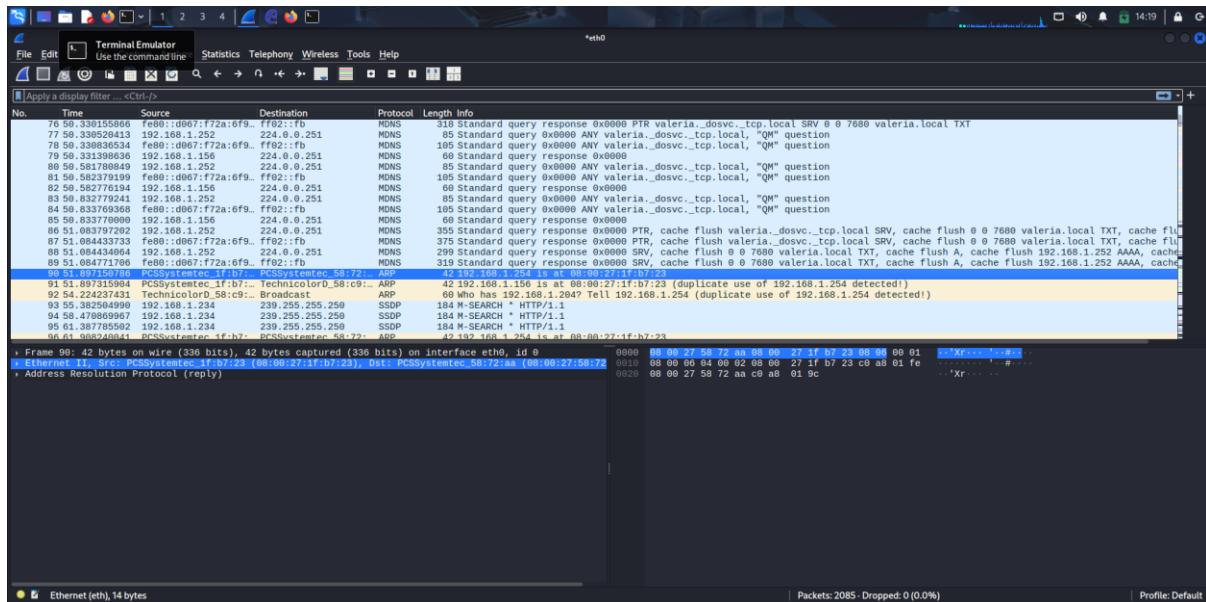
Troviamo l'ip della windows 192.168.1.156, il gateway 192.168.1.254 con mac address 10:13:31:58:C9:54 e l'ip 192.168.1.69 della kali con mac address 08:00:27:1f:b:23



Adesso lanciamo l'attacco arp poisoning e vediamo che il mac address del gateway è cambiato ed è identico a quello della kali. L'attacco è riuscito in quanto lo scopo era proprio quello di intercettare la comunicazione andando a modificare i mac address che permettono all'attaccante di interporsi tra due host e sniffare le comunicazioni.

```
Administrator:~ C:\Users\user>arp -s 192.168.1.156 00:0c:29:cd:0d:0d 1
Administrator:~ C:\Users\user>arp -a
C:\Users\user>ping 192.168.1.69
Pinging 192.168.1.69 with 32 bytes of data:
Reply from 192.168.1.69: bytes=32 time=1ms TTL=64
Administrator:~ C:\Users\user>arp -a
Interfaccia: 192.168.1.156 ... 0x4
Indirizzo Internet Indirizzo fisico Tipo
192.168.1.156 00:0c:29:cd:0d:0d dinamico
192.168.1.254 10:03:15:58:c9:54 dinamico
192.168.1.255 ff:ff:ff:ff:ff:ff statico
224.0.0.2 01:00:5e:00:00:02 statico
224.0.0.9 01:00:5e:00:00:09 statico
224.0.0.22 01:00:5e:00:00:16 statico
224.0.0.251 01:00:5e:00:00:f0 statico
224.0.0.252 01:00:5e:00:00:f1 statico
239.252.255.250 01:00:5e:7f:ff:fa statico
255.255.255.255 ff:ff:ff:ff:ff:ff statico
Administrator:~ C:\Users\user>
```

Si ha la controprova con wireshark e dunque si lancia una cattura per osservare i pacchetti trovati



si vede come il gateway ha preso il mac address della kali.

Ora si cerca di andare su una pagina web vulnerabile per tentare un altro attacco

The screenshot shows a web browser window with the following details:

- Address Bar:** testphp.vulnweb.com/login.php
- Page Title:** Acunetix acuart
- Form Fields:**
 - Username:
 - Password:
 - Login:
- Note:** You can also sign up here. Signup disabled. Please use the username **test** and the password **test**.
- Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and learn manual hacking techniques as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

```
Listening on:
eth0 -> 08:00:27:1F:87:23
192.168.1.69/255.255.255.0
fe80::7ba4:5626%1907:50a6/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcOS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
6 hosts added to the hosts list...
HTTP :44.228.249.3.80 -> USER: mario PASS: rossi INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=mario&pass=rossi
```

Vediamo come siamo riusciti ad intercettare una comunicazione ed ad ottenere username e password per entrare in una pagina web privata.