

Corso di laurea
in informatica e comunicazione digitali

Caso di studio

Cyber Security

Red Team

Man in The Middle

Rico Palmisano

1.Introduzione

L'obiettivo di questo caso di studio è quello di mostrare un attacco MiTM, Man in The Middle, da parte del red team. Un attacco Man in The Middle è una tecnica in cui un attaccante si inserisce nella comunicazione tra due parti con l'obiettivo di intercettare, alterare o rubare informazioni. Questo tipo di attacco può essere utilizzato per rubare informazioni sensibili come credenziali di accesso e dati finanziari.

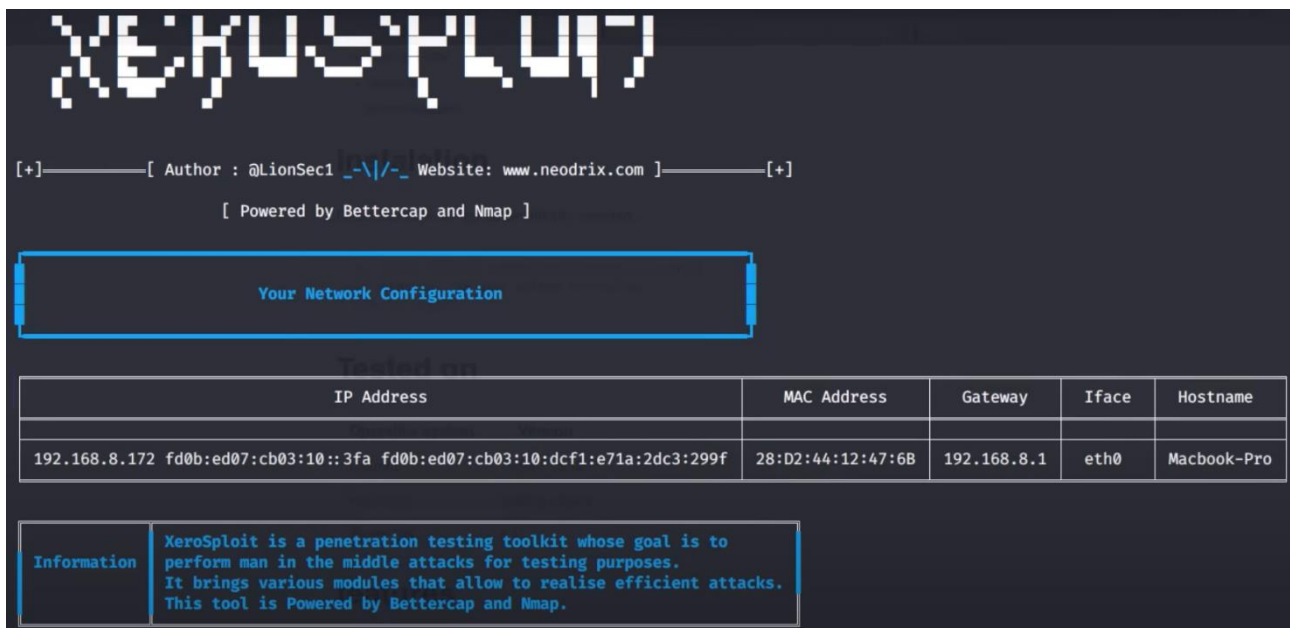
Gli attacchi Man in The Middle prevedono 3 fasi:

- Manipolazione: l'attaccante posiziona se stesso tra le due parti comunicanti, ingannando la rete locale fingendosi uno dei due comunicanti
- Intercettazione di dati: una volta stabilita la posizione, l'attaccante può intercettare tutto il traffico di rete locale tra le due parti, acquisendo dati sensibili trasmesse in chiaro
- Manipolazione: in alcuni casi l'attaccante può alterare i messaggi in transito.

Questo documento descrive come eseguire un attacco MiTM utilizzando xerosploit facendo riferimento alle fasi della Cyber Kill Chain.

2. Panoramica su Xerosploit

Xerosploit è un toolkit di penetration test, utilizzato principalmente per eseguire attacchi MiTM su una rete locale. Esso include anche altri moduli che permettono di effettuare scansioni, spoofing, e intercettazione del traffico.



```
XEROSPLOIT

[+]-----[ Author : @LionSec1 _-\\/_- Website: www.neodrix.com ]-----[+]

[ Powered by Bettercap and Nmap ]

Your Network Configuration

Tested on

IP Address                               MAC Address    Gateway        Iface          Hostname
-----
192.168.8.172 fd0b:ed07:cb03:10::3fa fd0b:ed07:cb03:10:dcf1:e71a:2dc3:299f 28:D2:44:12:47:6B 192.168.8.1    eth0           Macbook-Pro

Information
XeroSploit is a penetration testing toolkit whose goal is to
perform man in the middle attacks for testing purposes.
It brings various modules that allow to realise efficient attacks.
This tool is Powered by Bettercap and Nmap.
```

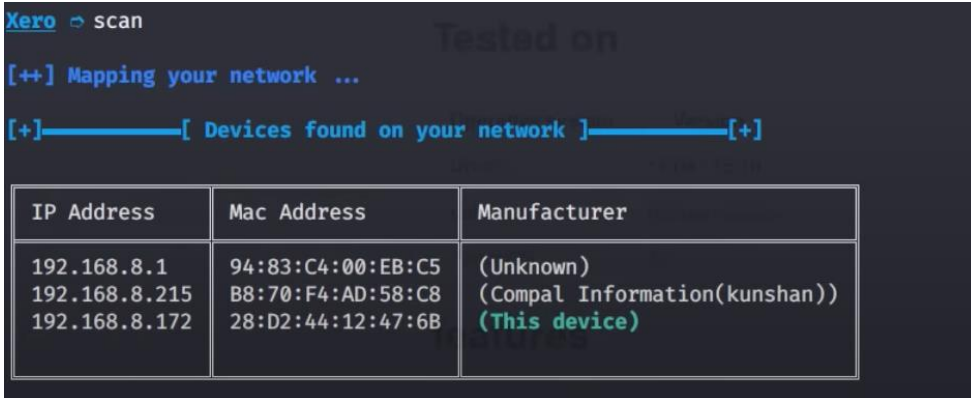
3. Cyber Kill Chain e MiTM

Recoinnnaissance

La fase di ricognizione è il primo step della Cyber Kill Chain, un modello sviluppato per descrivere le fasi di un attacco informatico. Durante questa fase, l'attaccante raccoglie informazioni sulla vittima per pianificare e facilitare ulteriori azioni, tra cui indirizzo ip, e-mail, informazioni personali.

Per questa tipologia di attacco è necessario sapere l'indirizzo ip locale del bersaglio.

Il tool Xerosploit ci consente di effettuare una scannerizzazione della rete mediante il comando 'scan' per verificare i dispositivi connessi con i loro rispettivi indirizzi ip, insieme ai loro indirizzi MAC e altri dettagli rilevanti.



IP Address	Mac Address	Manufacturer
192.168.8.1	94:83:C4:00:EB:C5	(Unknown)
192.168.8.215	B8:70:F4:AD:58:C8	(Compal Information(kunshan))
192.168.8.172	28:D2:44:12:47:6B	(This device)

I risultati della scansione forniranno una panoramica di tutti i dispositivi connessi alla rete.

Weaponization

La fase di weaponization riguarda la creazione o la modifica di un malware e strumenti dannosi che verranno utilizzati per compromettere i sistemi con l'obiettivo di preparare un attacco che possa essere efficacemente lanciato durante le fasi successive della kill chain.

In questo caso Xerosploit rappresenta l'arma usata in questo contesto al fine di effettuare l'attacco MiTM.

Delivery

La fase di consegna riguarda il metodo utilizzato dall'attaccante per trasferire il malware alla vittima. Nel contesto di un attacco MiTM la consegna implica stabilire una posizione di intermediario tra la vittima ed il resto della rete per manipolare ed intercettare il traffico.

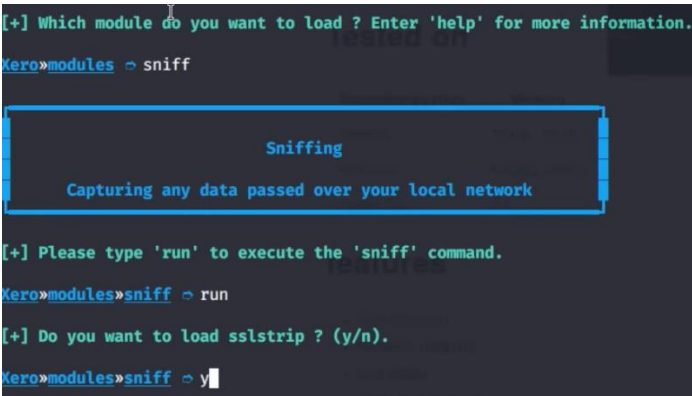
In questo caso l'attaccante seleziona il dispositivo della vittima ed avvia l'attacco.

```
[+] Please choose a target (e.g. 192.168.1.10). Enter 'help' for more information.  
Xero ➔ 192.168.8.215
```

Exploitation

La fase di Exploitation si verifica quando l'attaccante sfrutta una vulnerabilità nel sistema della vittima per ottenere accesso o eseguire codice malevolo. Nel caso di un attacco MiTM l'attaccante sfrutta la posizione di intermediario per intercettare e analizzare il traffico di rete della vittima cercando informazioni sensibili.

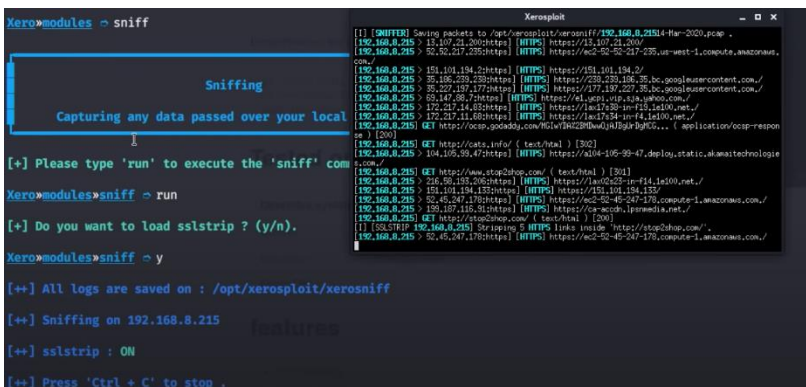
In questa fase, dopo aver stabilito la posizione da intermediario mediante la fase di delivery, viene eseguito lo sniffing. È anche possibile abilitare la funzione sslstrip che permette di intercettare e decrittografare il traffico HTTPS, trasformandolo in http non cifrato. Questo consente di leggere e manipolare dati protetti da SSL/TSL.



Command and Control

L'attaccante stabilisce un canale di comando e controllo per comunicare con il malware sulla macchina.

Dopo aver avviato il malware, è possibile controllare tutti i movimenti che la nostra vittima sta effettuando. Tramite Xerosploit, l'attaccante consente di ricevere dati estratti e monitorare il traffico dati della vittima.



Action on Objectives

La fase di Action on Objectives è la fase finale dove l'attaccante realizza i propri scopi finali, riuscendo ad accedere ai dati sensibili.

Xerosploit consente di poter salvare i dati in un file .log, all'interno del file è anche possibile salvare eventuali credenziali nel caso in cui la vittima ha cercato di accedere ad un sito mentre il nostro malware era in funzione.

4 Prevenzione

Prevenire un attacco MiTM è una componente fondamentale di qualsiasi strategia di cyber security. Ecco alcuni meccanismi di prevenzione contro attacchi MiTM:

- **Utilizzo di connessioni crittografate:** assicurarsi che tutte le comunicazioni web utilizzino HTTPS invece di HTTP. HTTPS utilizza TLS (Transport Layer Security) per crittografare i dati trasmessi tra client e server, rendendo difficile per un attaccante intercettare e leggere i dati.
- **Uso di reti private virtuali (VPN):** Le VPN proteggono i dati trasmessi su reti non sicure, come le reti Wi-Fi pubbliche, rendendo difficile per gli attaccanti intercettare o manipolare il traffico.
- **Multi-Factor Authentication(MFA) :** Implementare l'autenticazione a più fattori per aggiungere un ulteriore livello di sicurezza. Oltre alla password, l'MFA richiede un secondo fattore come un codice inviato al telefono o una chiave hardware.
- **Monitoraggio:** analizzare regolarmente i log di rete per identificare anomalie che potrebbero indicare un attacco in corso
- **Educazione e consapevolezza negli utenti**