**SVEUČILIŠTE U ZAGREBU**

**FAKULTET ORGANIZACIJE I INFORMATIKE**

**V A R A Ž D I N**

**David Kajzogaj**

**Hrvoje Lukšić**

**Rene Ivetić**

**Augustin Lukić**

**Building a Red Team Infrastructure**

**Projektni rad**

**Varaždin, 2024.**

**SVEUČILIŠTE U ZAGREBU**

**FAKULTET ORGANIZACIJE I INFORMATIKE**

**V A R A Ž D I N**

**David Kajzogaj**

**Hrvoje Lukšić**

**Rene Ivetić**

**Augustin Lukić**

**Building a Red Team Infrastructure**

**Projektni RAD**

**Varaždin, siječanj 2024.**

*David Kajzogaj*

*Hrvoje Lukšić*

*Rene Ivetić*

*Augustin Lukić*

**Izjava o izvornosti**

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

*Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Sažetak**

Red tim (eng. red team) infrastruktura predstavlja ključni element u jačanju sigurnosti organizacije. Ovaj tim ima zadatak simulirati napade na sustav kako bi identificirao ranjivosti i nedostatke u sigurnosnim mjerama. Izrada red tim infrastrukture zahtijeva pažljivo planiranje i implementaciju različitih alata i tehnika kako bi se osiguralo realistično testiranje sigurnosnih sustava. Prilikom izrade, potrebno je definirati jasne ciljeve testiranja, identificirati ključne mete, te odabrati i konfigurirati alate koji će omogućiti simulaciju napada. Red tim infrastruktura također uključuje postavljanje monitoringa i logiranja kako bi se pratio tijek testiranja te pravovremeno identificirale anomalije. Uz to, važno je educirati članove red tima o trenutačnim prijetnjama i tehnikama napada. Kroz sustavno i dobro vođeno testiranje, organizacija može poboljšati svoje sigurnosne mjere i proaktivno reagirati na potencijalne prijetnje.

**Ključne riječi:** Red tim, infrastruktura, simulacija napada, alati, monitoring, logiranje…

# **Sadržaj**

[**Sadržaj** iii](#_Toc157001930)

[**1.** **Uvod** 1](#_Toc157001931)

[**1.** **Metode i tehnike rada** 2](#_Toc157001932)

[**2.** **Vlastiti praktični dio** 3](#_Toc157001933)

[**2.1** **C2 centralni server - Sliver** 3](#_Toc157001934)

[**2.2** **HTTP/S i DNS redirektori** 3](#_Toc157001935)

[**2.3** **Payload** 6](#_Toc157001936)

[**2.4** **Postfix** 7](#_Toc157001937)

[**2.5 Gophish** 9](#_Toc157001938)

[**3.** **Zaključak** 16](#_Toc157001939)

[**Popis slika** 19](#_Toc157001940)

# **Uvod**

U današnjem digitalnom okruženju, gdje su informacije ključna valuta, organizacije se suočavaju s sve sofisticiranijim prijetnjama koje zahtijevaju inovativne i proaktivne pristupe sigurnosti. U tom kontekstu, koncept red tim infrastrukture izranja kao esencijalna komponenta strateškog odgovora na suvremene izazove. Red tim, kao dinamičan skup stručnjaka, ne samo da simulira napade na organizaciju, već pruža dubok uvid u stvarnu otpornost njenih sigurnosnih sustava.

Ključna svrha red tima nije samo otkrivanje ranjivosti, već i razumijevanje složenosti napadačkih scenarija te testiranje sposobnosti organizacije da prepozna, zaustavi i reagira na prijetnje u stvarnom vremenu. Red tim infrastruktura ne samo da identificira tehničke ranjivosti, već i procjenjuje efikasnost procesa, ljudskih resursa te politika sigurnosti.

U uvodu naglašavamo važnost proaktivnog pristupa sigurnosti, izazove koje donosi brza evolucija tehnologije, te potrebu za stalnim usavršavanjem sigurnosnih praksi. Red tim postaje ključan instrument u ostvarivanju ovog proaktivnog pristupa, omogućavajući organizacijama da anticipiraju prijetnje prije nego što postanu ozbiljni rizici. Ovaj uvod poziva na dublje istraživanje red tim infrastrukture kao kritičnog elementa zaštite informacijske sigurnosti u suvremenom poslovnom okruženju.

# **Metode i tehnike rada**

Pri razradi teme korišteni su sljedeći alati:

* **C2 server**  – slanje naredbi/kontrola nad zaraženim računalom.
* **Postfix** – slanje elektroničke pošte.
* **Gophish** – simulacija phishing napada
* **HTTP/S i DNS redirektori** – preusmjeravanje prometa
* **Google Chrome** - pretraživanje postojećih radova i istraživanje teme.
* **Microsoft Word 2020** – alat kojim smo se koristili za oblikovanje i pisanje teksta.
* **Powerpoint** – alat za izradu prezentacije.

# **Vlastiti praktični dio**

# **C2 centralni server - Sliver**

1. Instalirati server na linuxu <https://sliver.sh/docs?name=Getting+Started>   
   Za lokalne operacije i testiranje dovoljno je jednostavno pokrenuti „sliver-server“   
   Za operacije s više sudionika server se može uspostaviti i kao linux servis i instalirat u npr. DigitalOcean serveru za laku uporabu od bilo kuda kao u našem projektu.
2. Multiplayer (više operatora u Sliveru):

DETALJI <https://sliver.sh/docs?name=Multi-player+Mode>   
Na strani servera:

* Pokrenuti server
* Kreirati konfiguraciju operatora, za parametar lhost unijeti javni IP računala/servera („ip addr show“)
* **Pokrenuti multiplayer mode**

Na strani klijenta:

* Preuzeti datoteku sliver-client za odgovarajući OS sa Sliver Githuba
* Preuzeti konfiguracijsku datoteku koju je generirao server
* Pokrenuti sliver-client (pisat će gdje se konfiguracija treba nalaziti)
* Klijent bi sada trebao biti povezan na Sliver server od bilo kuda sa svim mogućnostima

# **HTTP/S i DNS redirektori**

HTTP domena registrirana na ap.www.namecheap.com: **sis-projekt.shop**

A screenshot of a computer

Description automatically generated

Slika 1. HTTP domena [Vlastita izrada]

Za domenu je potrebno dodati posebne nameserver adrese ovisno o tome gdje hostamo server, u ovom slučaju ns1.digitalocean.com i ns2.digitalocean.com

A screen shot of a computer

Description automatically generated

Slika 2. Namerserver adrese za domenu [Vlastita izrada]

Besplatan server hosting na digitalocean.com (lozinka za pristup ssh: 1JakaLozinka), dodana prethodno registrirana domena radi povezanosti

<https://cloud.digitalocean.com/projects/58c65d2c-a699-48e0-9b65-d5f29596daa1>

A screenshot of a computer

Description automatically generated

Slika 3. Digitalocean hosting [Vlastita izrada]

U virtualci uspostavljen HTTPS certifikat pomoću Certbot (<https://certbot.eff.org/instructions?ws=nginx&os=ubuntufocal&tab=standard>)

A screenshot of a computer

Description automatically generated

Slika 4. HTTPS certifikat [Vlastita izrada]

A computer screen with text

Description automatically generated

Slika 5. Opis certifikata [Vlastita izrada]

Zadnji korak je uspostaviti nginx redirekciju na naš C2 Sliver server. Za to se treba postaviti tajna putanja i provjeriti sadrži li http zahtjev ispravan *user-agent string.* Tajna putanja je postavljena na sis-projekt.shop/secret*,* a potreban *user-agent* je “c2agent” (postavlja se u sliver-server http-c2.json datoteci).

A computer screen with white text

Description automatically generated

Slika 6. Nginx redirekcija na C2 sliver server [Vlastita izrada]

Pristupom tajnoj lokaciji bez ispravnog *user-agenta* dobivamo grešku 403, a pristupom korijenu stranice poruku dobrodošlice, no radi prividne legitimnosti bilo bi dobro izraditi neku normalnu stranicu.

DNS redirektor uspostavlja se postavljanjem IPTABLES pravila na redirektoru.

A computer screen with white text

Description automatically generated

Slika 7. IPTABLES pravila redirektora [Vlastita izrada]

Zatim i potrebnih DNS recorda na DigitalOceanu prema uputama na <https://sliver.sh/docs?name=DNS+C2>

A screenshot of a computer

Description automatically generated

Slika 8. DNS recordi na DigitalOceanu [Vlastita izrada]

# **Payload**

Payload je srž našeg napada, datoteka koja kad se pokrene šalje C2 Serveru remote command line čime cijelo računalo pada pod našu kontrolu. U našem slučaju koristili smo https session generiran sljedećom naredbom u Sliveru (ovo je debug verzija s informacijama o povezanosti). Primijetimo korištenje registrirane domene i tajne putanje koju smo definirali ranije:

A screen shot of a computer program

Description automatically generated

Slika 9. HTTP session u Sliveru [Vlastita izrada]

Takvu datoteku šaljemo mailom žrtvama pomoću Gophisha i postfixa. Nakon pokretanja http/s listenera na našoj instanci C2 Servera, pokretanjem datoteke na računalu žrtve dobivamo potpunu sesiju terminala žrtve (istoj sesiji može se pristupiti od bilo kuda pomoću Sliver multiplayera!):

A black screen with white text

Description automatically generated

Slika 10. Sesija žrtve u terminalu [Vlastita izrada]

# **Postfix**

Potreban nam je operativni sistem baziran na **Linuxu**.

Za potrebe ovog projekta koristiti ćemo **Ubuntu** na virtual boxu.

Otvaramo terminal i instaliramo potrebne pakete za **Postfix** i **Mail Utilities**.



Otvaramo konfiguracijsku datoteku Postfixa.



Modificiramo ga tako da izmjenjujemo/dodajemo ove retke pomoću Vim, Gedit ili Nano editora teksta.



Spremamo datoteku.

Kreiramo novu datoteku koja će sadržavati podatke o našem mailu koji koristimo.



Kreiramo hash mapu za datoteku u kojoj su sadržani podaci o pristupu mailu koji koristimo.



Kreirati datoteku header\_checks sa sljedećim postavkama (također je potrebno instalirati sudo apt install postfix-pcre):

A screen shot of a computer

Description automatically generated

Slika 11. Datoteka header\_checks [Vlastita izrada]

Ponovo pokrećemo postfix kako bi učitali nove postavke.



# **2.5 Gophish**

GoPhish se koristi kao alat za izvođenje phishing kampanja. Njegova uloga je pomoći u postavljanju infrastrukture za phishing, kao i u kreiranju, izvođenju i evaluaciji phishing kampanja. To uključuje instalaciju GoPhish-a, postavljanje mail poslužitelja, postavljanje

DNS zapisa, te testiranje i pokretanje kampanje. GoPhish omogućuje administratorima da lako postave i upravljaju phishing simulacijama kako bi testirali i poboljšali sigurnosne mjere protiv phishing napada.

KORACI za konfiguriranje GoPhish alata:

* Preuzeti .zip datoteku sa službene web stranice GoPhsish  <https://github.com/GoPhish/GoPhish/releases/download/v0.12.1/GoPhish-v0.12.1-windows-64bit.zip>
* U ovom slučaju preuzeta je instalacija za Windows, međutim postoje verzije i za Linux i OSX
* Raspakirati arhivu i pokrenuti GoPhish program
* Nakon pokretanja otvorit će se prozor s definiranim username I password računom za prijavu:
  + "Please login with the username admin and the password 05dece88f52d80f3" i s poveznicom na stranicu za prijavu <http://127.0.0.1:3333>
* Navedenu stranicu otvaramo u pregledniku bez preporučenih defaultnih sigurnosin postavki, te zanemarujemo u ovom slučaju sigurnost te kroz napredne postavke učitamo stranicu
* Nakon učitanja strancie upisujemo početne podatke za login:
  + username: admin
  + password 05dece88f52d80f3
* Zatim nas stranica traži da resetiramo lozinke na način da postavimo neku svoju po želji u minimalnoj duljini od 8 znakova. Nova lozinka: admin321
* Zatim nam se nakon uspješne prijave učitava početni ekran alata.

A screenshot of a computer

Description automatically generated

Slika 12. Gophish [Vlastita izrada]

Od kojih su nam najvažnije ove funkcionalnosti:

* Prvo se postavlja novi profil pod sekcijom Sending Profiles
* Potom se postavlja Landing Pages
* Zatim se postavljaju Email Templates
* Nakon toga se konfiguriraju Users & Groups
* Te naposlijetku kad već imamo sve definirano na samom kraju izrađuje se kampanja pod sekcijom Campaigns gdje se iz padajućih lista odabiru prethodno definirani elementi te se postavlja datum početka I završetka kampanje

U prvom koraku se postavlja Sending profile u kojem je potrebno unijeti sljedeće podatke u naznačena polja u obrascu (zapamtimo da postfix sluša na localhost:25 i preuzima mailove koje šalje Gophish):

A screenshot of a computer

Description automatically generated

Slika 13. Gophish profil [Vlastita izrada]

Ostale mogućnosti ostavimo kakve jesu po default te zatim testiramo slanje maila klikom na Send Test Email u kojem nas traži da upišemo ime, prezime i mail adresu na koju će stići testni email (bilo koja mail adresa kojoj imamo pristup ulaznoj pošti) te tako provjeriti je li profil uspješno postavljen. Nakon uspješno postavljenog profila može se prijeći na ostale funkcionalnosti GoPhisha.

Gophish sadrži vrlo detaljne funkcionalnosti kao što su HTML uređivač maila i landing stranice na koju vodi phishing link. No u našem projektu koristimo običan .exe virus koji se preuzima na linku. U stvarnim uvjetima mogao bi se izraditi vrlo uvjerljiv primjerak.

A screenshot of a computer

Description automatically generated

Slika 14. Primjer gophish maila [Vlastita izrada]

U ovom koraku se dodaju korisnici na kojima će se testirati simulacija, gdje je potrebno unijeti ime, prezime, email adresu i broj pozicije.

A screenshot of a group

Description automatically generated

Slika 15. Gophish simulacija nad korisnicima [Vlastita izrada]

Nakon što imamo sve definirano iz padajućeg izbornika odaberemo template koje smo stvorili, damo mu željeni naziv, a za polje URL: https://0.0.0.0

A screenshot of a email form

Description automatically generated

Slika 16. Primjer kampanje [Vlastita izrada]

 

Nakon pokretanja kampanje navedene grupe trebale bi primiti naš mail.

Kao što vidimo, naš mail prolazi spam filtere i ne sadrži nikakve gophish headere.

A screenshot of a computer

Description automatically generated

Slika 17. Prolazak mail-a kroz spam filtere i bez gophish headera [Vlastita izrada]

# **Zaključak**

Uvođenje red team infrastrukture u organizaciju predstavlja ključni korak prema jačanju njezine sigurnosti u dinamičnom digitalnom okruženju. Kroz simulaciju napada i analizu ranjivosti, red tim omogućuje identifikaciju potencijalnih rizika prije nego što postanu ozbiljni sigurnosni problemi. Ovaj pristup ne samo da pruža uvid u tehnološke aspekte sigurnosti, već i naglašava važnost educiranja osoblja i poboljšanja sigurnosne svijesti unutar organizacije.

Red team infrastruktura postaje neophodan element u proaktivnom pristupu zaštiti od cyber prijetnji. Kroz sustavno testiranje, organizacije mogu unaprijediti svoje sigurnosne mjere, jačati reakciju na incidente te stvarati otpornije okružje protiv naprednih prijetnji. U zaključku, red tim infrastruktura predstavlja ne samo alat za otkrivanje i rješavanje ranjivosti, već i sredstvo za podizanje sigurnosne svijesti i spremnosti organizacije na izazove suvremenog cyber prostora.

**Popis literature**

*Building a Red Team Infrastructure in 2023*. (bez dat.). Preuzeto 03. siječnja 2024. s <https://www.securesystems.de/blog/building-a-red-team-infrastructure-in-2023/>

*Certbot Instructions*. (bez dat.). Preuzeto 03. siječnja 2024. s <https://certbot.eff.org/instructions?ws=nginx&os=ubuntufocal&tab=standard>

CYE. (2023, travanj 27). Building a Modern Red Team Infrastructure. *CYESEC*. Preuzeto 03. siječnja 2024. s <https://medium.com/cyesec/building-a-modern-red-team-infrastructure-e5501784a287>

*DigitalOcean—The developer cloud*. (bez dat.). DigitalOcean. Preuzeto 03. siječnja 2024. s <https://www.digitalocean.com/>

*GoPhish*. (bez dat.). [Software]. GitHub. Preuzeto 03. siječnja 2024. s <https://github.com/GoPhish/GoPhish/releases/download/v0.12.1/GoPhish-v0.12.1-windows-64bit.zip>

Hipstertrojan. (2023, travanj 28). Building a Red Team Infrastructure in 2023. *SSE Blog*. Preuzeto 03. siječnja 2024. s <https://medium.com/sse-blog/building-a-red-team-infrastructure-in-2023-4eaef5414d92>

*Namecheap.com • Login*. (bez dat.). Preuzeto 03. siječnja 2024. s <https://www.namecheap.com/myaccount/login/?ReturnUrl=%2f>

Secprentice. (2019, siječanj 3). How To: Build Inexpensive Red Team Infrastructure. *Medium*. Preuzeto 03. siječnja 2024. s <https://secprentice.medium.com/how-to-build-inexpensive-red-team-infrastructure-dfb6af0fe15d>

*Sliver Docs*. (bez dat.). Preuzeto 03. siječnja 2024. s <https://sliver.sh/>

*SMTP Forwarders / Relays*. (bez dat.). Preuzeto 03. siječnja 2024. s <https://www.ired.team/offensive-security/red-team-infrastructure/smtp>

*The C2 Matrix*. (bez dat.). Preuzeto 03. siječnja 2024. s <https://www.thec2matrix.com/>

# **Popis slika**

[Slika 1. HTTP domena [Vlastita izrada]..................................................................................3](#Slika_1)

[Slika 2. Namerserver adrese za domenu [Vlastita izrada].......................................................4](#Slika_2)

[Slika 3. Digitalocean hosting [Vlastita izrada]..........................................................................4](#Slika_3)

[Slika 4. HTTPS certifikat [Vlastita izrada].................................................................................4](#Slika_4)

[Slika 5. Opis certifikata [Vlastita izrada]...................................................................................5](#Slika_5)

[Slika 6. Nginx redirekcija na C2 sliver server [Vlastita izrada].................................................5](#Slika_6)

[Slika 7. IPTABLES pravila redirektora [Vlastita izrada]............................................................6](#Slika_7)

[Slika 8. DNS recordi na DigitalOceanu [Vlastita izrada]……………………………………........6](#Slika_8)

[Slika 9. HTTP session u Sliveru [Vlastita izrada]…………………………………………............7](#Slika_9)

[Slika 10. Sesija žrtve u terminalu [Vlastita izrada]…………………………………………..........7](#Slika_10)

[Slika 11. Datoteka header\_checks [Vlastita izrada]………………………………………….......8](#Slika_11)

[Slika 12. Gophish [Vlastita izrada]…………………………………………………….................10](#Slika_12)

[Slika 13. Gophish profil [Vlastita izrada]……………………………………………...................11](#Slika_13)

[Slika 14. Primjer gophish maila [Vlastita izrada]…………………………………………...........12](#Slika_14)

[Slika 15. Gophish simulacija nad korisnicima [Vlastita izrada]…………………………...........13](#Slika_15)

[Slika 16. Primjer kampanje [Vlastita izrada]……………………………………………..............14](#Slika_16)

[Slika 17. Prolazak mail-a kroz spam filtere i bez gophish headera [Vlastita izrada]…….......15](#Slika_17)