UDK 343.983:004.738.5]:656.1/.8
10.7251/ZRSNG2001034T

DIGITALNA FORENZIKA MREŽNIH UREĐAJA I SAOBRAĆAJA

DIGITAL FORENSICS OF NETWORK DEVICES AND NETWORK TRAFFIC

Autoi: Mladen Trakilović, Stevo Jokić Univerzitet Sinergija, Aleksandar Sandro Cvetković Univerzitet Sinergija

***Sažetak* — Svakodnevnica savremenog čovjeka bez upotrebe savremene tehnologije je nezamisliva pa samim tim i porast sajber kriminala je neminovan. Različite okolnosti i dostupni resursi forenzičko ispitivanje mogu dovesti do izazova. Ovaj rad je nastao na realnim praktičnim primjerima kroz aktivne i pasivne metode forenzike počev od sakupljanja enkriptovanog saobraćaja u realnom vremenu, njegovu dekripciju i analizu dobijenih podataka. Aktivnom forenzikom kroz različite načine dobili smo dosta konkretnije informacije važne za forenziku. Koristio sam i tehnike koje koriste sajber kriminalci za upade u zaštićene mreže, računare i mrežne uređaje kada je to bilo neizbježno kako bi direktno spriječio napade i štetu ali i sačuvao što više podataka o toku napada na mrežu, računara i mrežne uređaje. Uz odgovarajuću mrežnu opremu koja je pravilno podešena dokazano je da je moguće spriječiti vršenje najtežih sajber napada, kao i presresti i dekriptovati i *ransomware* napade koji prave štetu u milijardama dolara na globalnom nivou. Svi softveri korišteni za ovaj rad počev od operativnog sistema i aplikacija su opensource i dostupni su svima.**

***Ključne riječi* – digitalna forenzika; mrežna forenzika; forenzika mrežnih uređaja; forenzika mrežnog saobraćaja; analiza mrežnog saobraćaja u realnom vremenu**

Abstract – Everyday life of modern man without the use of modern technology is unthinkable, and therefore the rise of cybercrime is inevitable. Different circumstances and available resources forensic examination can lead to challenges. This paper is based on real practical examples through active and passive methods of forensics, starting with the collection of encrypted traffic in real time, its decryption and analysis of the obtained data. Through active forensics, we have obtained much more specific information important for forensics in various ways. I also used the techniques used by cybercriminals to hack into protected networks, computers and network devices when it was inevitable in order to directly prevent attacks and damage, but also to save as much data as possible on the course of attacks on networks, computers and network devices. With the right network equipment set up properly, it has been proven that it is possible to prevent the most severe cyber attacks, as well as intercept and decrypt ransomware attacks that cause billions of dollars in damage globally. All software used for this work starting with the operating system and applications are open source and available to everyone.

***Keywords* – digital forensics; network forensics; network device forensics; network traffic forensics; real-time network traffic analysis**

I. UVOD

Razvojem tehnologije, računarstva kao i interneta uopšte poslednjih decenija u mnogome je olakšan život čovjeka. Poslednjih petnaestak godina skoro svaki uređaj je povezan na neku vrstu mreže ili na internet. Čak i osmobitni mikrokontroleri dobili su mogućnost pristupa internetu na bilo kojoj tački svijeta. Moguće je upravljati uređajima i stvarima za koje je bilo nezamislivo prije par godina. Razvoj IOT *internet of things* uređaja kao što su razne vrste kućnih aparata, mjernih stanica sa sofisticiranim senzorima, pametnim automobilima, pametnim kućama, parking sistemima, ogrlicama i hranilicama za kućne ljubimce, alarmnih sistema i drugih je dao osjećaj komotiteta, jeftinijeg korištenja i ubrzao život svakodnevnice.

Postavlja se pitanje koliko i kako je taj svijet zaštićen i koje su posledice po čovjeka u slučaju da taj sistem nekad jednostavno prestane da radi iz benignih razloga kao što su običan prestanak snabdijevanjem električnom energijom na par sekundi ili minuta do velikih padova sistema i mreža iz zlonamjernih razloga. Obično se s vremena na vrijeme dešavaju razne situacije gdje čovjek iz bilo kog razloga ometa ili onemogućuje rad i umrežavanje tehnologije. Ti napadi mogu da budu veoma opasni u zavisnosti sta je meta napada. Infrastrukturni sistemi jedne zemlje koji su napadnuti mogu da otežaju ili onemoguće rad raznih institucija kao što su zdravstvo, energetika, birokratski aparati, bankarski sektor, saobraćaj, vodosnabdijevanje, transport usluga, dobara i ljudi i drugo.

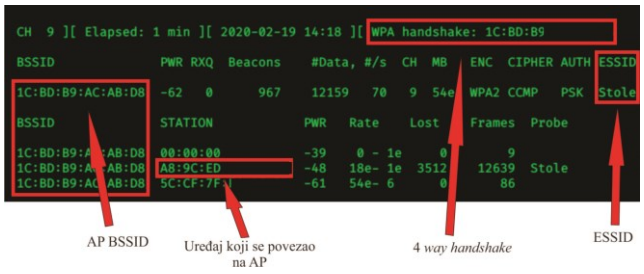
II. METODI

U ovom radu ćemo se posvetiti praktičnim primjerima digitalne mrežne forenzike, mrežnih uređaja i saobraćaja na mrežnoj infrastrukturi koju sam sam podesio tako da djeluje što realističnije. Koristiću različite softvere i alate otvorenog koda (Open source). Demonstriraću mrežnu forenziku jednog demo slučaja koji je sačinjen od mreže više uređaja povezanih preko bežične WiFi (Wireless Fidelity) mreže i fizičkim kablovskim mrežnim instalacijama.

A. Pasivna forenzika WiFi enkriptovanog saobraćaja u realnom vremenu

Ovom metodom forenzike se obrađuje određena WiFi mreža koja je zaštićena WPA ili WPA2 (***W****ireless Fidelity* ***P****rotected* ***A****ccess*) enkripcijom a ne postoji informacija o ključu kako bi se saobraćaj mogao u realnom

vremenu dekriptovati i analizirati. . Sav saobraćaj koju se u tom momentu obrađuje iako je enkriptovan može se snimiti i naknadno obrađivati. Ovu metodu je moguće iskoristiti i za nadzor i rad policijski službi ili drugih bezbijednosnih struktura. Softver koji to omogućava je aircrack-ng[1] koji se nalazi u paket menadžerima na svim većim linux distribucijama kao i za Windows operativne sisteme.
Na slici broj 1 je prikazan rezultat poslije jednog minuta od kako smo počeli da snimamo saobraćaj u datoteku Stole.cap. Vidimo broj povezanih uređaja (station) na taj AP (access point) od kojih se je jedan u trenutku snimanja povezao na AP i omogućio nam snimanje i *4 way handshake* koji može kasnije da se upotrijebi za dekripciju saobraćaja te mreže putem *bruteforce* metode dekripcije. Snimljenu datodeku možemo da importujemo u druge softvere za mrežnu forenziku o kojima ćemo kasnije govoriti u ovom radu.



Ovim smo pokazali da postoje određeni podaci koji mogu biti korisni za istragu bezobzira sto su zaštićeni enkripcijom. Dalje je moguće pomoću različitih antena utvrditi okvirnu lokaciju AP kao i uređaja koji su povezanih na taj AP.

Za tu svrhu možemo koristiti direkcione antene kao što si *Yagi-Uda*[2] antena, *Cantenna*[3], parabolične *grid* reflektorske antene[4] *ili WokF*[5]*i* antene koje se čak mogu i napraviti u kućnim uslovima pogotovo *cantenna.* Za tu svrhu možemo koristiti onlajn kalkulatore[6] za izračunavanje dimenzija i karakteristika antene. Iako mnoge pravljene antene ponekad izgledaju možda čak i komično u praksi su se pokazale kao veoma dobre. Najobičnija *cantenna* je imala pojačavanje signala od 9-11 dB u odnosu na standardnu eksternu omnidirekcionu antenu koja ima perfomanse od samo 3dB a da ne pominjemo da onnidirekciona antena prikuplja WiFi zračenje sa svih 360 stepeni koje mogu da imaju radio interferencu ciljanog AP sa ostalim AP-ovima koji su na istim ili susjednim kanalima naročito u gusto naseljenim mjestima i objektima.

B. Dekriptovanje snimljenog WiFi saobraćaja

Snimljeni saobraćaj koji smo sačuvali radom airodump-ng u datoteku u našm primjeru Stole.cap možemo iskoristiti da iz nje saznamo koja je lozinka u pitanju putem *bruteforce* metode. Za tu svrhu najpogodnije je korisiti alat hashcat koji ima mogućnost akceleracije pokušaja lozinki sa procesorskim, grafičkim ili FPGA (engl. Field-Programmable Gate Array) jedinicama. Veoma uspješan i efikasan način je izveden sa Spartan 6 i Ztex razvojim FPGA pločicama na Tehničkom Univerzitetu u Beču od strane Markus Kamerštetera, Markusa Milnera, Daniela Buriana, Kristiana Kudera i Volfganga Kastnera (Markus Kammerstetter, Markus Muellner, Daniel Burian, Christian Kudera, and Wolfgang Kastner) [7].

C. Dekriptovanje WiFi saobraćaja i pasivna mrežna forenzika korišćenjem softvera Wireshark

Jedan od najčešćih i najkorišćenijih alata za u digitalnoj mrežnoj forenzici je svakako WireShark[8] nastao krajem već davne 1997. godine od strane Džeralda Kombsa (Gerald Combs) na bazi biblioteke tcpdump i prvobitno nazvan Ethereal.
Na inicijalnom otvaranju Wiresharka-a potrebno je izabrati mrežni interfejs koji ćemo koristiti. U našem slučaju to je eth0. Odmah po biranju i startovanju dobijamo mnoštvo paketa koji velikom brzinom registruje Wireshark. Teško je pratiti golim okom detalje bez filtriranja paketa koji su nam interesantni. Za tu svrhu koristimo aktivne filtere koje nudi Wireshark, a možemo i samo da ih kreiramo ili kombinujemo sa drugim filterima.
Filtriranjem saobraćaja u realnom vremenu ili filtriranjem saobraćaja iz snimljene datoteke možemo da dobijemo mnoštvo korisnih informacija vezanih za forenzičku istragu. Wireshark je sposoban da detektuje razne maliciozne aktivnosti na mreži, a korišćenjem filtera se lako uočavaju. Navešću par osnovnih filtera. Korišćenjem filtera „arp“ dobijamo spisak svih IP adresa iz opsega koje imaju aktivnu komunikaciju u vremenu analize. Filterom „ip.addr==192.168.1.104“ možemo da se fokusiramo samo na jednu IP adresu (192.168.1.104) koju želimo da analiziramo kao i da dodamo više filtera u nizu koristeći komandu „&&“. SMB filterom možemo okvirno saznati koji operativni sistem se koristi na toj adresi jer većina operativnih sistema Windows ima otvoren SMB 445 port. Specifičnim odgovorom za svaki operativni sistem se dobija okvirna informacija o kojem je sistemu riječ. Analizom MAC adresa se dobijaju informacije o proizvođaču mrežne opreme ili samog uređaja. Filtriranjem DNS zahtjeva i odgovora dobijamo jasniju sliku šta koji uređaj na mreži radi i koje veb stranice posjećuje. *Wireshark*-om je moguće detektovati i razna ometanja WiFi mreže i pomoću detekcije okvira za deautentifikaciju (deauthentication frame) kao i otkrivanje lokacije napadača uz pomoć navedenih antena.

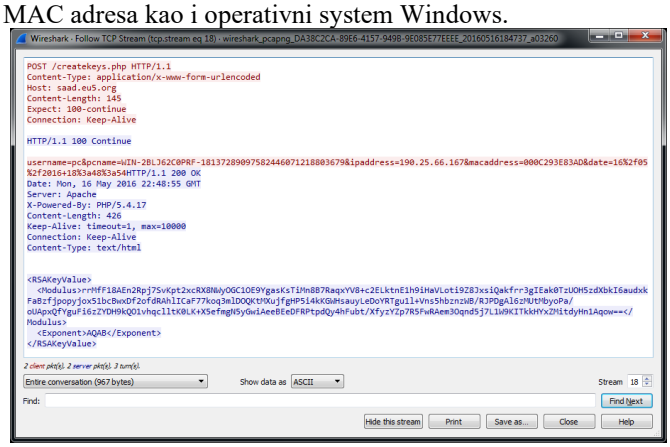
[1] https://www.aircrack-ng.org/
[2] https://en.wikipedia.org/wiki/Yagi%E2%80%93Uda_antenna
[3] https://en.wikipedia.org/wiki/Cantenna
[4] https://en.wikipedia.org/wiki/Parabolic_antenna
[5] https://en.wikipedia.org/wiki/WokFi
[6] https://www.changpuak.ch/electronics/cantenna.php
[7] https://eprint.iacr.org/2016/547.pdf
[8] https://www.wireshark.org/

Sav saobraćaj koji je wireshark detektovao moguće je snimiti u posebnu datoteku i kasnije je obrađivati u wiresharku ili u nekom drugom alatu. Datoteke iz drugih softvera moguće je takođe otvoriti u wiresharku i forenzički obrađivati.
Kao što smo već napomenuli, prethodno snimljeni WiFi saobraćaj u datoteci Stole.cap možemo otovriti u Wireshark-u. Bez poznatog ključa ne možemo mnogo toga otkriti što bi nam bilo od koristi. Ako imamo lozinku onda je možemo unijeti u Wireshark i dobiti dekriptovan saobraćaj.
To ćemo uraditi na sledeći način:
Edit>>Preferences>>Protocols>>IEEE802.11>>Decryption keys>>Edit
Važno je napomenuti da sav saobraćaj koji je bio zaštićen SSL sertifikatom ili bilo kojom drugom enkripcijskom zaštitom je nemoguće dekriptovati osim ako se u radu koristi aktivne metode forenzike koje aktivno utiču u rad mreže.

D. *Detekcija ransomware napada i moguća dekripcija podataka*

Razvoj i *ransomware*-a je veoma brz i raznolik. Sajber kriminalci imaju ponekad genijalne ideje kojima prevazilaze i najveće zaštitne sisteme, antiviruse, *firewall*-e ali najlakše prolaze kroz najslabiju kariku a to je sam čovjek. Ti napadi su najčešće pokretani preko zaraženih e-mailova, zaraženih USB memorija, sajtova i naravno sadržaja skinutog preko torrent mreža.

Jedan od načina kako se izboriti sa *ransomware* napadima može nam ponuditi i Wireshark kojim je moguće rano otkriti *ransomware* napad i izvući ključ za dekripciju iz mrežnog saobraćaja između zaraženog računara i napadača ako se blagovremeno reaguje. Ovaj način je neizvodljiv ako je do kriptovanja podataka već došlo a ključ poslat napadaču. Blagovremeni preventivni nadzor mreže pruža veliku šansu za rješenje.
Jedno od rješenja nudi i MikroTik[9] uređaji koji imaju mogućnost snimanja cjelokupnog saobraćaja i skladištenja u memoriji. Memorija samo MikroTik urejaja je obično mala, svega par desetina megabajta ali se može dodati USB memorijski stik velikog kapaciteta i snimati na njega ili čak strimovati saobraćaj na neku drugu mrežnu lokaciju koja je možda i najbolja opcija. Snimljeni saobraćaj se snima u datoteku sa ekstenzijom .cap koja se može importovati u Wireshark. Na podešavanjima u MikroTiku se može definisati maksimalna veličina datoteke koja kada se popuni zadati limit briše najstarije pakete iz snimljene datoteke osvježavajući ih novijim paketima. Veoma je korisno recimo ako se može sačuvati snimljeni saobraćaj u vremenskom rasponu od mjesec dana jer ako dođe do napada onda sigurno postoji snimljen saobraćaj između zaraženog računara i servera napdača. Osim ključa može se saznati i IP adresa na koju se salje ključ kao i potencijalna lokacija samog napadača. Moguće je i dobiti više informacija kako je došlo do napada na mrežu i računare, da li je to bilo putem e-maila ili skinutog sadržaja sa interneta. Sa tim osnovnim podacima može se pokrenuti pravno gonjenje ili neke druge sudske i istražne radnje koje su važne za taj slučaj.
Na sledećoj slici vidimo snimljeni saobraćaj između zaraženog računara kojem su već kriptovani podaci i servera sajber kriminalca koji sadrži RSA ključ. Tu su i osnovni podaci o zaraženom računaru. Korisničko ime, *hostname,* IP adresa, MAC adresa kao i operativni system Windows.



https://sensorstechforum.com/wp-content/uploads/2016/05/wireshark-solution2-sensorstechforum.png

Iako je taktika kreatora *ransomware*-a da napada računare sa Windows operativnim sistemom, n ate napade nisu imuni ni drugi operativni sistemi. Dešavalo se da *ransomware* bude pokrenuti na Linux ili MacOS operativnim sistemima koji imaju Wine ili drugi emulator Windows okruženja.

E. *AKTIVNE METODE MREŽNE FORENZIKE*

Pasivnom metodom forenzike je moguće dosegnuti dosta podataka sa mreže i time ne otkrivati da se obavljaju radnje mrežne forenzike ali dosta informacija ostaje nedorečeno. Uređajaji koji su pasivno povezani na mrežu ali nemaju trenutno aktivnosti obično se teško primjete kao i uređajaji koji koriste neke od vidova enkripcije saobraćaja kao na primjer saobraćaj koji je zaštićen SSL (Secure Socket Layer) sertifikatima. U tim slučajevim se pristupa sa aktivnom mrežnom forenzikom. Zavisno od načina rada aktivna mrežna forenzika može da bude veoma neprimjetna ali i veoma invazivna pa čak u određenim uslovima da ometa rad mreže skoro do potpunog pada. To najčešće uzrokuje loša i slaba mrežna oprema ali i slaba oprema samog forenzičara kao i loša veza forenzičara i mreže.

F. *Ettercap, arpspoof, bettercap i sslstrip*

Preusmjeravanje saobraćaja se vrši nekim od alata kao što su arpspoof[10], ettercap[11] ili njegov naslednik bettercap[12]. Uz njih se mogu koristiti i sslstrip[13] koji vrši manipulaciju sa SSL sertifikatima i time omogućuje dekripciju saobraćaja razmjenjujući lažne ključeve sa korisnikom i serverom.
Vrlo uspješno se može pomoću BASH skripte kreirati komanda koja snima sav saobraćaj u pcap datoteke, kreira

[9] https://wiki.mikrotik.com/wiki/Manual:Tools/Packet_Sniffer

[10] https://github.com/smikims/arpspoof
[11] https://www.ettercap-project.org/index.html
[12] https://www.bettercap.org/
[13] https://moxie.org/software/sslstrip/

dnevnike (logove), preusmjerava sav saobraćaj a objedinjuje ettercap i sslstrip.

G. Aktivna mrežna forenzika kroz invazivni pristup

Kada dođe do napada na mrežu ili mrežne uređaje i kada su ugroženi podaci, uređaji ili integritet cjelokupne mreže važno je djelovati brzo na zaštiti podataka i same mreže pa je tim od izuzetnog značaja lociranje napadača i neutralisanje prijetnje. U ekstremnim situacijama javlja se potreba da napadač bude direktno napadnut sa ili bez njegovog znanja kako bi se što prije i što bolje zaštitila mreža ili računarski sitem a time prikupio što veći broj podataka i informacija koje su značajne za forenzičko ispitivanje. Za tu svrhu možemo koristiti razne alate ali mi ćemo koristiti *metasploit framework*[14].

Metasploit posjeduje široku paletu modula, enkodera, *eksploita,* skenera i drugih alata. Moguće je učitati rezultate drugih mrežnih skenera kao što je nmap i po njima planirati dalje akcije forenzičke istrage. Koliko je *metasploit* moćan govori podatak da osim osnovnih i naprednih mrežnih i sistemskih radnji, moguće je pristupiti ranjivim računarima bez ikakvih ozbiljnijih prepreka ili bez prepreka uopšte. Moguće je uvesti i druge module koje ne dolaze standardno uz metasploit ili čak napraviti svoje. U ovom radu ćemo prikazati praktičan prijmer invazivnog pristupa jednom računaru sa operativnim sistemom Windows XP koji napadač koristi.

Korištenjem Wireshark-a i Etherape-a lako možemo otkriti i DOS (Denial Of Service) napade. Iako je Etherape oskudniji sa opcijama i filterima u ovom slučaju lakše se primjećuje abnormalna mrežna aktivnost. Wireshark detektuje istu mrežnu abnormalnost ali sa detaljnijim prikazom događaja. U filtriranju adresa i količine paketa vidimo da je skoro kompletan saobraćaj popunjen paketima sa dvije IP adrese. Količina paketa koja je prošla kroz Wireshark a odnosi se na ovaj DOS napad čini preko 49,9% cjelokupnog saobraćaja. Ovim i ostalim podacima koje je zabilježio Wireshark lako zaključujemo da se radi o DOS napadu koji se odvija u lokalnoj mreži.

Korišćenjem softvera nmap metodom horizontalnog, vertikalnog i dubinskog skeniranja dobijamo informaciju da napadač koristi operativni system Windows XP koji je zbog prestanka ažuriranja od strane kompanije Microsoft ostavljen na milost i nemilost raznim prijetnjama. Vidimo da je otvoren port i 445 koji je uobičajeno ranjiv na ovom operativnom sistemu i njegovim srodnim sistemima. Konkretno se radi od propustu CVE-2008-4250[15].

Koristićemo ovaj sigurnosni propust kako bi pristupili računaru koji koristi napadač i saznali više informacija važnih za forenzičko istraživanje. *Metasploit* pokrećemo na operativnom sistemu Kali linux komandom u terminalu "msfconsole". Po otvaranju metasploit konzole unosimo komandu sa parametrima "use exploit/windows/smb/ms08_067netapi". Dalje koristimo našu IP adresu kako bi smo uspostavili komunikaciju na željenom portu koji može biti bilo koji slobodan port kao i IP adresu napadača uz pomoć komande LHOST, LPORT i RHOST. Kada smo unijeli sve odgovarajuće parametre pokrećemo napad komandom "exploit".

Po pokretanju napada vidimo otvorenu sesiju na napadnutom računaru i pokrećemo dalje istraživanje. U ovom momentu imamo dosta načina da saznamo šta napadač trenutno radi na računaru putem prikupljanja rada na tastaturi i mišu, snimanja trenutnog stanja na ekranu, paljenje i slikanje sa veb kamerom, snimanje zvuka u okruženju računara paljenjem i snimanjem putem mikrofona ugrađenog u računar, snimanje mrežnog saobraćaja direktno u napadačevom računaru i brojne druge mogućnosti.

Pristupom na napadačevom računaru daje mogućnost snimanja saobraćaja. Snimanje mrežnog saobraćaja možemo vršiti na dva načina putem modula sniffer i packetrecorder.

Sniffer modul je dovoljno pametan da prepozna i ignoriše pakete od metasploit sesije i koristi SSL/TLS tunel tako da je potpuno enkriptovan. Jedina mana ovog modula je ograničena količina paketa koju može da snimi a to je 200 000 paketa.

Drugi način snimanja saobraćaja je putem modula packetrecorder koji može neograničeno snimati saobraćaj na lokaciju u našem računaru. Korišćenjem komande "–i" za redni broj mrežnog interfejsa, komande "-l" kojom određujemo lokaciju snimanja saobraćaja, kao i vremenski okvir snimanja saobraćaja uz modul packetrecorder započinjemo snimanje saobraćaja.

Odredili smo vremensko snimanje na 120 sekundi kako bi lakše i brže obrađivali snimljeni saobraćaj.

Daljom analizom snimljenog saobraćaja dobijamo više podataka korišćenjem softvera tshark. Kombinacijom tshark-a i komandom za pretragu grep brzo pretražujemo podatke iz snimljenih datoteka. Traženje pojma dns nam pokazuje njegove DNS upite kao i pojam "cookie" koji pokazuje snimljene sesije kolačića koje je upotrijebio internet pregledač. Ovim putem možemo snimiti i izolovati kolačić neke od društvenih mreža koje su ostale snimljene u pregledaču i unijeti ih u naš pregledač kako bi direktno saznali o kojem se licu tačno radi. Ovo poslednje opisano se zove *cookie hijacking* odnosno krađa kolačića ili sesije i ovaj metod je široko rasprostranjen od strane sajber kriminalaca koji imaju za cilj krađu identiteta ili nanošenja štete.

Modulom ps vidimo pokrenute aplikacije a između ostalih i aplikaciju cmd.exe kao i ping.exe. Napdač ima pokrenut i internet pregledač Mozila Firefox.

Da bismo spriječili dalji napad unosimo komandu kill i broj aktivnog procesa koji je u ovom slučaju 1000. Da bi smo potvrdili prekid napada sa računara napadača, ponovo snimamo ekran napadačevog računara sa paralelnim praćenjem mreže gdje u se jasno vidi da je DOS napad prestao onog trenutka kada smo prekinuli proces ping.exe.

Ova metoda je krajnje invazivna jer smo doslovno rečeno upali u računar napadača koji u tom trenutku vrši napad. Slične ili iste metode koriste sajber kriminalci širom svijeta pa ovakav vid forenzike može da bude sa pravnog aspekta upitan ako ne i nelegalan. Zavisno od zemlje do zemlje svijeta, pravnog sistema i zakona kao i ugovora između poslodavca i

[14] https://www.metasploit.com/
[15] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

zaposlenih ovaj vid forenzike može da bude i krajnje legitiman.

H. BitTorrent protokol i zloupotreba

U današnjim vremenima često se susrećemo sa aplikacijama koje omogućuju dijeljenje sadržaja putem torent (torrent) klijenata. Velike pogodnosti i jeftina implementacija takvog načina dijeljenja je vrlo popularna u svijetu ali je vrlo često zloupotrijebljena. Obzirom da je koršćenje BitTorrent protokola uglavnom vezao za kršenje autorskih prava, većina razvijenih zemalja je zabranila ovaj protocol preko svojih internet provajdera. BitTorrent saobraćaj se putem WireSharka može pratiti korištenjem odgovarajućeg filtera, kao na primjer bittorent koji su implementirani u WireShark.

I. Nmap ili Zenmap

Nmap[16] je nezaobilazni i najpotpuniji alat za skeniranje i mreže, uređajaja i mrežnih portova. Postoji i njegova verzija sa grafičkim okruženjem koja se zove zenmap. Ima mogućnosti skeniranja i prepoznavanja operativnog sistema uređaja koje se nalaze na mreži kao i topologiju kompletne mreže ali u svojoj verziji sa grafičkim okruženjem. Može da snimi rezultate skeniranja u posebnu datoteku koju je moguće kasnije otvoriti i obrađivati u drugim softverima. Nmap ima mogućnost prepoznavanja operativnog sistema skeniranog uređajaja na mreži sa viskom stopom uspješosti, takođe i stelt mod (Stealth mode) koji omogućava skeniranje mreže sa što manje mrežne buke kao i lažiranje MAC adrese (MAC spoofing) kojom omogućava skeniranje mreže ali sa lažnom MAC adresom i time ne otkriva tačnu MAC adresu mrežnog uređajaja osobe koja vrši aktivnu mrežnu forenziku. Detekcijom operativnog sistema sužavamo i sortiramo uređaje koji su povezani na mrežu koju obrađujemo.

III. DIGITALNA FORENZIKA MREŽNOG UREĐAJA

A. MikroTik – RouterOS

MikroTik[17] je kompanija osnovana 1996. godine u Letoniji sa ciljem da razvije i unaprijedi poslovanje i internet provajdera kroz tehnička rješenja i razvoj mrežne opreme.
Fleksibilnost RouterOS sistema dala mu je mogućnost instalacije na široku lepezu harverskih platformi. RouterOS se uspiješno pokreće na mikroprocesorima MIPS, PowerPC, X86, TILE i ARM arhitekturama.

Kada želimo da radimo forenziku na nekom uređaju bilo da je mrežni uređaj, mobilni telefon, računar ili server prvo na šta obraćamo pažnju su naravno logovi. Ne cuvaju svi uređaji logove u toku rada i kada ih čuvaju ne bilježe sve događaje. Obično se logovi na standardnim konfiguracijama čuvaju u okviru RAM memorije kao što je slučaj i sa MikroTik uređajima osim ako nismo u podešavanjima podesili da logove čuva na fleš memoriji. Kod MikroTik uređaja standardna podešavanja čuvaju do sto linija događaja u okviru RAM memorije pa se odmah nakon gašenja uređaja svi događaji izgube. Zbog toga moramo biti veoma oprezni i imati na umu tu činjenicu kako ne bismo izgubili dragocjene podatke važne za forenziku. U slučaju da nemamo pristupne podatke od uređaja možemo da pristupimo drastičnim mjerama i pokušamo da pristupimo uređaju metodom *bruteforce* koja u ovom slučaju može da ima više štete nego koristi jer RouterOS sve pokušaje pristupa bilježi u logove kao novu liniju brišući najstariju liniju.

Jedan od najpoznatijih sigurnosnih propusta je CVE-2018-14847[18] koji je omogućio napadačima pristup hiljadama MikroTik uređaja širom svijeta. Najveću štetu su pretrpjeli uređaji u Brazilu gdje je bilo zaraženo preko 200 000 MikroTik uređaja. Napadači su najčešće podešavali uređaje tako da svako ko je povezan na MikroTik mogao da postane žrtva *CryptoJacking*[19] -a. Ako nemamo pristupne podatke MikroTik uređaja koji želimo forenzički da obrađujemo možemo da koristimo i već pomenuti sigurnosni propust CVE-2018-14847 ali samo na verzijama RouterOS-a od 6.29rc1 do 6.43rc3 kao i sve *Stable* verzije između koji imaju otvoren port 8291 ili port 80. Ovom metodom ne narušavamo integritet log evidencije događaja ništa više nego kao i da imamo pristupne podatke jer se u logu uređaja evidentira MAC adresa uređaja koji se u tom momentu povezao na MikroTik a na sledećoj liniji loga IP adresa sa koje se pristupilo podešavanjima.

Pristupom MikroTik uređaju možemo da vidimo aktivne konekcije na mrežnim interfejsima kao i logove. Mrežni interfejs ether2, ether3 i wlan1 povezani su kao portovi u bridge-u i dijeli isti IP opseg adresa spojenih na jedan DHCP server dok je mrežni interfejs ether1 ima ulogu kao DHCP klijent, odnosno povezan je na WAN (Wide Area Network) i putem njega dobija pristup internetu. Na podešavanjima vezanim za *firewall* vidimo sedam preusmjeravanja sa lokalnih IP adresa i njihovih portova na javnu IP adresu. Analizom tih lokalnih IP adresa dolazimo do zaključka da je sa četiri prethodno pomenuta servera koja smo otkrili softverom nmap preusmjereni svih sedam portova. Ovim preusmjeravanjima dobija se direktan pristup serverima i njihovim servisima sa drugih javnih adresa. Svi portovi su nespecifični osim porta 8080 koji se može koristiti kao alternativni port 80 u slučaju da je port 80 zauzet nekim drugim aktivnostima ili internet provajder jednostavno zabrani pristup iz WAN mreže na port 80. Pretragom logova na ovom uređaju vidimo pokušaje neovlašćenog pristupa različitim korisničim imenima i lozinkama koje su uspiješno odbijene. IP adrese sa koje se vrše ti napadi odgovaraju zemljama dalekog istoka a naročito NR Kine kao i zemljama centralne Afrike.

B. Cisco

Cisko[20] (Cisco) je multinacionalna i najveća kompanija koja se bavi razvojem mrežne oprememe i najuticajnija je u domenu mrežnih standarda. U današnje vrijeme nemoguće je zamisliti

[16] https://nmap.org/
[17] https://mikrotik.com/
[18] https://nvd.nist.gov/vuln/detail/CVE-2018-14847
[19] https://www.wired.com/story/cryptojacking-took-over-internet/
[20] https://www.cisco.com/

bilo kakav ozbiljniji mrežni sistem bez ciska. Kao najrasprostranjenija kompanija u svijetu logično je da je njihovo iskustvo u domenu zaštite i forenzike najveće. Iskusan forenzičar mora da ima neophodno znanje kako i na koji način pravilno forenzički ispitati jedan ciskov mrežni uređaj. U slučaju nepravilnog foreničkog ispitivanja sasvim sigurno se dokazi mogu kompromitovati ili uništiti. Kada dobijemo slučaj i neophodno forenzičko ispitivanje najbitnije je ne gasiti uređaj a osoba koja je zadužena na održavanju mreže koja je vjerovatno prijavila slučaj da ne dira ništa. Starije metode koje su se koristile u mrežnoj bezbijednosti iziskivale su momentalno gašenje uređaja ali sa tim bi trajno nestali podaci koji se nalaze u RAM memoriji mrežnog uređaja.

Kompromitovan mrežni uređaj je podložan različitim vrstamna napada. Napadač ga može onesposobiti, koristiti za DOS ili DDoS napade, zaobići filtere paketa (firewall), upasti i napasti druge mrežne uređaje ili računare, snimati i prisluškivati saobraćaj, preusmjeriti dio ili cjelokupan saobraćaj i drugo. Lista zloupotreba je velika.

Važno je imati na umu da ciskovi uređaji kao is vi uređaji imaju dcije vrste memorije a to su RAM i FLASH memorija. Zavisno od memorije možemo naći dvije vrste konfiguracije in a njih treba obratiti posebnu pažnju. Kod fleš (FLASH) memorije se nalazi startna konfiguracija uređaja koju napadač obično ne kompromituje. Fleš memorija je trajna i podaci koji se nalaze na njoj su trajni. Osim startne konfiguracije tu su i sistemski podaci od mrežnog uređaja. Tu konfiguraciju uređaj koristi za pokretanje osnovnih mrežnih funkcija. Za razliku od fleš memorije RAM memorija je mnogo interesantnija za forenzičko ispitivanje. RAM memorija sama po sebi ne zadržava podatke poslije ponovnog pokretanja uređaja zato je važno imati na umu ovu činjenicu. U njoj se nalazi radna konfiguracija (Running configuration) koja sadrži sve važne podatke kao što su dinamičke tabele za ARP, pravila rutiranja, statistike i drugo.

IV. Rezultati

Opensource zajednica je ogromna i svakim danom je sve veća. Dosta ljudi se uključuje u rad i razvoj različitih softvera i samim tim softveri za forenziku su sve brojniji i moćniji. Upotrebom ovih softvera došli smo do zaključka da bez ikakvih problema mogu parirati komercijalnim softverima a u mnogim segmentima ih nadmašuju. Pojedinačnim softverima možemo dosta saznati ali njihovom kombinacijom ili čak simultanim radom dobijamo dosta preciznije rezultate korisne istrazi ili nadzoru. Često smo koristili Wireshark sa standardnim filterima i dodacima koji dolaze uz njega. Dodavanjem drugih dodataka postaje moćniji i korisniji u zavisnosti šta forenzički istražujemo.

Forenzičkim ispitivanjem aktivno ili pasivno sa ili bez pristupa mreži može dovesti do interesantnih zaključaka koji su korisni za istragu, praćenje lica ili kriminalnih aktivnosti. Iako je pasivna metoda se vrlo teško otkriva od strane napadača ponekad ne pruža dovoljno informacija. Kao što napadači koriste razne sigurnosne propuste forenzičar ih može, uz pravilnu upotrebu upotrijebiti za istragu. Važno je napomenuti da invazivne metode mrežne forenzike prethodno imaju odobrenje od vlasnika mreže ili suda jer se nelegalno dobijeni dokazi mogu oboriti na sudu.

V. Zaključak

Svi smo danas na neki način onlajn, ako nismo direktno onda su neki od naših podataka sigurno smješteni u neku bazu ne nekom serveru ili postoji bilo kakav trag u elektronskom obliku koji može nekome koristiti a nama naškoditi u slučaju da padne u pogrešne ruke. Danas su sajber kriminalci aktivniji više nego ikad a kako vrijeme prolazi biće sve više. Redovno traže i nalaze načine kako da zaobiđu sigurnosne zaštite i vrlo teško je pratiti njihov razvoj. Nažalost, među njima ima i mnogo genijalnih umova koji bi mogli kada bi htjeli mnogo učiniti za dobrobit čovječanstva.

Zahvalnice

Želim da se zahvalim mom mentoru i profesoru Doc. Dr Nenadu Ristiću na nesebičnoj pomoći u radu, rukovodstvu i službama Univerziteta Sinergija kao i mojoj porodici.

Literatura

[1] Ahmad, M., & Ullah, K. (2017). SNORT IMPLEMENTATION WITH WIRESHARK HELPING AVOIDING DDOS ATTACK IN THE CLOUD COMPUTING. *International Journal of Computer Science and Information Security*, *15*(1), 504.

[2] Bijmans, H. L., Booij, T. M., & Doerr, C. (2019, November). Just the Tip of the Iceberg: Internet-Scale Exploitation of Routers for Cryptojacking. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 449-464).

[3] Bullock, J., & Parker, J. T. (2017). Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework. John Wiley & Sons.

[4] Chen, J., Wang, C., Zhao, Z., Chen, K., Du, R., & Ahn, G. J. (2017). Uncovering the face of android ransomware: Characterization and real-time detection. *IEEE Transactions on Information Forensics and Security*, *13*(5), 1286-1300.

[5] Jevremović, A., Veinović, M., Šarac, M., Šimić, G., (2018) Zaštita u računarskim mrežama, Univerzitet Singidunum,

[6] Kammerstetter, M., Muellner, M., Burian, D., Kudera, C., & Kastner, W. (2016, August). Efficient high-speed WPA2 brute force attacks using scalable low-cost FPGA clustering. In *International Conference on Cryptographic Hardware and Embedded Systems* (pp. 559-577). Springer, Berlin, Heidelberg.

[7] Morato, D., Berrueta, E., Magaña, E., & Izal, M. (2018). Ransomware early detection by the analysis of file sharing traffic. *Journal of Network and Computer Applications*, *124*, 14-32.

[8] Özer, E., & Iskefiyeli, M. (2017, October). Detection of DDoS attack via deep packet analysis in real time systems. In *2017 International Conference on Computer Science and Engineering (UBMK)* (pp. 1137-1140). IEEE.

[9] Sanders, C. (2017). Practical packet analysis: Using Wireshark to solve real-world network problems. No Starch Press.

[10] Scholten, C. P. B. (2019). Hacking the router: characterizing attacks targeting low-cost routers using a honeypot router (Bachelor's thesis, University of Twente).

[11] Shorey, T., Subbaiah, D., Goyal, A., Sakxena, A., & Mishra, A. K. (2018, September). Performance comparison and analysis of slowloris, goldeneye and xerxes ddos attack tools. In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 318-322). IEEE.

[12] Tayag, M. I., & De Vigal Capuno, M. E. A. (2019). Compromising Systems: Implementing Hacking Phases. *International Journal of Computer Science & Information Technology (IJCSIT) Vol*, *11*