Istruzioni per gli Studenti: Git e Cybersecurity

Lezione pratica di 4 ore

Benvenuti!

In questa lezione esploreremo Git, il framework MITRE ATT&CK, e alcune tecniche di cybersecurity, con particolare attenzione all'analisi del traffico di rete. Questa guida contiene tutte le istruzioni necessarie per completare le attività pratiche della lezione.

Requisiti

Prima di iniziare, assicurati di avere:

- Python 3.8 o superiore installato
- Git installato
- Privilegi di amministratore (per alcune attività)
- Connessione alla rete della classe

Installazione delle Dipendenze

bash

```
# Creazione ambiente virtuale (opzionale ma consigliato)
python -m venv cybersec_env
source cybersec_env/bin/activate  # Linux/Mac
# O
cybersec_env\Scripts\activate  # Windows

# Installazione dipendenze
pip install mitreattack-python scapy flask cryptography requests
```

Parte 1: Introduzione a Git

Esercizio 1.1: Configurazione di Git

bash

```bash
# Configurazione nome e email
git config --global user.name "Il Tuo Nome"
git config --global user.email "tua.email@example.com"

# Verifica configurazione
git config --list
```

Esercizio 1.2: Creazione del primo repository

bash

```bash
# Crea una nuova cartella per il progetto
mkdir progetto_git
cd progetto_git

# Inizializza un repository Git
git init

# Crea un file Python semplice
echo "print('Hello, Git World!')" > hello.py

# Verifica lo stato
git status

# Aggiungi il file all'area di staging
git add hello.py

# Fai il commit
git commit -m "Aggiunto script hello.py"
```

Esercizio 1.3: Tracciamento delle modifiche

```bash
# Modifica il file
echo "print('Questa è una modifica')" >> hello.py

# Vedi le differenze
git diff hello.py

# Aggiungi e committa le modifiche
git add hello.py
git commit -m "Aggiunta una seconda riga allo script"

# Visualizza la cronologia dei commit
git log
```

Parte 2: MITRE ATT&CK e Introduzione alla Cybersecurity

Esercizio 2.1: Esplorare il framework MITRE ATT&CK

Avvia lo script per esplorare il framework MITRE ATT&CK:

```bash
python mitre_attack_client.py
```

Attività da completare:

1. Visualizza tutte le tattiche (opzione 1)
2. Esplora le tecniche della tattica "Execution" (opzione 2)
3. Visualizza i dettagli della tecnica T1059 (Command and Scripting Interpreter)
4. Visualizza i dettagli della tecnica T1046 (Network Service Scanning)
5. Cerca tecniche legate a "network" (opzione 4)

Esercizio 2.2: Command Injection

Il docente ha avviato un server web vulnerabile. Prova ad attaccarlo!

1. Apri il browser e vai a `http://IP_DEL_DOCENTE:5000/ping`
2. Inserisci un input normale come "localhost" o "8.8.8.8"
3. Prova ad inserire `localhost; ls -la` (Linux) o `localhost && dir` (Windows)
4. Osserva il risultato e annota ciò che è successo

5. Visita `http://IP_DEL_DOCENTE:5000/ping_sicuro` e prova gli stessi input
6. Nota la differenza nel comportamento

Esercizio 2.3: Port Scanning

Esegui uno scanner di porte per individuare i servizi in esecuzione sul server del docente:

```bash
python port_scanner.py IP_DEL_DOCENTE
# Scegli l'opzione 1 (Porte comuni)
```

Domande da rispondere:

1. Quali porte sono aperte sul server?
2. Quali servizi sono in esecuzione?
3. In che modo queste informazioni potrebbero essere utilizzate da un attaccante?

Parte 3: Analisi del Traffico di Rete

Esercizio 3.1: Generare Traffico di Test

Prima di iniziare l'analisi del traffico, generiamo alcuni pacchetti di test:

```bash
# Richiede privilegi di amministratore/root
sudo python traffic_generator.py -t IP_DEL_DOCENTE --all
```

Questo script genererà diversi tipi di traffico:

- Richieste HTTP
- Ping (ICMP)
- Query DNS
- Tentativi di connessione TCP
- Pacchetti UDP

Esercizio 3.2: Cattura e Analisi con Packet Sniffer

Esegui il packet sniffer per analizzare il traffico di rete:

```bash
# Richiede privilegi di amministratore/root
sudo python packet_sniffer.py
```

Osservazioni da fare:

1. Quali tipi di pacchetti riesci a vedere?
2. Puoi identificare i pacchetti HTTP, DNS, TCP, UDP?
3. Come si differenziano i diversi protocolli?

Esercizio 3.3: Analisi con Wireshark

Se Wireshark è installato sul tuo computer, avvialo e:

1. Seleziona l'interfaccia di rete
2. Inizia la cattura
3. Genera altro traffico con lo script traffic_generator.py
4. Applica diversi filtri:
   - `tcp port 80` (HTTP)
   - `icmp` (Ping)
   - `dns` (DNS)
   - `udp` (UDP)

Esercizio 3.4: Comunicazione Non Sicura vs Sicura

Il docente avvierà un server di comunicazione in due modalità: sicura e non sicura.

Connessione al server non sicuro:

```bash
python secure_comms.py client --host IP_DEL_DOCENTE --no-encryption
```

1. Invia alcuni messaggi (es. "Ciao", "Questo è un test", ecc.)
2. Se hai Wireshark aperto, osserva i messaggi nel traffico catturato
3. I messaggi sono leggibili nel traffico catturato?

Connessione al server sicuro:

bash

```
python secure_comms.py client --host IP_DEL_DOCENTE
```

1. Invia gli stessi messaggi di prima
2. Osserva il traffico in Wireshark
3. Puoi leggere i messaggi nel traffico catturato?
4. Nota la differenza tra la comunicazione sicura e quella non sicura

---

Riepilogo delle Attività

Git

- Configurazione iniziale
- Creazione di un repository
- Aggiunta e committaggio di file
- Tracciamento delle modifiche

MITRE ATT&CK

- Esplorazione del framework
- Comprensione di tattiche e tecniche

Cybersecurity

- Sfruttamento di una vulnerabilità Command Injection
- Esecuzione di un port scan
- Analisi del traffico di rete
- Comunicazione sicura vs non sicura

Note Importanti

1. **Uso Etico**: Le tecniche apprese oggi devono essere utilizzate solo in ambienti controllati e con le dovute autorizzazioni. L'uso improprio di queste tecniche può essere illegale e comportare conseguenze gravi.
2. **Privilegi Amministrativi**: Alcune attività richiedono privilegi di amministratore/root. Su Linux/Mac, usa il comando `sudo`. Su Windows, esegui il terminale come amministratore.
3. **IP del Docente**: Sostituisci `IP_DEL_DOCENTE` con l'indirizzo IP effettivo che il docente ti comunicherà.

4. **Problemi Comuni**:
    - Se hai problemi di connessione, verifica di essere sulla stessa rete del docente
    - Se ricevi un errore di permessi, assicurati di eseguire il comando con privilegi di amministratore quando necessario
    - Se una libreria manca, installala con `pip install nome_libreria`

Risorse Aggiuntive

Git

- Git Documentation
- Git Cheat Sheet

MITRE ATT&CK

- MITRE ATT&CK Website
- ATT&CK Navigator

Cybersecurity

- OWASP Top 10
- Wireshark User's Guide
- Scapy Documentation

Buon Divertimento!

Questa lezione offre un'introduzione pratica a strumenti e tecniche importanti nel campo della cybersecurity. Sentiti libero di fare domande al docente in caso di difficoltà o curiosità!