Ana Baćak 3.F

Wireshark kao alat za etičko hakiranje

Ana Baćak 3.F

Kratak sadržaj

Ana Baćak 3.F

Uvod

U današnjem digitalnom dobu, sigurnost informacija postaje sve važnija kako se tehnologija brzo razvija. Tvrtke diljem svijeta suočavaju se s izazovima zaštite svojih sustava i podataka od sve sofisticiranijih prijetnji. Etičko hakiranje, praksa pronalaženja i ispravljanja sigurnosnih propusta radi zaštite sustava, postaje ključno sredstvo u ovom borbenom polju.

Ovaj rad istražuje koncept etičkog hakiranja i ulogu alata poput Wiresharka u tom kontekstu. Etičko hakiranje nije samo otkrivanje propusta, već i preventivno djelovanje kako bi se osigurala cjelovita sigurnost sustava. S druge strane, Wireshark, snažan alat za analizu mrežnih protokola, pruža dublji uvid u mrežni promet, omogućujući hakere da identificiraju ranjivosti i analiziraju neobične aktivnosti.

Ana Baćak 3.F

Etičko hakiranje

Iako se može činiti suglasnim, etičko hakiranje postaje sve važnije u svijetu brze digitalizacije. Tvrtke diljem svijeta sve češće angažiraju etičke hakere kako bi zaštitile svoje klijente i njihove osobne podatke. Etički hakeri imaju zadatak pronalaženja sigurnosnih propusta u sustavima ili mrežama tvrtki korištenjem specijaliziranih alata, tehnika i znanja o ranijim sigurnosnim propustima. Sigurnosni propusti mogu nastati iz raznih razloga poput mana operativnih sustava, loše konfiguriranih servera s bazom podataka ili nedostatka edukacije radnika o sigurnosnim prijetnjama.

Društveni inženjering je čest način napada na računalne sustave tvrtki, pri čemu se koriste tehnike manipulacije ljudima radi dobivanja informacija o tvrtki koje olakšavaju neovlašten pristup sustavima. Etički hakeri koriste specijalizirane alate kako bi otkrili takve propuste i objasnili kako ih ispraviti. Neki primjeri programa nagrađivanja etičkih hakera, poput Microsoftovog programa "bug bounty", pokazuju koliko su tvrtke spremne platiti za pronalazak sigurnosnih propusta u svojim sustavima.

Etičko hakiranje ima različite definicije, ali sukladno moralnim načelima i pravilima zajednice etičkih hakera, uvijek zahtijeva dobivanje dozvole od vlasnika sustava ili mreže prije bilo kakvog testiranja ili penetracije. Etički hakeri imaju odgovornost ne samo identificirati ranjivosti, već i popraviti ih kako bi osigurali sigurnost sustava ili mreže. Njihove dužnosti uključuju pronalaženje i rješavanje otvorenih rupa, provjeru sustava za prevenciju i otkrivanje upada te osiguravanje ažuriranja zakrpa.

Ana Baćak 3.F

Wireshark : Sharkfest

Gerald Combs počeo je stvarati Wireshark alat 1998. To je jedan od najpopularnijih alata za analizu mrežnih protokola. Besplatan je i radi na mnogim operativnim sustavima. Podržava analizu preko 100 mrežnih protokola. Može dekomprimirati komprimirane datoteke i dešifrirati protokole kao što su WPA/WPA2 i IPsec. Može hvatati podatke u stvarnom vremenu i analizirati ih izvan mreže. Može izvoziti podatke u različite formate kao što su XML, CSV i tekstualni format.

Za edukaciju mrežnih administratora i stručnjaka, organiziran je SharkFest. To su godišnje obrazovne konferencije diljem svijeta. Cilj im je razmjena znanja i iskustava o korištenju Wiresharka između razvojnog tima i korisnika. Na SharkFestu, polaznici mogu usavršavati svoje vještine u analizi paketa kroz predavanja i laboratorijske vježbe koje vode stručnjaci iz industrije.

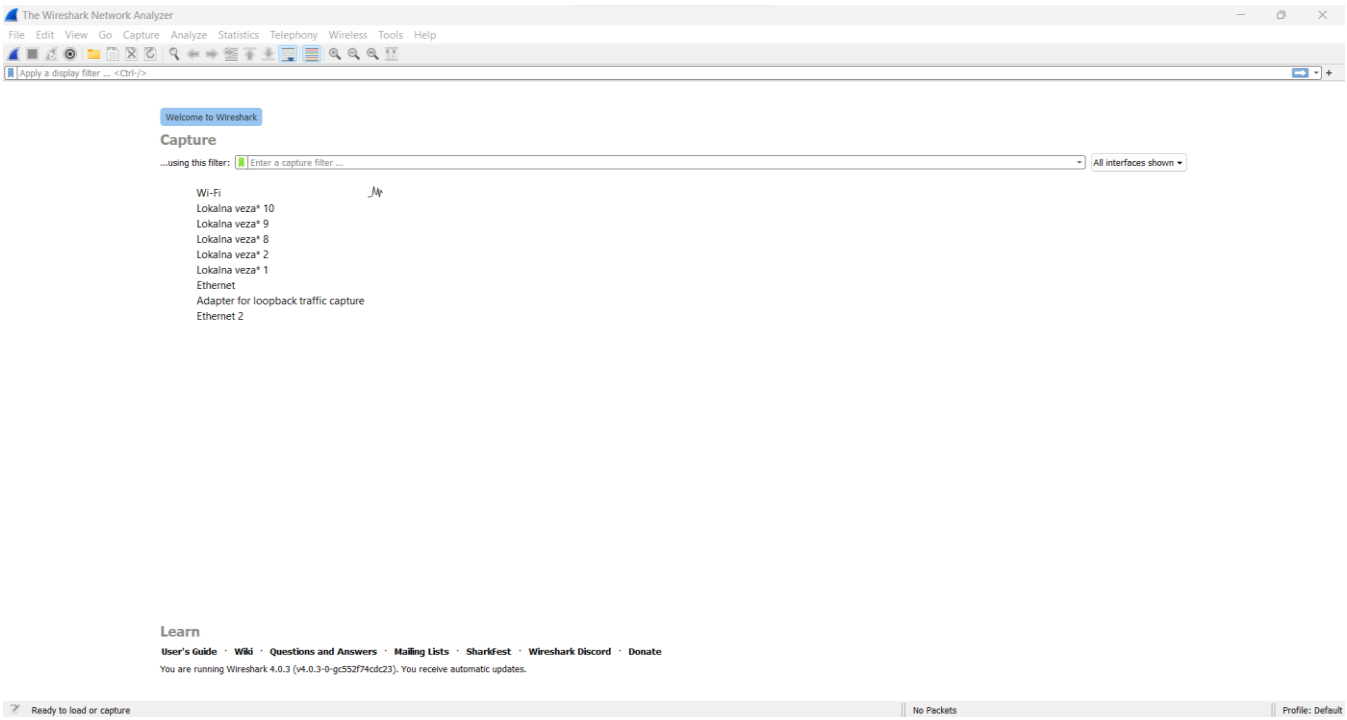
Glavni programeri Wiresharka okupljaju se tijekom SharkFesta kako bi poboljšali alat i osigurali da ostane relevantan. Wireshark se može pokrenuti pomoću naredbe "wireshark" u naredbenom retku. Također se može koristiti bez grafičkog sučelja upisivanjem naredbe "tshark". Sve mogućnosti i značajke ostaju iste, samo je oblik korištenja različit.

Wireshark : Pregled alata

Wireshark je besplatni alat za analizu mrežnih protokola koji je počeo razvijati 1998. godine. Korisnicima omogućuje praćenje i analizu prometa na mreži u stvarnom vremenu. Radi na različitim operativnim sustavima i nudi razne značajke poput otvaranja komprimiranih datoteka, dešifriranja sigurnosnih protokola kao što su WPA/WPA2 i IPsec, te mogućnosti izvoza podataka u različite formate.

Etički hakeri koriste Wireshark u raznim situacijama. To uključuje testiranje sigurnosti mrežnih sustava, otkrivanje ranjivosti, analizu protokola te praćenje i otkrivanje neobičnih aktivnosti u mreži. Mogu simulirati napade i provjeriti koliko su sigurnosne mjere organizacije učinkovite.

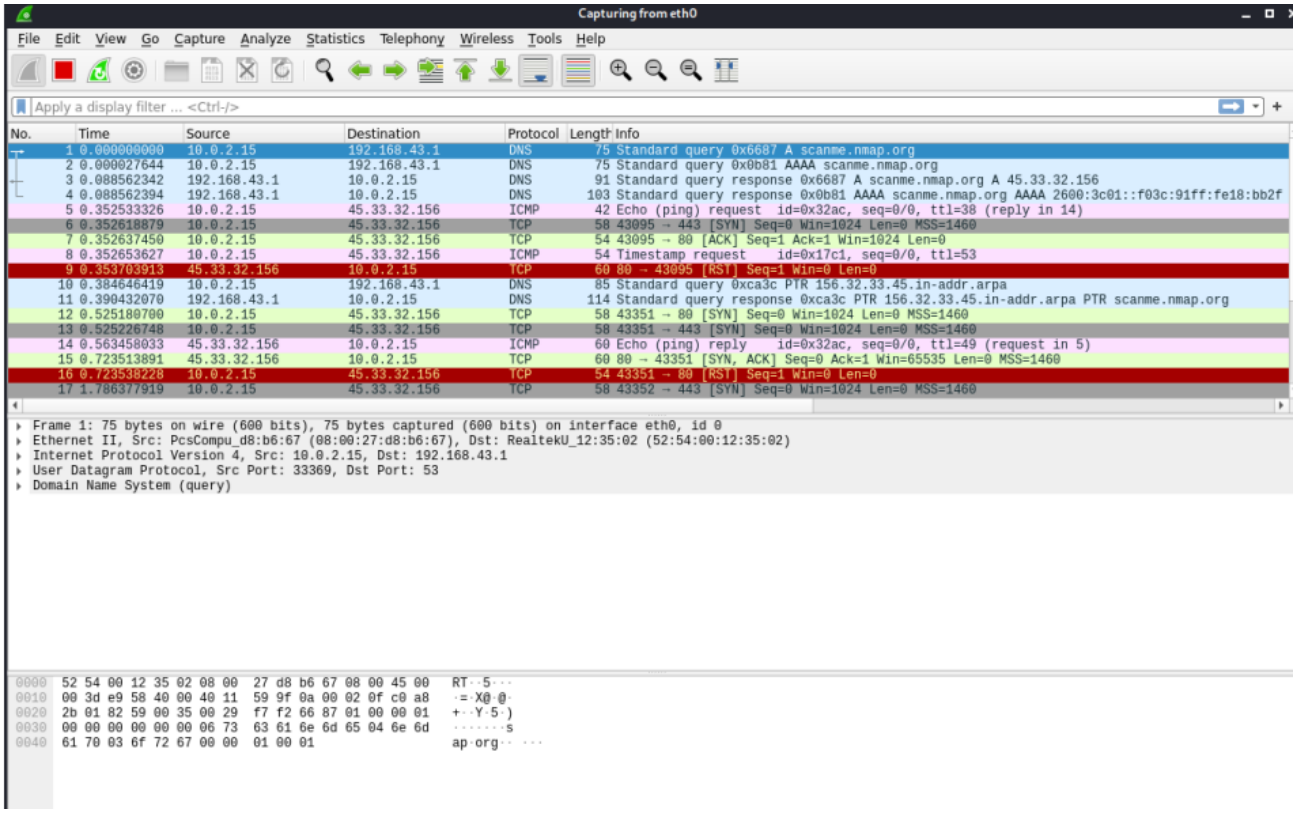
Važno je napomenuti da se Wireshark smije koristiti samo na mrežama gdje je dopušteno pratiti mrežne pakete jer je vrlo moćan alat. Primjeri protokola koji su osjetljivi na alate poput Wiresharka uključuju Telnet, HTTP, SMTP, FTP i drugi. Takvi protokoli šalju informacije u otvorenom obliku, što omogućuje da se lozinke i korisnička imena lako pronađu pregledom mrežnog prometa pomoću Wiresharka. Stoga je važno osigurati sigurnost mreže i šifrirati osjetljive podatke kako bi se spriječilo neovlašteno otkrivanje informacija.



Slika 1. Sučelje Wireshark -a

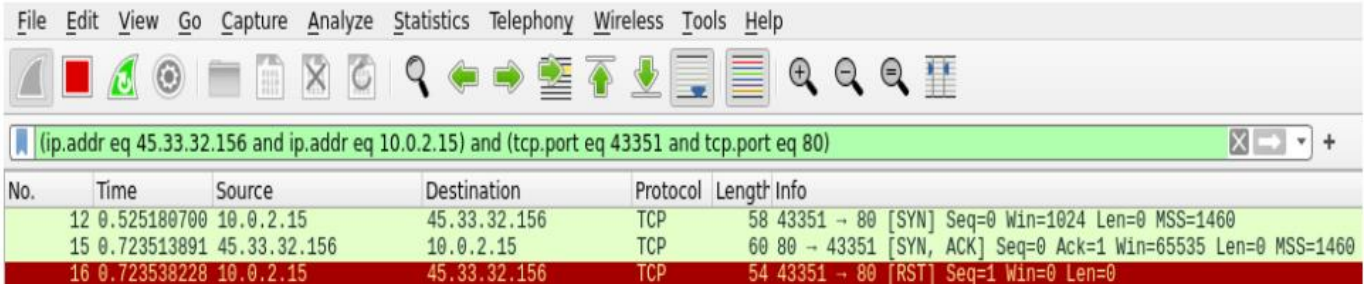
Primjena Wiresharka u praksi

PRIMJER: Na slici 2 prikazan je cijeli promet na mreži nakon što su upisane određene naredbe koje su prikazane na slici 11. Može biti teško razlikovati pakete s kojima želite nastaviti istraživanje, stoga su filteri izuzetno korisni. Filtere možete dodati u gornji dio alata iznad liste paketa. Postoje dvije vrste filtera: filteri za prikaz i filteri za hvatanje. Filteri za hvatanje određuju koje pakete treba uhvatiti, dok se filteri za prikaz koriste za određivanje koje uhvaćene pakete želite vidjeti u alatu. Filteri za hvatanje se postavljaju prije početka hvatanja prometa i ne mogu se mijenjati tijekom procesa, dok se filteri za prikaz mogu mijenjati i prije i tijekom procesa.



Slika 2: Ukupni uhvaćeni promet

U sljedećem primjeru, na slici 3, upisan je filter (ip.addr eq 45.33.32.156 and ip.addr eq 10.0.2.15) and (tcp.port eq 43351 and tcp.port eq 80) kako bi se filtrirale određene IP adrese, u ovom slučaju izvorna adresa je 45.33.32.156, a odredišna adresa je 10.0.2.15. Također, naredba tcp.port označava prikaz paketa s određenim TCP izvornim ili odredišnim portom, u ovom slučaju portovi su 43351 i 80.



Slika 3: Uhvaćeni mrežni promet uz korištenje filtera

U prvom redu vidljivo je da je poslana SYN poruka s izvorne IP adrese 10.0.2.15 na odredišnu adresu 45.33.32.156, s porta 43351 na port 80. Nakon toga poslana je SYN, ACK poruka s izvorne adrese 45.33.32.156 na odredišnu adresu 10.0.2.15, s porta 80 na port 43351. Nakon što je primljena SYN ACK poruka, poslana je RST poruka s IP adrese 10.0.2.15 na adresu 45.33.32.156 kako bi se zatvorila komunikacija. Iz ovog primjera vidljivo je kako funkcionira hvatanje mrežnog prometa pomoću Wiresharka i kako se koristi za analizu TCP SYN skeniranja pomoću Nmap alata.

Zaključak

Wireshark predstavlja snažan alat u arsenalu etičkih hakera za otkrivanje i ispravljanje sigurnosnih propusta u mrežama i sustavima. Kroz njegovu primjenu, organizacije mogu proaktivno djelovati u očuvanju sigurnosti svojih informacija i osigurati pouzdanost svojih mreža. Edukacija i razmjena znanja putem konferencija poput SharkFest-a ključni su za unaprjeđenje vještina i sposobnosti u korištenju ovog moćnog alata. Etičko hakiranje s Wiresharkom kao ključnim alatom postaje nezaobilazna praksa u osiguranju sigurnosti mreža i sustava u današnjem digitalnom okruženju.

Literaura

1. https://zir.nsk.hr/en/islandora/object/etfos%3A3145/datastream/PDF/view
2. https://repozitorij.foi.unizg.hr/islandora/object/foi:6158/datastream/PDF/download
3. https://repozitorij.unizd.hr/islandora/object/unizd%3A7847/datastream/PDF/view
4. https://www.synopsys.com/glossary/what-is-ethical-hacking.html