Wireshark kao alat za etičko hakiranje

Lovro Stjepanović, 3.F

Uvod

U današnjem digitalnom svijetu, na prvo mjesto dolazi sigurnost informacija. Sa sve kompleksnijom povezanošću uređaja i mreža, organizacijama i pojedincima je sve teže osigurati to da njihovi podaci ostanu zaštićeni od zlonamjernih napada. Etičko hakiranje predstavlja jedan od načina kako organizacije mogu identificirati i ispraviti slabosti u njihovim sustavima prije nego što postanu meta stvarnih napada. Wireshark, aplikacija za analizu mrežnog prometa, igra ključnu ulogu u ovom procesu.

Što je Wireshark?

Wireshark je popularan alat otvorenog koda koji omogućuje analizu mrežnog prometa u stvarnom vremenu. Dostupan je za različite platforme kao što su Windows, Linux i MacOS. Wireshark omogućuje korisnicima da prate mrežni promet koji prolazi kroz njihovu mrežnu karticu, pružajući dubok uvid u komunikaciju između različitih uređaja na mreži.

Što je etičko hakiranje?

Etičko hakiranje uključuje ovlašteni pokušaj dobivanja neovlaštenog pristupa računalnom sustavu, aplikaciji ili podatcima. Provođenje etičkog hakiranja uključuje dupliciranje strategija i radnji zlonamjernih napadača. Ova praksa pomaže identificirati sigurnosne ranjivosti koje zatim mogu riješiti prije nego što napadač ima priliku iskoristiti ih.

Podržava li Wireshark etičko hakiranje?
Wireshark pruža niz mogućnosti koje su od velikog značaja za etičko hakiranje, npr.:

Snimanje prometa - Wireshark omogućuje korisnicima da snime mrežni promet koji prolazi kroz njihovu mrežnu karticu. Ovo je korisno za analizu različitih vrsta prometa, uključujući HTTP, FTP, SSH, DNS, i mnoge druge protokole.

Detekcija ranjivosti - Koristeći Wireshark, etički hakeri mogu identificirati ranjivosti u mrežnim protokolima ili aplikacijama. Na primjer, mogu otkriti nekriptiranu komunikaciju ili slabe autentikacijske mehanizme.

Analiza paketa - Wireshark omogućuje detaljnu analizu svakog paketa u mrežnom prometu. Etički hakeri mogu proučavati sadržaj paketa kako bi identificirali potencijalne prijetnje ili neobične obrasce ponašanja.

Rekonstrukcija sesije - Wireshark može rekonstruirati TCP sesije, omogućavajući etičkim hakerima da prate tok komunikacije između klijenta i servera. Ovo je korisno za analizu interakcije između različitih dijelova sustava.

Identifikacija napada - Korištenjem Wiresharka, etički hakeri mogu identificirati i analizirati napade kao što su DDoS napadi, SQL injection ili phishing pokušaji. Analiza mrežnog prometa pomaže u prepoznavanju neobičnih aktivnosti koje bi mogle ukazivati na napad.

Etika korištenja Wiresharka
Iako Wireshark može biti moćan alat za etičko hakiranje, važno je naglasiti potrebu za odgovornim korištenjem. Etički hakeri trebaju djelovati u skladu s etičkim smjernicama i zakonskim propisima kako bi osigurali da se njihove aktivnosti ne koriste za nezakonite ili neetičke svrhe. To uključuje dobivanje dozvola prije testiranja sustava, zaštitu privatnosti podataka te suradnju s vlasnicima sustava kako bi se identificirale i ispravile ranjivosti.

Zaključak
Wireshark predstavlja moćan alat za etičko hakiranje koji omogućuje analizu mrežnog prometa i identifikaciju ranjivosti u sustavima. Korištenje Wiresharka zahtijeva odgovorno ponašanje i poštivanje etičkih smjernica kako bi se osiguralo da se alat koristi u svrhu poboljšanja sigurnosti sustava, a ne za zlonamjerne aktivnosti. Upravljanje rizicima i osiguranje sigurnosti informacija su ključni aspekti koji trebaju biti uzeti u obzir prilikom korištenja Wiresharka u etičkom hakiranju.

Literatura
Općenito o Wiresharku - https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it
Općenito o etičkom hakiranju - https://www.synopsys.com/glossary/what-is-ethical-hacking.html
Dodatno - https://group.miletic.net/hr/nastava/materijali/wireshark-snimanje-prometa/
DDoS napad - https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/