CONSEGNA W15D2

Traccia:

Prima parte Rispondere ai seguenti quesiti: Esercizio Traccia

- 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.

PRIMA PARTE

Null Session è un tipo di connessione non autenticato ai servizi di Windows mentre ARP Poisoning è un attacco che va a modificare la tabella ARP con lo scopo di intercettare il traffico di rete. Entrambe sono vulnerabilità che vanno a colpire le reti non protette ma i cui effetti possono essere mitigati configurando correttamente i firewall e usando strumenti di sicurezza adeguati.

1.Null Session è una vulnerabilità che consente di attaccare un dispositivo Windows permettendo di entrare in possesso di dati come gli accessi di account. Si verifica quando vi è una comunicazione tra un client e un server Windows, ma quando il primo è fondamentalmente una identità vuota ossia non ha effettuato alcun tipo di accesso tramite credenziali.

I sistemi operativi vulnerabili sono sostanzialmente sistemi che Microsoft non supporta più quali ad esempio Windows XP, Vista, 2000 o anche ad esempio Server 2003.

Per mitigare questo tipo di attacco basta:

1Disabilitare la condivisione file e stampanti su Windows: eliminare completamente la condivisione su tutti i computer e server della rete. Questa è una soluzione che nelle aziende però non può essere utilizzata in quanto queste ultime generalmente usano la condivisione dei file a livelli aziendali.

2.Configurare correttamente il firewall: rete: i firewall bloccano i tentativi di connessione remota non autorizzati e filtrano le connessioni in ingresso sulla base delle porta che tentano di utilizzare

3.Aggiornare a versioni più recenti di Windows: versioni che sono in costante aggiornamento da parte di Windows

4.Disattivare l'account Guest: visto che l'account guest consente l'accesso alle risorse della rete senza richiedere alcuna credenziale

5.Configurare le autorizzazioni di condivisione file: limitando in questo modo l'accesso alle risorse solamente a pochi utenti che effettivamente hanno bisogno di usare determinate risorse evitando in questo modo potenziali accessi non autorizzati.

6.Utilizzare un software di sicurezza: usare un software di sicurezza per i sistemi Windows in grado di monitorare e prevenire l'accesso non autorizzato.

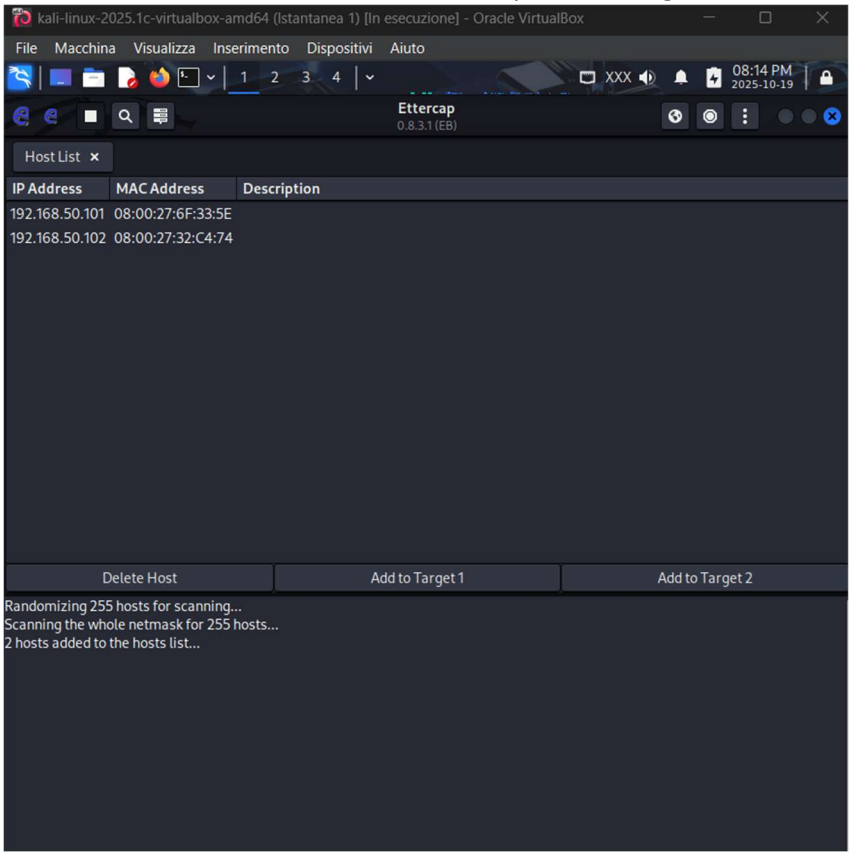
2.ARP Poisoning è un attacco che sfrutta l'assenza di autenticazione nel protocollo ARP. In questo attacco ARP invia false risposte allo scopo di associare il proprio MAC all'IP di un altro Host usando la tecnica Man-In-the-Middle al fine quindi di intercettare il traffico di rete tra macchine o con lo scopo di dirottare il traffico di rete ogni volta che una macchina invia il pacchetto al gateway o al router.

Questo genere di attacco colpisce esclusivamente i sistemi all'interno di una LAN, quindi macchine che operano sotto lo stesso gateway. Quindi tutti gli utenti sotto la stessa rete saranno vulnerabili a questo tipo

di attacco. Tutti i dispositivi che utilizzano una LAN che usa una IPv4 e ARP quindi ad esempio i dispositivi Windows, Linux e MacOS.
Per mitigare questo tipo di attacco esistono vari modi:
1.Utiilizzo di protocolli di sicurezza: usare protocolli che crittografano i dati in transito e impediscono agli attaccanti di leggere e di manipolare questi ultimi. Un esempio di protocolli di questo genere sono HTTPS, SSL o anche VPN
2.Usare uno switch livello 3: dividendo in questo modo la rete in sottoreti
3.Monitoraggio costante: controllare costantemente la rete allo scopo di individuare eventuali intrusioni, come accessi non autorizzati o eventuali attacchi (come ad esempio ARP Poisoning appunto)
4.Utilizzo di software di sicurezza: usare appunto alcuni software antivirus e anti-malware possono individuare e prevenire attacchi
5.Educazione del personale: Informare gli utenti sulla sicurezza informativa e sui rischi di attacchi. Informare gli utenti che non tutto il traffico può essere lecito.

SECONDA PARTE

Diversi produttori di software offrono anche dei programmi di monitoring con i quali si possono controllare le reti e rilevare i procedimenti ARP insoliti.
Andiamo ad utilizzare ETTERCAP.
Dopo averlo avviato e tenendo le altre macchine create accese avviamo una scansione e vediamo come sin da subito riusciamo a riconoscere tutti i dispositivi collegati alla rete.



Vediamo dopo attraverso i comandi arp i vari address collegati e vediamo dalla foto come corrispondano ai 3 ip address che sono collegati sulla stessa linea e sono rispettivamente la macchina kali, la seconda che corrisponde a Windows Vista e l'altro che è Metasploitable.

```
┌──(kali㉿kali)-[~]
└─$ arp -e
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.50.1                     (incomplete)                              eth0
192.168.50.102           ether   08:00:27:32:c4:74   C                     eth0
192.168.50.101           ether   08:00:27:6f:33:5e   C                     eth0

┌──(kali㉿kali)-[~]
└─$ arp -a
? (192.168.50.1) at <incomplete> on eth0
? (192.168.50.102) at 08:00:27:32:c4:74 [ether] on eth0
? (192.168.50.101) at 08:00:27:6f:33:5e [ether] on eth0
```

Facciamo in seguito una scansione dei pacchetti tramite Wireshark, osserviamo i pacchetti ARP. Dall'intercettazione avvenuta vediamo come Ettercap ha avviato correttamente l'attacco ARP Poisoning infatti il pacchetto evidenzia una collisione di indirizzi segno che Ettercap si è inserito nella comunicazione. Il nostro MITM è attivo in quanto stiamo impersonando un host e il sistema lo rileva come conflitto come confermato da Wireshark.