ASPIRA®
VELEUČILIŠTE

Laboratorijska Vježba 2 - Sigurnost Informacijskih Sustava

U ovoj vježbi ćemo početi rad s Linux operativnim sustavom, pripremiti laboratorijsko okruženje i napraviti određene vježbe iz područja analize prometa. Pripremljeno laboratorijsko okruženje će vam služiti i u narednim vježbama.

Postavljanje Virtualnog Laboratorijskog Okruženja

1. **Koristite virtualizacijsku platformu**: Preporučuje se korištenje Oracle VirtualBox-a jer je besplatan i jednostavan za korištenje.
2. **Podignite dva virtualna stroja:** Postavite Kali Linux, drugu Linux distribuciju (npr. Ubuntu) i host stroj.
3. **Konfigurirajte internu mrežu:** Postavite internu mrežu unutar VirtualBox-a kako bi sva tri stroja mogla komunicirati.
4. **Podesite IP adrese:** Ručno postavite IP adrese ili konfigurirajte DHCP na mreži. Provjerite komunikaciju između strojeva s naredbom ping.
5. **Priložite screenshotove:** Snimite slike postavki VirtualBox-a i rezultate ping testova.

Analiza Prometa pomoću nmap i Wireshark

1. **Koristite nmap:** Izvršite naredbu nmap na jednom od Linux strojeva kako biste skenirali otvorene portove na drugom stroju.
2. **Koristite Wireshark:** Pokrenite Wireshark na Kali Linux stroju kako biste pratili promet. Filtrirajte promet koristeći filter nmap kako biste pronašli pakete povezane s nmap skeniranjem.
3. **Priložite screenshotove:** Snimite slike rezultata nmap skeniranja i uhvaćenih paketa s Wiresharkom.

Prisluškivanje lokalnog prometa

1. **Instalirajte nmap za Windows:** Preuzmite i instalirajte nmap na lokalnom računalu s Windows operativnim sustavom.
2. **Konfigurirajte dvije računalne stanice:** Postavite dva računala na istoj mreži kako bi mogla komunicirati.
3. **Koristite netcat/nc/ncat:** Koristite naredbe netcat za slanje poruke s jednog računala na drugo.
4. **Pratite promet s Wiresharkom:** Pokrenite Wireshark na Kali Linux stroju kako biste pratili promet. Pomoću filtra pronađite pakete koji sadrže poslanu poruku.
5. **Priložite screenshotove:** Snimite slike instalacije nmap-a, netcat naredbi i rezultata Wireshark analize.

Macchanger aplikacija u Kali Linuxu

1. **Objasnite macchanger:**
2. **Demonstrirajte korištenje:** Pokažite korake korištenja macchanger na Kali Linux stroju. To uključuje prikazivanje trenutne MAC adrese i promjenu iste.
3. **Priložite rezultate:** Snimite slike prije i poslije primjene macchangera, kako biste pokazali promjenu MAC adrese.

Snimanje i Analiza HTTP Prometa

1. **Postavljanje HTTP servera:** Postavite jednostavan HTTP server na drugoj Linux distribuciji. Koristite alat poput python -m SimpleHTTPServer (Python 2) ili python -m http.server (Python 3).
2. **Izvršite HTTP zahtjev iz Kali Linuxa:** Koristite alat poput curl ili wget na Kali Linux stroju kako biste izvršili HTTP zahtjev prema IP adresi i portu drugog Linux stroja.
3. **Pratite HTTP promet s Wiresharkom:** Ponovno pokrenite Wireshark na Kali Linux stroju i pratite promet dok izvršavate HTTP zahtjev. Filtrirajte promet kako biste izdvojili samo HTTP pakete.
4. **Priložite screenshotove:** Snimite slike HTTP zahtjeva i odgovora iz Wiresharka kako biste pokazali zabilježeni promet.
5. **Analizirajte promet:** Otvorite snimljene HTTP pakete u Wiresharku i analizirajte ih. Pokušajte identificirati HTTP metodu, odgovoreni statusni kod, i sadržaj zahtjeva/odgovora.
6. **Napomena:** U README datoteku uključite opise koraka koje ste poduzeli kako biste postavili HTTP server, izvršili zahtjev te prateći i analizirali promet.

Nadam se da će vam ovo pomoći u provedbi laboratorijskih zadataka. Ako imate daljnja pitanja ili nejasnoće, slobodno pitajte!

Završene vježbe se moraju dostaviti na anteprojic@gmail.com