Digitalna forenzika, semestralni projekat
Istraga i zaštita nakon sajber napada na korporativnu mrežu

Fokus predmeta je bio na razumevanju sigurnosnih pretnji, zaštiti sistema i pronalaženju dokaza nakon incidenta. Završni projekat ima za cilj da integriše stečena znanja u realističan scenario, omogućavajući studentima da pokažu svoje veštine u simuliranom okruženju.

Scenario
Vi ste tim etičkih hakera i forenzičkih analitičara angažovani od kompanije koja je nedavno doživela sajber napad. Kompanija je primetila sumnjive aktivnosti u svojoj mreži: podaci su procureli, nekoliko servera je kompromitovano, a zaposleni su primili *phishing* mejlove. Vaš zadatak je da istražite incident, identifikujete ulaznu tačku napada, analizirate prikupljene dokaze, predložite rešenja za sanaciju i zaštitu sistema, te podnesete detaljan izveštaj.

Predloženi resursi, softveri i alati

- **Kali Linux virtuelna mašina** sa unapred instaliranim alatima (Nmap, Metasploit, Wireshark, Burp Suite, itd.).
- **Autopsy softver** za forenzičku analizu.
- **Snimak diska kompromitovanog servera** (u formatu koji Autopsy može da obradi, npr. .E01 fajl ili DD).
- **Mrežni promet** (u .pcap formatu, snimljen tokom napada).
- **Log fajlovi** sa web servera i firewall-a.
- **Primer phishing mejla** koji su zaposleni dobili. (pomoću alata generisati mejlove)

Postupak se vodi u četiri faze i to

1. **Faza 1: Prikupljanje i analiza dokaza (forenzička analiza)**

Pomoću Autopsy, analizirajte snimak diska kompromitovanog servera. Pronađite tragove malvera, izmenjene fajlove ili bilo kakve sumnjive aktivnosti (npr. kreiranje novih korisničkih naloga, instalacija backdoor-a). Analizirati log fajlove i pronađite anomalije (npr. sumnjive IP adrese, neobične konekcije). Koristeći Wireshark, analizirajte mrežni promet i identifikujte potencijalne komunikacije sa C&C (Command and Control) serverima.

2. **Faza 2: Identifikacija ulazne tačke napada (penetration testing)**

Analizirajte phishing mejl i utvrdite da li sadrži zlonamerne linkove ili priloge. Ako postoji link, simulirajte njegovu proveru (bez stvarnog pristupa). Koristeći alate poput Nmap i Metasploit, potrebno je identifikovati ranjivosti u mreži koje su mogle biti iskorišćene (npr. zastareli softver, slabe lozinke, nezaštićeni portovi). Pronaći najverovatniju ulaznu tačku napada (npr. phishing, eksploatacija ranjivosti u web aplikaciji, itd.).

3. **Faza 3 - sanacija i zaštita**

Potrebno je predložiti korake za sanaciju sistema: uklanjanje malvera, zatvaranje ranjivih portova, ažuriranje softvera i sve ono što smatrate relevantnim. Takođe, trebalo bi navesti mere za sprečavanje budućih napada: obuka zaposlenih, implementacija WAF-a (Web Application Firewall), podešavanje IDS/IPS sistema i drugo. Napisati kratku skriptu (u Pythonu, Bash-u ili bilo kojom tehnologijom prema sopstvenom izboru) koja automatizuje deo procesa sanacije (npr. proveru portova, čišćenje sumnjivih fajlova).

4. **Faza 4 - Izveštaj**

Sastavitii detaljan izveštaj koji uključuje:

a) Hronologiju napada (kako je napad izveden i šta je kompromitovano).
b) Pronađene dokaze (sa snimcima ekrana iz Autopsy-a, Wireshark-a, itd.).
c) Predložene mere za sanaciju i zaštitu.
d) Kod skripte i objašnjenje njene funkcionalnosti.

Sistem bodovanja (ukupno 30 poena)

- **Forenzička analiza (8 poena)**
  - Pronalazak i dokumentovanje dokaza sa diska: 4 poena
  - Analiza mrežnog prometa i log fajlova: 4 poena
- **Identifikacija ulazne tačke napada (7 poena)**
  - Analiza phishing mejla: 3 poena
  - Identifikacija ranjivosti i ulazne tačke: 4 poena
- **Sanacija i zaštita (8 poena)**
  - Predloženi koraci za sanaciju: 3 poena
  - Predlozi za sprečavanje budućih napada: 3 poena
  - Funkcionalnost skripte za automatizaciju: 2 poena
- **Izveštaj (7 poena)**
  - Jasnoća i strukturiranost izveštaja: 3 poena
  - Dokumentovanje dokaza (snimci ekrana, opisi): 2 poena
  - Kvalitet predloženih rešenja: 2 poena

Dodatne napomene za zaposlene studente

- Zaposleni studenti bi trebalo da prikažu dodatne tehnike prema sopstvenom izboru prilikom pristupa rešenja (npr. korišćenje dodatnih alata, dublja analiza) kako bi ostvarili poene za aktivnost.