Attacchi alle reti

Agenda
Le NULL Session
I tool per enumerazione share
ARP Poisoning

Le NULL Session

Una delle vulnerabilità storiche delle share di Windows sono le NULL session.
Share → cartelle condivise
Gli attacchi «null session» si possono utilizzare per recuperare dalla macchina target molte informazioni. Un attaccante, infatti, può riuscire a recuperare informazioni quali:

- Password
- Utenti di un sistema
- Gruppi di un sistema
- Processi in esecuzione
- Programmi aperti

→ si possono sfruttare da remoto
→ attacchi tramite API o RPC (Remote Procedure Call)
→ si basano su una vulnerabilità dell'autenticazione delle share amministrative di Windows → colelgamento senza autenticazione

nbtstat: è un tool da riga di comando per Windows per enumerare le share dato un determinato obiettivo.
Con il comando **nbtstat /?**, possiamo vedere come si utilizza il tool. Riportiamo l'output nella figura qui a destra. L'utilizzo più comune è con lo switch –A seguito dall'IP che visualizza le informazioni su un determinato target. Ad esempio:

```
Visualizza le statistiche di protocollo e le connessioni TCP/IP
correnti mediante NBT (NetBIOS su TCP/IP).

NBTSTAT [ [-a NomeRemoto] [-A indirizzo IP] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [intervallo] ]

  -a   (stato scheda)  In base al nome specificato il nome, elenca
                       la tabella dei nomi del computer remoto
  -A   (Stato scheda)  In base all'indirizzo IP specificato, elenca
                       la tabella dei nomi del computer remoto.
  -c   (cache)         Elenca la memoria cache di NBT dei nomi remoti
                       [computer] e dei relativi indirizzi IP
  -n   (nomi)          Elenca i nomi NetBIOS locali.
  -r   (risolti)       Elenca i nomi risolti mediante broadcast e WINS
  -R   (Ricaricamento) Ripulisce la tabella dei nomi cache remota
                       e la ricarica
  -S   (Sessioni)      Elenca la tabella delle sessioni con gli indirizzi
                       IP di destinazione
  -s   (sessioni)      Elenca la tabella delle sessioni che converte
                       gli indirizzi IP di destinazione in nomi
                       computer  NETBIOS.
  -RR  (Agg.Rilascio)  Invia pacchetti di rilascio nome a WINS,
                       quindi avvia l'aggiornamento

  Nome Remoto    Nome del computer host remoto.
  Indirizzo IP   Notazione decimale puntata dell'indirizzo IP.
  intervallo     Rivisualizza le statistiche selezionate, interrompendo
                 per un numero di secondi pari all'intervallo tra ogni
                 visualizzazione. Premere Ctrl+C per interrompere la
                 visualizzazione delle statistiche.
```

```
>nbtstat -A 10.130.40.80

Local Area Connection:
Node Padres: [10.0.2.15] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    ELS-WINXP      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    ELS-WINXP      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered

    MAC Address = 00-0C-29-BF-98-BD
```

Vediamo da vicino l'output del comando.
La prima riga della tabella di suggerisce che il nome del PC con indirizzo 10.130.40.80 è «ELS-WINXP»

Il record type <00> indica che il PC è una workstation, mentre il tipo «UNIQUE» ci dice che questo computer ha solo un indirizzo IP assegnato.


```
>nbtstat -A 10.130.40.80

Local Area Connection:
Node Padres: [10.0.2.15] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    ELS-WINXP      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    ELS-WINXP      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered

    MAC Address = 00-0C-29-BF-98-BD
```

La seconda linea, inclusa nel rettangolo in rosso, contiene il gruppo di lavoro oppure il dominio al quale appartiene il computer (in questo caso è un gruppo di lavoro).

La terza riga, evidenziata dal rettangolo in blu, è una riga particolarmente interessante.

Il record di tipo <20> ci informa che il servizio di condivisione su quella data macchina è attivo, e che quindi possiamo provare a recuperare qualche informazione utile sul computer.

```
>nbtstat -A 10.130.40.80

Local Area Connection:
Node Padres: [10.0.2.15] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    ELS-WINXP      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    ELS-WINXP      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered

    MAC Address = 00-0C-29-BF-98-BD
```

Quando un attaccante sa che una macchina ha il servizio di file Server attivo, può enumerare gli share utilizzando il comando NET VIEW. La figura sotto riporta il comando net view verso il target 10.130.40.80

Queste due righe rappresentano due directory condivise dalla macchina in esame

```
>NET VIEW 10.130.40.80
Shared resources at 10.130.40.80

Share name      Type  Used as  Comment
-------------------------------------------
eLS             Disk
WIA_RIS_SHARE   Disk
The command completed successfully.
```

I tool che abbiamo visto finora sono tool per Windows. E' possibile fare enumerazione delle share anche da un computer con Linux, utilizzando i tool forniti dalla suite Samba.

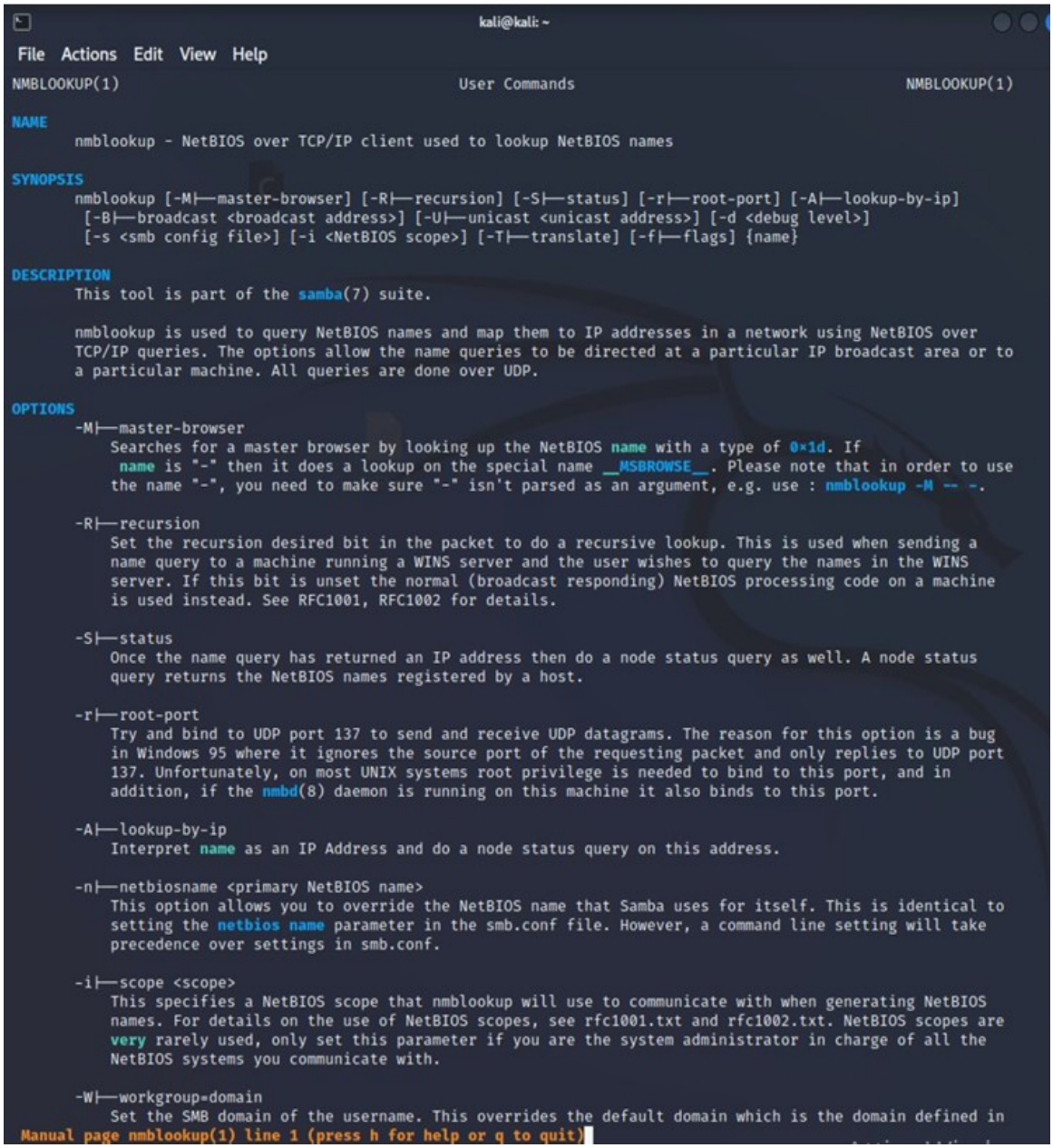
Gli strumenti della suite Samba sono preinstallati su Kali Linux, ma sono anche disponibili praticamente per tutte le altre distribuzioni Linux.
Per lanciare le stesse operazioni che abbiamo visto con nbtstat, si può utilizzare nmblookup. Al netto del comando stesso, la sintassi è molto simile a quella già vista per nbtstat.

```
nmblookup -A <target ip address>
```

Potete utilizzare il manuale di nmblookup, oppure l'help rapido con lo switch --help, come in figura in basso. Nell'immagine di fianco, è riportato l'output del comando nmblookup sul target 10.130.40.80 analizzato in precedenza. Notate come i risultato sono gli stessi:

```
$ nmblookup -A 10.130.40.80
Looking up status of 10.130.40.80
        ELS-WINXP       <00> -         M <ACTIVE>
        WORKGROUP       <00> - <GROUP> M <ACTIVE>
        ELS-WINXP       <20> -         M <ACTIVE>
        WORKGROUP       <1e> - <GROUP> M <ACTIVE>

        MAC Address = 00-0C-29-BF-98-BD
```



La suite Samba fornisce un ulteriore tool, ovvero **smbclient**.

Smbclient è un client simile a ftp per accedere alle share di Windows.
Questo tool è in grado, tra le altre cose, di fare enumerazione delle share di un host con riferimento alla figura in basso:

- -L, permette di visualizzare quali servizi sono disponibili sul target
- //, l'indirizzo IP deve essere preceduto da due slash
- -N, fa in modo che il tool non chieda una password

Come potete vedere dalla figura qui a destra, smbclient non solo riporta tutte le share identificate dai tool che abbiamo visto in precedenza.

Ma mostra anche le share amministrative che vengono nascoste dagli strumenti standard di Windows per ragioni di sicurezza.

```
$ smbclient -L //10.130.40.80 -N
Domain=[ELS-WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

        Sharename       Type      Comment
        ---------       ----      -------
        eLS             Disk
        IPC$            IPC       Remote IPC
        WIA_RIS_SHARE   Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
Domain=[ELS-WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
```

Dopo aver stabilito che il servizio condivisione file è attivo ed aver enumerato gli share disponibili su un dato target, è il momento di capire se l'attacco basato sulle null session sia possibile.

Per verificarlo, possiamo provare a sfruttare la share amministrativa IPC$, cercando di avviare una connessione senza credenziali valide.

La prima cosa che dobbiamo fare è collegarci alla share IPC$, utilizzando un nome utente ed una password vuoti. Possiamo farlo in diversi modi:

- Con il comando **NET USE**

```
> NET USE \\<target IP address>\IPC$ '' /u:''
```

- Con il comando **smbclient**

```
# smbclient //10.130.40.80/IPC$ -N
```

Un altro tool per Linux per sfruttare vulnerabilità del tipo «null session» è Enum4Linux. Come di consueto possiamo consultare l'help del comando per capire il suo utilizzo.

Tra gli switch più significativi troviamo:
«**–S**» che permette di enumerare le share di una macchina, compresi le share amministrative.
«**-U**» che permette di estrarre i nomi utente
«**-P**» che permette di controllare le password policy. Può essere poi utilizzato per configurare un attacco all'autenticazione su rete.

```
┌──(kali㉿kali)-[~]
└─$ enum4linux
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com).  Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This option is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,guest,krbtgt,d
)
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
    -o        Get OS information
    -i        Get printer information
    -w wrkg   Specify workgroup manually (usually found automatically)
    -n        Do an nmblookup (similar to nbtstat)
    -v        Verbose.  Shows full commands being run (net, rpcclient, etc.)
    -A        Aggressive. Do write checks on shares etc

RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
access: Allow anonymous SID/Name translation" enabled (XP, 2003).

NB: Samba servers often seem to have RIDs in the range 3000-3050.
```

Attiva Wind
Passa a Imposta

ARP Poisoning

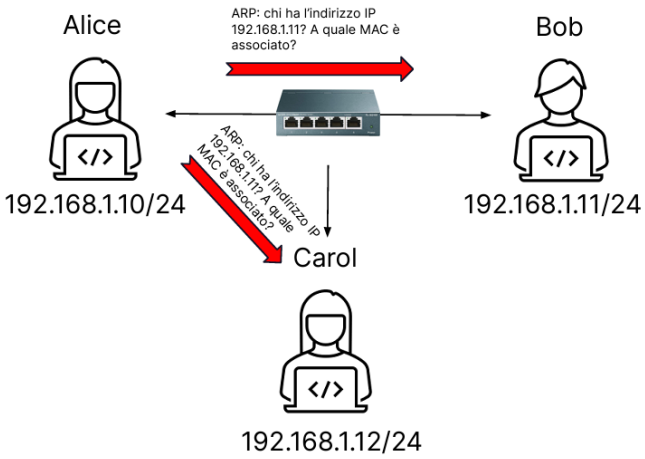
→ è un attacco che si può utilizzare per intercettare del traffico su una rete basata su switch.

Come abbiamo visto nel modulo delle reti, un host deve conoscere il MAC address del next hop quando invia un pacchetto IP.

Il next hop potrebbe essere qualsiasi device, anche un router, uno switch oppure l'host di destinazione.

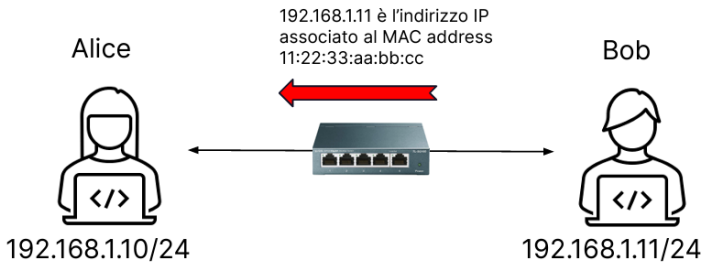
Per identificare il MAC address, gli host su una rete utilizzano il protocollo ARP – Address Resolution Protocol.

ARP è un protocollo fondamentale per le reti, tramite ARP un host, Alice nel nostro caso, può costruire le associazioni tra IP e MAC.
Ipotizziamo che Alice voglia inviare un pacchetto a Bob, che è sulla stessa rete, Alice conosce l'IP di Bob ma non ne conosce il MAC. Alice creerà una richiesta ARP contenente l'IP di Bob e lo invierà a tutti i nodi della rete **utilizzando il MAC Address di broadcast,** richiedendo associazione IP / MAC.



Importante: l'indirizzo MAC FF:FF:FF:FF:FF:FF è l'indirizzo MAC di broadcast. Gli indirizzi di broadcast servono per inviare simultaneamente un messaggio a tutti i nodi della rete

Bob, che ha l'IP richiesto da Alice, risponderà con il suo MAC address.
Così, Alice avrà recuperato il MAC address di Bob e sarà pronta ad inviarle la comunicazione.
Alice salverà la coppia IP – MAC nella propria ARP cache, una tabella con le coppia IP – MAC salvata localmente per futuri utilizzi.



Se un attaccante trova il modo di manipolare la tabella «ARP cache», potrebbe essere in grado di ricevere del traffico destinato ad altri indirizzi, e quindi sniffare eventualmente comunicazioni riservate.

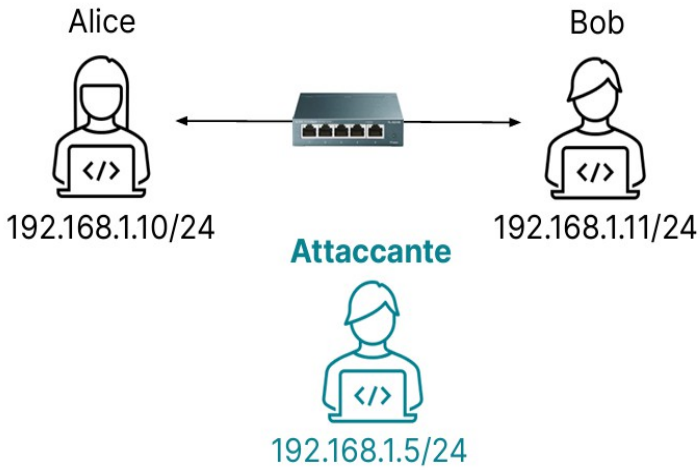
Inoltre, fintanto che l'indirizzo MAC di destinazione resta all'interno della tabella ARP cache, l'attaccante può continuare ad intercettare liberamente il traffico.

Manipolando le tabelle ARP delle due entità coinvolte in una comunicazione bidirezionale, un utente malevolo potrebbe essere in grado di intercettare e dirottare la comunicazione. Questo tipo di attacchi è anche chiamato **MITM – Man in the middle**.

In un attacco di tipo ARP poisoning, partecipano 3 attori principali:

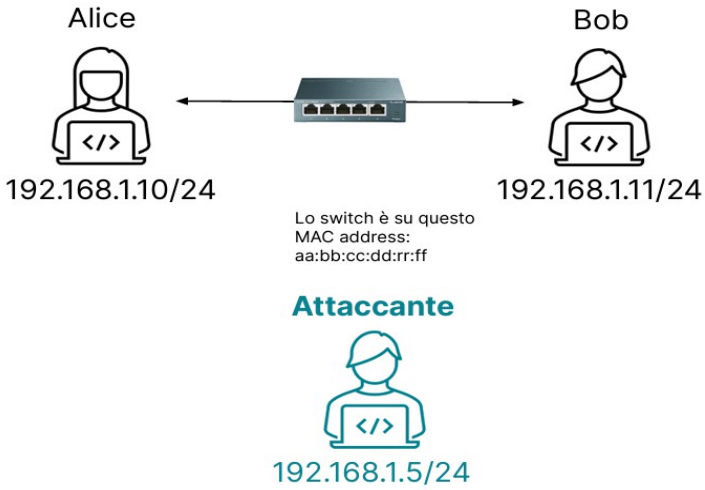
- Due nodi della rete, ad esempio client, server, router, stampanti ed altro
- L'attaccante

L'attaccante è in grado di modificare la tabella ARP degli altri host inviando delle risposte ARP non richieste (Gratuitous ARP). In pratica, l'attaccante invia delle risposte ARP senza aspettare che un host invii una richiesta ARP, per modificare volutamente le tabelle ARP degli host sulla rete.



Prendiamo come esempio la figura: la comunicazione tra Alice e Bob passa per lo switch.

Che succede se l'attaccante invia delle richieste ARP per modificare le tabelle ARP di Alice e Bob in modo tale da far risultare l'IP dello switch associato al suo Mac address? Semplice, tutte le future comunicazioni tra Alice e Bob non passeranno più per lo switch, ma passeranno per la macchina dell'attaccante che potrà sniffare le comunicazioni.



Vediamo uno strumento per mettere in pratica un attacco ARP poisoning.

dsniff (https://www.kali.org/tools/dsniff/) è una collezione di tool per il network auditing e penetration testing. Al suo interno contiene l'utility **arpspoof**, un'utility progettata per intercettare il traffico su una LAN basata su switch.
Prima di lanciare il tool è necessario abilitare l'IP forwarding del Kernel Linux, ovvero la funzione che trasforma un computer Linux in una sorta di router.
Abilitando l'IP forwarding, la vostra macchina sarà in grado di inoltrare alla destinazione corretta i pacchetti che intercetterà. Il comando per abilitare l'IP forwarding è il seguente:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
# arpspoof -i <interface> -t <target> -r <host>
```

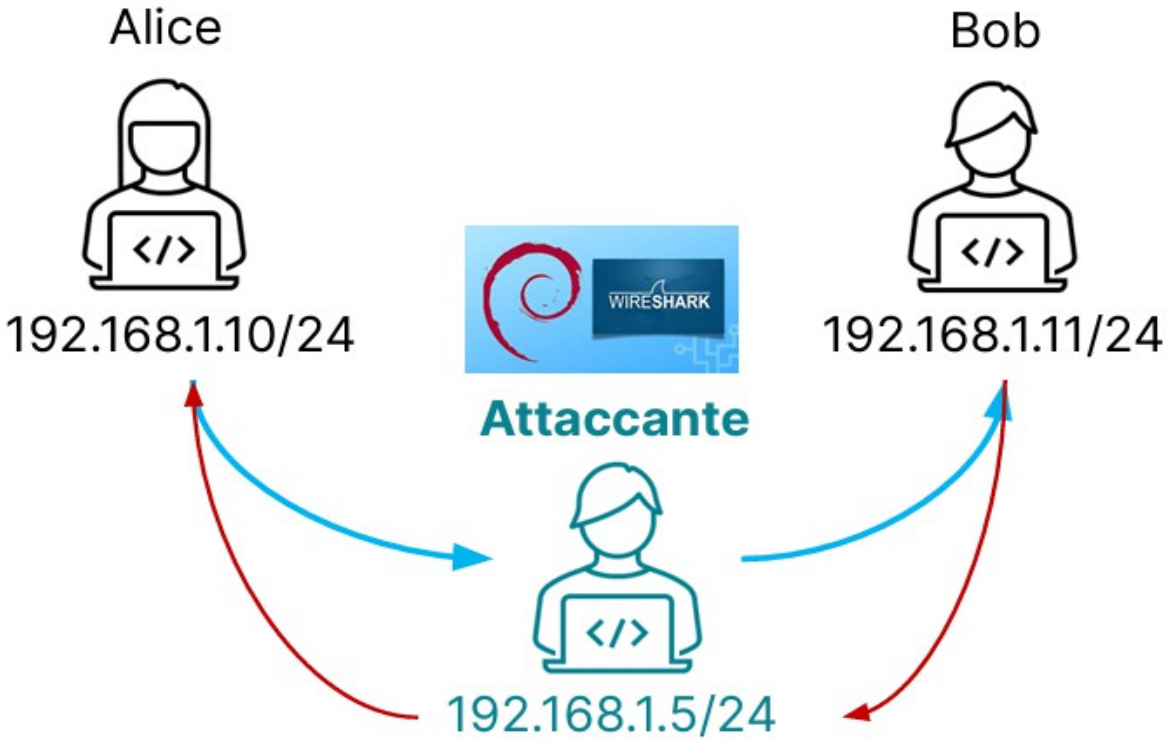
Una volta eseguito il comando per attivare l'IP forwarding, si può eseguire arpspoof
Dove:
-i, ci permette di specificare l'interfaccia di rete, ad esempio la nostra eth0 o eth1, o altro nome dipendentemente dalla vostra configurazione
Target, Host, sono gli indirizzi delle vittime dell'arpspoof

Ad esempio, ipotizziamo di voler sniffare il traffico tra l'ip 192.168.4.11 e l'ip 192.168.4.16

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
# arpspoof -i eth0 -t 192.168.4.11 -r 192.168.4.16
```

Una volta che ci siamo messi tra i due ip, e abbiamo fatto in modo di far passare il traffico per la nostra macchina, possiamo attivare Wireshark per sniffare tutte le comunicazioni.

La comunicazione tra Alice e Bob passerà per la vostra macchina, che avendo attivato l'ip forwarding trasmetterà il traffico al destinatario corretto. Nel frattempo, potete attivare Wireshark per intercettare l'intero flusso. Per Alice e Bob sarà tutto trasparente in quanto loro continueranno a ricevere correttamente i pacchetti.



W15D1 - Pratica (1)
Null session
Nella lezione teorica abbiamo visto la Null Session, vulnerabilità che colpisce Windows

Traccia
• Spiegare brevemente cosa vuol dire Null Session
• Elencare i sistemi che sono vulnerabili a Null Session
• Questi sistemi operativi esistono ancora oppure sono estinti da anni e anni?
• Elencare le modalità per mitigare o risolvere questa vulnerabilità
• Commentare queste azioni di mitigazione, spiegando l'efficacia e l'effort per l'utente/azienda.

W15D1 - Soluzione (1)
La vulnerabilità Null Session su Windows è una vulnerabilità di sicurezza che consente a un attaccante di accedere a informazioni sensibili sui sistemi Windows, come nomi di account utente, password e informazioni di condivisione delle risorse. Questa vulnerabilità si verifica quando un client Windows si connette a un server Windows utilizzando un'identità vuota, ovvero senza specificare alcuna credenziale di accesso.

La vulnerabilità Null Session colpisce i sistemi operativi Windows NT, Windows 2000, Windows XP e Windows Server 2003. Tuttavia, è importante notare che è stata risolta in versioni successive dei sistemi operativi Windows e che molti amministratori di sistema di Windows hanno adottato misure di sicurezza per mitigare questa vulnerabilità.

Per mitigare questa vulnerabilità, è possibile adottare i seguenti metodi:

1. Disabilitare la condivisione file e stampanti su Windows: eliminare completamente la condivisione su tutti i computer e server della rete. Estirpo il problema alla radice, ma le aziende usano la condivisione dei file e non è un ottima risoluzione
2. Disabilitare il supporto per NetBIOS su TCP/IP: questo riduce il numero di porte aperte sul sistema e rimuove il supporto per il protocollo NetBIOS che è vulnerabile alla null session.
3. Utilizzare il filtro del traffico di 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. Il monitoraggio di rete è una delle pratiche di sicurezza sempre raccomandate
4. Disattivare l'account Guest: l'account guest consente l'accesso alle risorse della rete senza richiedere alcuna credenziale. Disabilitare l'account Guest può limitare l'accesso di utenti non autorizzati. Certamente un'ottima soluzione, da applicare in ogni caso
5. Aggiornare il sistema operativo: Microsoft rilascia regolarmente gli aggiornamenti di sicurezza per il sistema operativo Windows. Assicurarsi di aver installato l'ultimo aggiornamento di sicurezza per mitigare i rischi di vulnerabilità. Con una pach l'effort per l'azienda è basso. Passare ad un sistema operativo più moderno è oneroso a livello di configurazione e richieste hardware
6. Configurare le autorizzazioni di condivisione file: limita l'accesso alle risorse ai soli utenti specifici che ne hanno bisogno, utilizzando i permessi appropriati. Questo evita il potenziale accesso non autorizzato. Certamente un ottimo sistema e una best practice in ogni caso, non sempre applicato nelle aziende medio/piccole
7. Utilizzare un software di sicurezza: implementare un software di sicurezza per i sistemi Windows che possa monitorare e prevenire l'accesso non autorizzato. Fa parte delle soluzioni base da applicare sempre

   Possono esserci anche altre azioni di mitigazione, ad esempio intervenire sul registro di Windows

W15D1 - Pratica (2) ARP Poisoning

Nella lezione teorica abbiamo visto l’attacco ARP Poisoning
Traccia
• Spiegare brevemente come funziona l’APR Poisoning
• Elencare i sistemi che sono vulnerabili a APR Poisoning
• Elencare le modalità per mitigare, rilevare o annullare questo attacco
• Commentare queste azioni di mitigazione, spiegando l’efficacia e l’effort per l’utente/azienda.

W15D1 - Soluzione (2)

L'attacco ARP Poisoning è una tecnica malevola utilizzata per intercettare, analizzare o manipolare il traffico di rete all'interno di una LAN (rete locale). Questo attacco sfrutta il protocollo ARP (Address Resolution Protocol) per inviare informazioni ARP false sulla rete, promuovendo il proprio indirizzo MAC come il legittimo indirizzo MAC del router o di un altra macchina. 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.

L'attacco ARP Poisoning colpisce esclusivamente i sistemi all'interno di una LAN, in particolare tutte le macchine che utilizzano lo stesso gateway e lo stesso indirizzo IP di rete. In altre parole, gli utenti all'interno della stessa rete locale saranno vulnerabili all'attacco ARP Poisoning.

Esistono diverse tecniche per mitigare questo tipo di attacco:

1. Utilizzo di protocolli di sicurezza: i protocolli come HTTPS, SSL, TLS o VPN crittografano i dati in transito e impediscono agli attaccanti di leggerli o manipolarli.
2. Utilizzare Switch livello 3: in questo modo si divide la rete in sottoreti, ma gli switch layer 3 hanno un costo maggiore e richiedono configurazione.
3. Monitoraggio costante: controllare regolarmente la rete per individuare eventuali intrusioni, come accessi non autorizzati o attacchi di ARP poisoning.
4. Utilizzo di software per la sicurezza: alcuni software antivirus e anti-malware possono individuare e prevenire attacchi ARP poisoning.
5. Educazione del personale: informare gli utenti sulla sicurezza informatica e sui rischi di attacchi come l'ARP poisoning può aiutare a prevenire incidenti. Informare gli utenti che non tutto il traffico può essere lecito.

Monitoraggio di rete

Diversi produttori di software offrono anche dei programmi di monitoring con i quali si possono controllare le reti e rilevare i procedimenti ARP insoliti. Ad esempio:

Arpwatch

XArp

Altrimenti possiamo usare l’**IDS Snort** per effettuare il monitoraggio