

MITM con password sniffer

Premessa:

Il progetto è stato sviluppato a scopo didattico e testato su reti e dispositivi privati di mio possesso, senza arrecare danno a cose o persone esterne, e su siti appositamente dedicati. Per ragioni di sicurezza gli indirizzi MAC verranno oscurati totalmente o parzialmente.

Termini utili:

Di seguito verranno esplicitati concetti e termini utili alla piena comprensione della relazione.

MITM: per MITM o Man-In-The-Middle si intende una tipologia di attacchi informatici nei quali il criminale intercetta il traffico di rete tra due dispositivi frapponendosi segretamente tra essi in modo tale che essi credano di comunicare direttamente.

Nodo: con “nodo” si intendono tutti gli apparecchi in grado di comunicare connessi ad una rete come computer, stampanti, switch, hub e molti altri. Verranno utilizzati come sinonimi i termini “apparecchio”, “dispositivo” o “macchina”.

MAC: l'indirizzo MAC o Media Access Control è un indirizzo univoco per ogni nodo. È composto da 12 caratteri separati da “:”, i primi 6 indicano la compagnia che ha creato dell'interfaccia di rete e i restanti sono unici per ogni dispositivo. Quest'ultima caratteristica rende gli indirizzi MAC estremamente importanti in quanto identificano un apparecchio in modo univoco.

IP: l'Internet Protocol è un protocollo di livello tre o network nel modello ISO/OSI. Viene utilizzato per indirizzare e instradare le comunicazioni tra nodi di una stessa rete.

ARP: l'ARP o Address Resolution Protocol è un protocollo di livello due o data-link nel modello ISO/OSI. Questo protocollo è molto utilizzato nelle reti LAN che permette di mappare gli indirizzi MAC dei nodi di una rete coi rispettivi IP. Si compone di due principali frame:

- ARP Request: frame inviato dal richiedente in broadcast sulla rete contenente l'indirizzo IP del quale si vuole conoscere l'indirizzo MAC.
- ARP Reply: frame inviato dal nodo interrogato al richiedente contenente l'indirizzo MAC del dispositivo.

Spoofing: attacco informatico nel quale il criminale si fa identificare come un altro nodo della rete.

Sniffer: software malevolo utilizzato nei crimini informatici per rilevare informazioni e/o credenziali di accesso, come username, e-mail e password, contenuti nei pacchetti inviati e ricevuti dalla vittima.

Nmap: software molto diffuso nella sicurezza informatica che permette di scansionare i dispositivi in una rete e le loro porte.

Macchina Virtuale: una macchina virtuale è un ambiente virtuale con componenti hardware virtuali che permette di utilizzare un sistema operativo e i relativi software senza intaccare la macchina ospitante.

Hypervisor: un hypervisor è un software in grado di creare e gestire ambienti virtuali, simulando componenti hardware e software, e separandoli dalla macchina ospitante, ossia la macchina sulla quale viene avviato l'hypervisor.

Scapy: libreria di python e software che permette di comporre e inviare pacchetti di vari tipi e livelli come i frame ARP.

IP Forwarding: l'IP Forwarding è un protocollo che permette di riconoscere quando un pacchetto ricevuto è destinato a un altro nodo e inviarlo ad esso di conseguenza.

Funzionamento:

L'attacco MITM è stato effettuato da una macchina virtuale con sistema operativo Linux, su hypervisor Oracle VM Virtualbox, alla comunicazione tra una macchina con sistema operativo Windows e il router.

Per mettere in atto l'attacco è stato utilizzato un ARP spoofer. Un ARP spoofer è un software che permette di identificarsi all'interno di una rete con l'indirizzo MAC di un altro nodo.

Il primo passaggio è quello di ottenere l'indirizzo IP delle due vittime, in questo caso la macchina Windows e il router. L'IP del router è solitamente il primo indirizzo dopo quello di rete che nel nostro caso sarà 192.168.0.1. Se l'IP della macchina Windows non è noto, si può ricorrere a un software di scansione delle reti come Nmap.

Col comando "nmap -O networkIP/CIDR" scansioniamo la rete:

```
(root@kali)-[~]
# nmap -O 192.168.0.0/24

Nmap scan report for skyhub4.Home (192.168.0.1)
Host is up (0.00089s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE      SERVICE
22/tcp    filtered  ssh
23/tcp    filtered  telnet
53/tcp    open       domain
80/tcp    open       http
111/tcp   filtered  rpcbind
443/tcp   open       https
8080/tcp   filtered  http-proxy
8181/tcp   filtered  intermapper
9000/tcp   filtered  cslistener

Nmap scan report for fissoMatteo.Home (192.168.0.234)
Host is up (0.00018s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE      SERVICE
135/tcp    open       msrpc
139/tcp    open       netbios-ssn
445/tcp    open       microsoft-ds
5357/tcp   open       wsdapi
MAC Address: (Micro-Star Intl)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10|XP (91%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows Server 2019 (91%), Microsoft Windows
10 1909 (90%), Microsoft Windows XP SP3 (85%), Microsoft Windows XP SP2 (85%
)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Grazie alla scansione sono stati trovati, tra i vari dispositivi, il router con IP 192.168.0.1, come da ipotesi, e una macchina Windows con IP 192.168.0.234.

Tramite l'utilizzo della libreria Scapy vengono inviati due ARP Request per ottenere gli indirizzi MAC dei due nodi.

Possiamo quindi visualizzare le ARP Reply:

```

1 <Ether
2 dst=08:00:27
3 src=00:a3:88
4 type=ARP
5
6 <ARP
7 hwtype=Ethernet (10Mb)
8 ptype=IPv4
9 hwlen=6
10 plen=4
11 op=is-at
12 hwsrc=00:a3:88:
13 psrc=192.168.0.1
14 hwdst=08:00:27
15 pdst=192.168.0.19
16
17 <Padding
  load='\x00\x00\x00\x00\x00\x00\x00\x00\x00'
  x00' >

```

```

1 <Ether
2 dst=08:00:27
3 src=2c:f0:5d
4 type=ARP
5
6 <ARP
7 hwtype=Ethernet (10Mb)
8 ptype=IPv4
9 hwlen=6
10 plen=4
11 op=is-at
12 hwsrc=2c:f0:5d
13 psrc=192.168.0.234
14 hwdst=08:00:27
15 pdst=192.168.0.19
16
17 <Padding
  load='\x00\x00\x00\x00\x00\x00\x00\x00\x00'
  x00' >

```

Nella figura di sinistra vediamo l'ARP Reply del router mentre in quella di destra l'ARP Reply della macchina Windows.

Ottenuti gli indirizzi, vengono inviati due ARP Reply: una verso il router fingendo di essere la macchina Windows, quindi con indirizzo IP e MAC della sorgente uguali a quelli della macchina Windows; e una verso la macchina Windows fingendosi il router.

Dato che le ARP Request e Reply tra router e nodi vengono inviate ogni 15 secondi, per mantenere l'ARP spoofing bisogna inviare i frame in loop con time-out inferiore a 15 secondi.

Per fare in modo che le vittime ricevano lo stesso i pacchetti bisogna abilitare l'IP Forwarding.

Tramite il prompt dei comandi sulla macchina Windows possiamo visualizzare l'ARP cache contenente tutti gli IP e i rispettivi indirizzi MAC:

```

Interfaccia: 192.168.0.234 --- 0x10
Indirizzo Internet    Indirizzo fisico      Tipo
192.168.0.1           00-a3-88-            dinamico
192.168.0.19          08-00-27-            dinamico

```

Come possiamo vedere il primo indirizzo, ossia l'IP del router, ha indirizzo MAC diverso dal secondo, che è invece la macchina Linux del criminale.

Quando viene avviato l'ARP spoofer vengono visualizzati gli stessi indirizzi MAC:

```

Interfaccia: 192.168.0.234 --- 0x10
Indirizzo Internet    Indirizzo fisico      Tipo
192.168.0.1           08-00-27-            dinamico
192.168.0.19          08-00-27-            dinamico

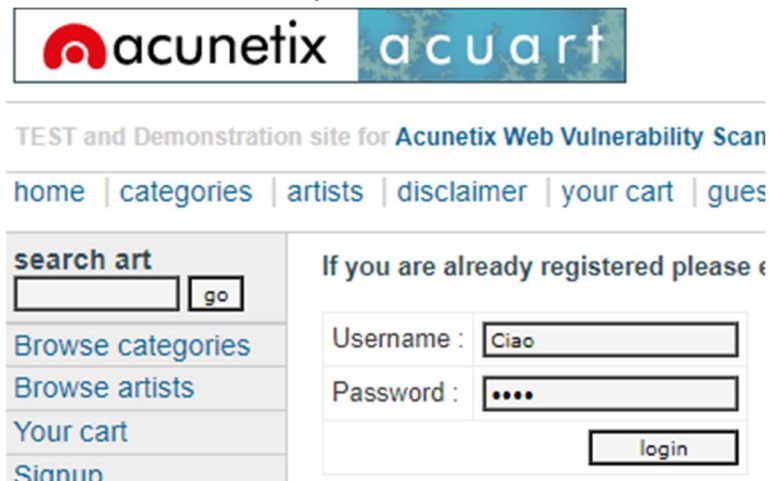
```

Mentre l'ARP spoofer è in funzione, si possono eseguire diverse operazioni di sniffing del traffico di rete come il password sniffing.

Il password sniffing viene eseguito analizzando i pacchetti HTTP in entrata e in uscita e cercando nel “body” delle corrispondenze con parole chiave note come pass, password, passwd, email, username, uname e molti altri.

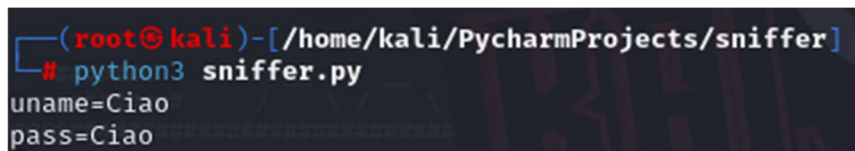
Per simulare un accesso è stato utilizzato il sito <http://testphp.vulnweb.com/login.php> di Acunetix sviluppato appositamente per simulare un sito vulnerabile e svolgere test di sicurezza.

Utilizzando con username “Ciao” e come password “Ciao” visualizzeremo questo:



The screenshot shows the Acunetix test site interface. At the top, there's a logo for 'acunetix' and 'acu art'. Below it, a navigation bar contains links: 'home', 'categories', 'artists', 'disclaimer', 'your cart', and 'gues'. A search bar labeled 'search art' is on the left. On the right, there's a login section titled 'If you are already registered please'. It contains a 'Username' field with the value 'Ciao', a 'Password' field with masked characters (dots), and a 'login' button. Below the search bar, there are links for 'Browse categories', 'Browse artists', 'Your cart', and 'Sign up'.

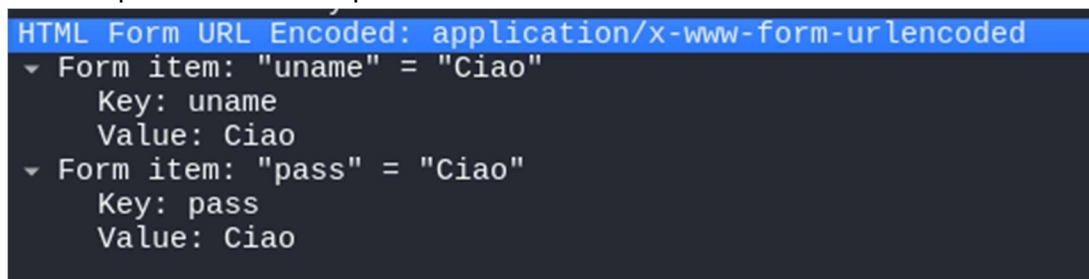
Figura 1: Visuale dal sito di Acunetix



```
(root@kali)-[/home/kali/PycharmProjects/sniffer]
# python3 sniffer.py
uname=Ciao
pass=Ciao
```

Figura 2: Visuale dal terminale

Utilizzando il software per l'analisi dei pacchetti Wireshark possiamo vedere il contenuto del pacchetto nei quali username e password sono in chiaro:



The screenshot shows the raw data of an HTTP form submission in Wireshark. The top line is 'HTML Form URL Encoded: application/x-www-form-urlencoded'. Below it, the form data is expanded, showing two items: 'Form item: "uname" = "Ciao"' and 'Form item: "pass" = "Ciao"'. Each item shows the key and value, with the value being 'Ciao' for both.

Codici:

I codici dei rispettivi programmi e la loro spiegazione si possono trovare [qui](#).

Vulnerabilità:

Il programma sfrutta prima di tutto la bassa sicurezza del protocollo ARP che è facilmente infettabile da un criminale per eseguire MITM, ARP poisoning e altri attacchi. Per quanto riguarda lo sniffer, questo sfrutta la mancanza di sicurezza nei siti internet sprovvisti di HTTPS o che inviano le password e gli username degli utenti “in chiaro”, ossia senza sistemi di crittografia come MD5 o SHA, tramite PHP.

Come difendersi:

Per bloccare attacchi di tipo ARP spoofer è possibile installare vari tool in grado di rendere il protocollo ARP più sicuro, per esempio, integrando SSL/TLS o delle whitelist per mantenere una MAC table più solida rispetto alla cache ARP.

Lo sniffer, invece, funziona solo su siti che utilizzano HTTP e inviano le credenziali con PHP i quali sono ormai difficili da trovare in quanto risulta molto facile abilitare tecnologie di crittografia piuttosto che utilizzare protocolli come HTTPS o sHTTP. Viene dunque consigliato di preferire i siti certificati con HTTPS quando si naviga online.