Cyber Security Analyst

PROJECT REPORT

W4D4 PRATICA

Prepared by

Fulvio Zalateu

In risposta all'esercizio di simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (Kali). Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS. Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

Security Rookies

Impostazione dell'IP statico e configurazione del Client Windows 7

Per prima cosa andiamo ad impostare l'ip statico su windows 7 seguendo questi passaggi: Pannello di controllo -> Centro connessioni di rete e condivisione -> Modifica impostazioni scheda -> Proprietà della connessione -> Protocollo Internet versione 4 (TCP/IPv4) -> Proprietà -> Utilizza il seguente indirizzo IP:

- **Indirizzo IP: 192.168.32.101**
- **Subnet mask: 255.255.255.0**
- **Gateway predefinito: 192.168.32.1**
- **Server DNS preferito: 192.168.32.100**

Impostazione di Kali Linux come Server

Secondariamente andiamo a modificare la CONFIGURAZIONE DI RETE su Kali Linux con i comandi da terminale: **sudo nano /etc/network/interfaces**
e aggiungendo le seguenti righe:
auto eth0
iface eth0 inet static
address 192.168.32.100
netmask 255.255.255.0
gateway 192.168.32.1
Riavviamo la rete per assicurare il salvataggio delle impostazioni con: **sudo systemctl restart networking**

Configurazione di Inetsim (Internet Service Simulation Suite)

Inetsim è un software che permette di simulare i servizi di rete in un ambiente controllato.
Dopo aver scaricato QUESTO software su Kali Linux, procediamo alla sua configurazione attraverso i comandi a terminale: **sudo nano /etc/inetsim/inetsim.conf**

Configurazione del DNS su Inetsim

Modifichiamo il file di configurazione DNS in INetSim per rispondere con l'indirizzo IP di Kali per epicode.internal con il comando: **sudo nano /etc/inetsim/dns/config**

Aggiungiamo la seguente riga: **A epicode.internal 192.168.32.100**
e in seguito avviamo inetsim con il seguente comando: **sudo inetsim**

Wireshark: che tipo di software è e installazione

Wireshark è uno strumento di analisi del traffico di rete utilizzato per CATTURARE E VISUALIZZARE I DATI CHE TRANSITANO ATTRAVERSO UNA RETE in tempo reale. Su Kali Linux, Wireshark è particolarmente utile per diverse attività legate alla cyber security e alla gestione della rete.
Procediamo all'installazione di Wireshark con i comandi: **sudo apt-get update**
sudo apt-get install wireshark

Intercettazione del Traffico con Wireshark

Avviamo Wireshark su Kali per lanciare la cattura del traffico.

Esecuzione della Richiesta HTTPS dal Client Windows 7:

Apriamo un web browser su Windows 7 e naviga verso https://epicode.internal.

Analisi Traffico HTTPS en HTTP con Wireshark:

Interrompiamo la cattura del traffico su Wireshark e analizziamo i pacchetti HTTPS. Successivamente identifichiamo i MAC address di sorgente e destinazione e il contenuto della richiesta. Infine ripetiamo l'esercizio per intercettare e analizzare il traffico HTTP.

Confronto tra HTTP e HTTPS

- HTTPS: Il traffico è cifrato. In Wireshark, vedremo pacchetti TLS con dati cifrati.
- HTTP: Il traffico è in chiaro. In Wireshark, possiamo vedere tutto il contenuto della richiesta e della risposta HTTP.

Conclusione

Utilizzando INetSim, abbiamo configurato un ambiente di laboratorio sicuro per simulare e analizzare le richieste HTTP e HTTPS. Questo ci ha permesso di vedere le differenze tra i due protocolli e comprendere l'importanza della cifratura nella trasmissione dei dati sensibili.

Simulazione di un caso reale sulla base di questo esercizio.

Scenario: Una azienda, "XYZ Corp", utilizza un'applicazione web interna per la gestione dei dati sensibili dei clienti. Questa applicazione è accessibile tramite HTTPS, ma per ragioni di test e sviluppo, è stata lasciata anche una versione HTTP non sicura. L'azienda ha inoltre una politica di BYOD (Bring Your Own Device) che consente ai dipendenti di accedere all'applicazione tramite dispositivi personali collegati alla rete aziendale tramite Wi-Fi. Minaccia: Un attaccante esterno ha sfruttato la versione HTTP non sicura dell'applicazione per intercettare le credenziali di login dei dipendenti utilizzando un attacco "Man-in-the-Middle" (MitM). L'attaccante si è inserito nella rete Wi-Fi dell'azienda e ha monitorato il traffico non cifrato, riuscendo a catturare nomi utente e password.

Con queste credenziali, l'attaccante ha ottenuto accesso non autorizzato ai dati sensibili dei clienti.

Soluzione al problema

1) Rimozione dell'accesso HTTP:

- Disabilitare immediatamente l'accesso HTTP all'applicazione, garantendo che tutte le comunicazioni avvengano esclusivamente tramite HTTPS.

COMUNICAZIONE AL CLIENTE:

"Attueremo un miglioramento della Sicurezza della Comunicazione garantendo che tutte le comunicazioni tra gli utenti e l'applicazione siano completamente sicure e impedendo agli attaccanti di intercettare le informazioni".

2) Audit completo del sistema:

- Condurre un'analisi approfondita per identificare e correggere eventuali altre vulnerabilità.

COMUNICAZIONE AL CLIENTE: Verifica e correzione delle Vulnerabilità:

"Effettueremo un'analisi dettagliata del sistema per identificare e correggere qualsiasi altra possibile falla nella sicurezza".

3) Reset delle Password e 2FA:

- Forzare il reset delle password per tutti gli utenti e implementare l'autenticazione a due fattori per aumentare la sicurezza degli account.

COMUNICAZIONE AL CLIENTE: Aggiornamento delle Misure di Protezione degli Account:

"Rafforzeremo la sicurezza degli account degli utenti, rendendo più difficile per gli attaccanti accedere ai dati sensibili".

4) Monitoraggio del Traffico di Rete:

- Implementare strumenti di monitoraggio del traffico di rete per rilevare attività sospette e configurare allarmi per attività insolite.

COMUNICAZIONE AL CLIENTE: Monitoraggio della Rete:

"Implementeremo strumenti avanzati di monitoraggio per rilevare e reagire tempestivamente ad attività sospette".

5) Formazione e Consapevolezza:

- Organizzare sessioni di formazione per i dipendenti sulla sicurezza informatica e le migliori pratiche per l'uso delle reti Wi-Fi e la gestione delle password.

COMUNICAZIONE AL CLIENTE: Formazione del Personale:

"Formaremo il personale per assicurarci che tutti comprendano l'importanza della sicurezza delle informazioni e sappiano come comportarsi per prevenire futuri incidenti".

6) Implementazione di una DMZ:

- Configurare una DMZ per separare i server accessibili al pubblico dalla rete interna, proteggendo ulteriormente i dati sensibili.

COMUNICAZIONE AL CLIENTE: Separazione delle Reti:

"Riorganizzeremo la rete aziendale in modo da proteggere meglio i dati sensibili, separando le parti più vulnerabili da quelle più critiche".

In questo modo risolveremo il problema specifico dell'azienda e saremo in grado di comunicarlo in maniera efficace senza entrare nel dettaglio delle azioni pratiche che andremo a fare per annullarlo.

GRAZIE