Teoridel

Oppgave 1

Hvis selskapet ikke gjennomfører en penetrasjonstest kan det øke risikoen for at de utsettes for et hackerangrep. En angriper kan utføre ondsinnede angrep, slik som XSS (Cross Site Scripting), SQL injections eller spre malware for å kompromittere systemet. Dette kan medføre til at angriper kan kjøre skadelig kode, får autorisert til systemet eller at bedriftens konfidensiell faller i hendene hos angriper som videre kan bruke dette til noe ondsinnet. Dersom bedriften ofte utsettes for angrep kan dette føre til at kundene mister tilliten til selskapet som kan påvirke bedriftskontinuiteten. Dette kan medføre til et økonomisk tap i bedriften og gi andre konsekvenser dersom sårbarhetene ikke fikses.

Over 60 % av selskapene verden over har blitt utsatt for et cyberangrep i 2022 (Bulao, 2022).Dette gir en indikasjon på hvor svak sikkerheten er i bedriften. Ut ifra dette tolker jeg det som at bedriftene har ikke prioritert sikkerheten sin. Eller de har ikke implementert de riktige sikkerhetsprotokollene eller tiltakene som trengs for å beskytte virksomhetens system. Dette resulterte til at de ble utsatt for hacker angrep. Penetrasjonstesting kan beskytte disse bedriftene fra å bli utsatt for angrep. Dette kan bidra med å blant annet sikre bedriftene med å ivareta konfidensielle data eller sikre systemet mot nedtur. En hacker kan utføre ondsinnede handlinger slik som å slette og modifisere innhold på systemet. Derfor kan de være en fordel å gjennomføre penetrasjonstest mot systemene for å unngå at slikt skjer.

En penetrasjonstest er test som utføres mot systemer, applikasjoner, enheter eller nettverk for å avgjøre sikkerhetsnivået i bedriften, dette kan gi en innsikt i hvor sårbar bedriften er for cyberangrep. Penetrasjonstesting kan bidra med å oppdage og tette sårbarhetene som befinner seg i bedriftssystemet som dermed styrke sikkerheten i bedriften som minimerer risikoen for at de utsette for hackerangrep (vaultes.com, 2022). Dette kan bidra bedriften med å implementere de nødvendige sikkerhetstiltakene som er nødvendig for å sikre systemet mot ondsinnede angrep.

Siden bedriftens IT infrastruktur stadig er i utvikling er behovet for penetrasjonstesting økende ettersom det kan oppstå nye sårbarheter. Bedriften bør utføre kontinuerlig penetrasjonstesting for å styrke sikkerheten i systemet som forhindrer sårbarheter fra å oppstå. Og ettersom trusselbildet vokser benytter hackere seg av nye teknikker og metoder for å få uautorisert tilgang til systemet. Penetrasjonstesting sikrer systemet og IT miljøet som forhindrer angripere å utføre ondsinnede angrep. Dette vil også kunne bidra til å styrke integriteten i bedriften.

En etisk hacker er en sikkerhetsekspert som enten innleid eller hyret av en bedrift og har til oppgave å bryte seg inn i et system ved bruk hackingsmetoder for å identifisere sikkerhetshull og svakheter i systemet eller applikasjoner før de utnyttes av en angriper. I en sikkerhetsorganisasjon spiller de en viktig rolle siden de utfører penetrasjonstest på bedriftens IT system. De fleste mellomstore bedrifter lagrer store mengder av data på bedriftssystemene sine, dette gjør dem sårbare for hackerangrep.

I følge securitymagazine, kan databrudd i en bedrift i gjennomsnitt koste opp mot 4 millioner dollar (Henriquez, 2021). Dette er ufattelig mye penger og hvis bedriften ikke gjennomfører

penetrasjonstesting på systemene sine, så er de ikke i stand til å vite hvilke sårbarheter som befinner seg i systemet og kan ikke forhindre det heller. Hvis bedriften ofte utsettes for databrudd, kan dette etter hvert bli en kostbar faktor. Derfor kan det være en fordel å ansette eller leie etiske hackere for å finne disse sårbarhetene. Dette kan dermed redusere kostnadene i bedriften.

En etisk hacker kalles også for en white-hat-hacker og de må få autorisasjon fra bedriften før de kan ta en sikkerhetsvurdering på systemet og må i tillegg følge bedriftens retningslinjer for å utføre oppdraget sitt. De har som mål å styrke bedriftens cyberforsvar for å beskytte bedriftens konfidensielle informasjon og data. Programmering er viktig for en etisk hacker å kunne for å utføre kodeanalyse for å finne sårbarheter i en programvare og programmeringskunnskapene kan i tillegg brukes til å utvikle verktøy for å teste sårbarhetene i et system. De vanligste programmeringsspråkene er C, Java, PHP og Python (Østby, 2022).

Når de skal angripe et system gjelder det å tenke som en hacker, da må de implementere de samme kriminelle teknikkene en hacker hadde brukt for å få uautorisert tilgang for å stjele konfidensiell data eller informasjon. Deretter kan etisk hackere bruke disse sårbarhetene til å utvikle løsninger for hvordan bedrifter skal motstå ondsinnede angrep.

Etiske hackere bruker blant annet portskanningsverktøy slik som NMAP, verktøy for nettverksanalyse og penetrasjonsverktøy slik som Nessus og Owasp Zap for å se etter sårbarheter i systemet. Dersom de finner sårbarheter i systemet er det viktig at sårbarhetene dokumenteres på en riktig måte for å forhindre hacker angrep mot bedriften. En etisk hacker bør ikke dele sårbarhetsfunnene med offentligheten. Dette kan i verste fall medføre til at en hacker utnytter disse for å kompromittere systemet.

Mennesker er et av hovedårsakene til at bedriften risikerer å bli utsatt for ondsinnet angrep som kan gi en angriper uautorisert tilgang til systemet. Etiske hackere kan styrke bevisstheten blant ansatte og gi den nødvendige opplæringen dem opp til å unngå phishing metoder. Angripere kan benytte seg av phishing eller social engineerings som å ringe, sende SMS eller sende epost for å manipulere ansatte til å oppgi login credentials på systemet. Dette kan hackere utnytte for å få tilgang til systemet og opptre som brukere selv.

Angripere kan i tillegg manipulere ansatte til å laste ned skadevare på maskinene sine slik som deretter spres seg til de andre maskinene. Dette kan gi organisasjonen store konsekvenser. Derfor er det viktig for ansatte ha den opplæring slik at de kan oppdage phishing angrepene angriperen utnytter mot dem. Da lærer de å unngå svindelforsøk som kan bidra til å styrke informasjonssikkerheten til ansatte og minimere risikoen for at bedriften utsettes for angrep. Behovet for etiske hackere vil alltid være stor blant bedrifter ettersom angripere tester nye metoder for å bryte seg inn i systemet. Etisk hackere bidrar bedriften med å forbedre og ivareta sikkerheten i systemet, nettverket eller applikasjonene sine mot databrudd og andre ondsinnede angrep.

Oppgave 2

Enternalblue var en sårbarhet utviklet av NSA og lekket av en hackergruppe kalt Shadow Brokers til offentligheten i 2017 etter at de brøt seg inn i NSA og stjal den (hypr.com, 2022). Enternalblue rammet hovedsakelig de maskiner som kjørte Windows operativsystemet. Den utnytter en sårbarhet som befant seg i første versjonen av SMB protokollen som gav angripere uautorisert tilgang til nettverket og muliggjorde det å kjøre skadelig kode som spredde seg til andre maskinene på nettverket.

Ifølge nettsiden Wikipedia (Wikipedia.com , 2022), varslet NSA om Enternalblue til Windows etter lekkasjen. Videre medførte dette til at de måtte forberede en patch som ble lansert til de fleste Windows versjonene slik som Windows Vista, Windows 10, Windows 7 og Windows XP. Patchen skal forhindre Enternalblue fra å infisere de sårbare maskinene, men etter at Windows la ut en patch var det fremdeles mange organisasjoner og brukere som ikke hadde patchet maskinene som resulterte til mange maskiner var sårbare for Enternalblue. Dette åpnet dørene for ondsinnede aktørene å aksessere nettverket og spre ondsinnede pakker for å utløse malware angrep på de maskinene som ikke var patchet i nettverket.

Som nevnt tidligere utnyttet Enternalblue sårbarheten SMB protokollen som er en protokoll for deling av filer som muliggjorde det for eksterne angripere å få uautorisert tilgang til nettverket og utløse malware angrep slik som ramsonware, trojanere og virus. Dersom en ondsinnet aktør infiserte en maskin med Enternalblue, ville dette ramme alle maskinene som er koblet på samme nettverk. Enternalblue ble brukt av ondsinnede aktører til å spre skadevare.

Skadevare er skadelige programvare utviklet av ondsinnede aktører. Skadevarene har som hensikt å utføre ondsinnede handlinger mot et system. Malware sprer seg gjennom phishing mail eller via internett. Eksempelvis, kan en angriper benytte seg av enternalblue til å spre en dataorm til alle maskinene i det samme nettverket. Dette kan medføre til distraksjoner og sabotasje i et system eller sletting og modifisering av filer på maskinen.

Sårbarheten ble brukt blant annet i ramsonware angrepene WannaCry og NotPetya (SentinelOne, 2019). WannaCry var et ramsonware angrep som spredde seg til Windows maskinene og fungerte ved krypterte maskinen og krevde betaling med bitcoin fra brukere for å dekryptere filene sine.

WannaCry spredde seg til store organisasjoner, sykehus og skoler (MalwareBytes , 2022). Dette medførte til at enkelte selskaper mistet kunder som risikerte dem for konkurs. Skoler som ble rammet av dette angrepet var i fare for å oppleve nedtur i skolesystemet eller miste konfidensiell data, som påvirket blant annet utdanningen. Sykehus ble også i tillegg infisert som gjorde at de ikke kunne utføre arbeidsoperasjonene eller pasientene var ikke i stand til å bestille en konsultasjon hos legene ettersom systemet var kompromittert.

Den benyttet seg av Enternalblue som spredningsvektor for å spre seg til maskinene i nettverket. Det var kun maskinene som ikke var patchet var utsatt for angrepet. Avast påstår at angrepet infiserte den mer en 230 000 maskiner i 150 land i løpet av en dag (Avast , 2022

). NotPetya var også et angrep som benyttet seg av Enternalblue for å spre seg. Dette var også en ramsonware som spredde seg til Windows maskiner. NotPetya var en variant av Petya angrepet som brøt ut i 2017 og var et angrep som var ment for Ukraina (Shepherd, 2021). Dersom maskinen ble infisert, var det ingen måte man kunne gjenopprette filene på. Dette medførte til at alt av data og filer gikk tapt.

Cybertrusler er fremdeles et økende problem i dag og dette rammer i all hovedsak myndigheter og store bedrifter. Motivasjonen for slike angrep er i all hovedsak penger og formålet med slike angrep er å sabotere eller forstyrre et system. Ifølge nettsiden Washingtonpost (sett inn kilde) spredde NotPetya seg til land som Danmark, India og Storbritannia. Dette er et bevis på at et cyberangrep kan ikke bare påvirke organisasjoner i et land, men også påvirke organisasjoner i andre land. Dette kan være truende for organisasjoner, dersom en cybertrussel inntar i systemet. NotPetya er et eksempel på trusler som ikke bare påvirker verden fysisk, men dette kan gi en påvirkning for organisasjoner som benytter seg av digitale systemer.

Stadig flere og flere bedrifter benytter seg av digitale løsninger. Digitalisering har blitt en såpass viktig del ikke bare for mennesker, men også bedrifter. Dette har gitt bedriftene mange fordeler som å lagre data i systemene sine og dette har bidratt bedriften med økt produktivitet og effektivitet. Digitalisering har bidratt å gi ansatte en enklere arbeidshverdag. I tillegg har digitalisering hjulpet bedriftene med å etablere et bedre forhold til kundene sine som tiltrekker kunder til å kjøpe produkter. Digitalisering kan bidra bedriftene med å vokse og gi bedrifter en høyere posisjon på markedet.

Siden digitalisering er en viktig og dominerende faktor for de fleste bedriftene og organisasjoner, har dette gitt økt risiko for at de utsettes for cybertrusler. Trussel landskapet fortsetter å vokse, og angripere utvikler nye skadevare for å kunne få tilgang til bedriftssystemene. Etter hvert vil jeg frykte at det vil komme flere cybertrusler som vil resultere til å gjøre det vanskeligere og vanskeligere for bedrifter å forsvare seg mot cybertrusler etter hvert som de vokser seg til å bli flere og mer alvorlige. Dersom disse truslene ikke fjernes fra systemet kan dette gi langsiktige konsekvenser for bedrifter og organisasjoner og påvirke driften dersom de ikke har etablert god sikkerhet på systemene sine.

I dag er det fremdeles mange utdaterte maskiner som risikerer å bli utsatt for enternalblue sårbarheten. For tilbake i 2019 ble det rapportert at nær 1 million maskiner er infisert av Enternalblue (netsec news , 2019). Dette er et skremmende høyt tall, og jeg antar at årsaken til at Enternalblue infiserte mange maskiner er fordi organisasjonene ikke har implementert godt nok beskyttelse på systemene sine.

For å forhindre slike angrep er det viktig å implementere de riktige sikkerhetstiltakene. Eksempelvis hvis en organisasjon infiseres av WannaCry ramsonware er det viktig å ha backup av dataen og filene for å forhindre at dataen går tapt. Andre tiltak man kan innføre er å benytte seg av antivirus. Antivirus er programmer som er utviklet for å detektere og eliminere skadevare fra å infisere et system dette kan være viktig ettersom det beskytter systemet mot at den kompromitteres. Ved å implementere riktige sikkerhetstiltak kan dette forhindre cyberangrep fra å innta i systemet og dermed minimerer dette risikoen for at organisasjoner blir utsatt for potensielle angrep.

Oppgave 3

Ifølge kaspersky.com er Living Off The Land teknikker og verktøy som allerede eksisterer i systemet som angriper utnytter for å utføre ondsinnede handlinger på offerets maskin (Encyclopedia kaspersky, 2022). Med andre ord, betyr dette at angriperen ikke behøver å laste ned skadelig program på offerets maskin, og heller benytter seg av verktøyene i maskinen for å utføre handlingene sine.

Eksempelvis kan angripere benytte seg av PowerShell for å eskalere privilegier til offerets system, installere bakdører og kjøre skadelig kode på dem som kan gi dem tilgang til konfidensielle data de kan bruke til noe ondsinnet. Andre eksempler på LOL verktøyer er commandshell, ssh og netsh i Windows som en ondsinnet aktør også kan benytte seg av for å få utvidet tilgang til maskinens system.

LOL angrep sprer seg blant annet gjennom internett (ironnet.com, 2022). Angripere benytter seg av phishing teknikker slik som å sende mail til brukere. Dette har til hensikt å manipulere brukere til å gi ifra seg login credentials for å aksessere systemet eller manipulere brukere til å laste ned skadelige koder på maskinene sine utilsiktet. Brukere kan også infiseres ved å besøke usikre websider eller ved å plugge inn USB-er til maskinene sine. Disse kodene utnytter sårbarhetene i systemet som muliggjør det for angripere å få tilgang til maskin og utføre handlinger.

Det er hovedsakelig ikke patchede systemer eller brukere med høye privilegier som er mest utsatt for slike angrep. Årsaken til det er at disse brukerne gjør det enklere for angripere å kompromittere systemet. Disse brukere muliggjør det for angripere til å få fullt tilgang til systemet. Dette vil medføre til at angriperen kan slette og modifisere innhold eller utløse kode som forstyrrer maskinen utilsiktet.

Living Off The Land øker stadig i popularitet blant angripere. Ifølge trussel rapporten utgitt av CrowdStrike, økte Living Off The Land med ca. 40 prosent i 2021 (The CrowStrike Global Threat Report 2022.pdf, 2022). Dette betyr at nesten halvparten parten av angrepene ble utført ved bruk av lokale verktøy på systemet slik som psxes.exe og wmic.exe. Årsaken til det, er at disse teknikkene muliggjør det for angripere å utføre vellykkede angrep mot systemet uten å bli oppdaget. På denne måten er de i stand til å gjøre hva de vil i systemet, som er en fordel for dem når de utfører ønskede handlinger for å kompromittere et system.

Siden angripere opptrer som administrator brukere på systemet, utfører de disse angrepene på de troverdige verktøyene eller programmene på maskinen for å unngå deteksjon. Dette gjør det hardere for blant annet antivirus og SOC å detektere. Slike angrep kan gi angripere et større spillerom og dette kan dermed sette systemet i fare. Hvis man blir utsatt for et slikt angrep vil de ikke bare påvirke enkelte brukere, det kan også spre seg til andre brukere. Eksempelvis hvis et system blir infisert av et virus eller en orm, kan dette infisere de andre maskinene som er koblet til det samme nettverk. Dette kan gi store konsekvenser ikke bare for brukere, men også for store selskaper, institutter og organisasjoner.

Living Off The Land kan være spesielt viktig for dem som utfører red-team øvelser. Red team er en gruppe med sikkerhetseksperter og har som oppdrag å utføre angrep mot virksomhetens system for å finne eventuelle sårbarheter i systemet (Techtarget , 2021). Det gjør de ved å benytte seg av de samme teknikkene en hacker benytter for å få uautorisert

tilgang til et system. LOL teknikker som red teamet benytter seg av kan videre brukes til å teste systemet for sårbarheter og dermed brukes til styrke virksomhetenes system mot LOL angrep. Dette kan de gjøre ved å implementere sikkerhetsprotokoller slik som autentisering og patching, dette er et av sikkerhetstiltak som kan gi økt forsvar og vil kunne bidra med å minske risikoen for at systemet utsettes for LOL angrep.

GitHub har en liste over kjente LOL teknikker og metoder som angripere benytter seg av (lolbas-project, u.d.). Siden en red team har som formål å utføre et simulert angrep mot systemet uten å bli detektert, kan disse teknikkene være nyttig i red team oppdrag.

Csc.exe er et pålitelig verktøy i Windows maskiner og det kan brukes av et red team seg av csc.exe for å bygge ondsinnede koder eller skadelige programmer som kan kjøres på systemet uten at det blir oppdaget. Andre teknikker red teams kan benytte seg av er verktøy slik som certutil.exe. Dette kan brukes om for å laste opp ondsinnede koder til offerets system eller utføre andre operasjoner slik som kopiere filer fra offerets maskin som kan medføre til stjeling av sensitiv informasjon.

PowerShell er også et nyttig verktøy for å utføre red team oppdrag. Som nevnt tidligere benytter angripere seg av for å finne konfidensielle data eller kjøre skadelige koder på offerets maskin. For et red team er det viktig å grave seg inn i et system på leting etter konfidensiell data og andre sårbarheter.

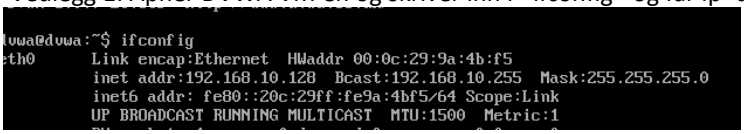
Red team benytter seg av slike teknikker for å misbruke informasjonen de kan finne i systemet. De kan i tillegg bruke dette til å kjøre skadelig kode eller gjemme nyttelast på offerets maskin uten å bli detektert av sikkerhetskomponentene. PowerShell er et eksempel på verktøy som kan bidra red team med å utføre et vellykket red team oppdrag.

Dette var noen få eksempler på LOL teknikker som en red team kan benytte seg av for å utføre en red team operasjon. Teknikker som en red team prioriterer mest er de populære teknikkene angripere bruker for å kompromittere offerets system.

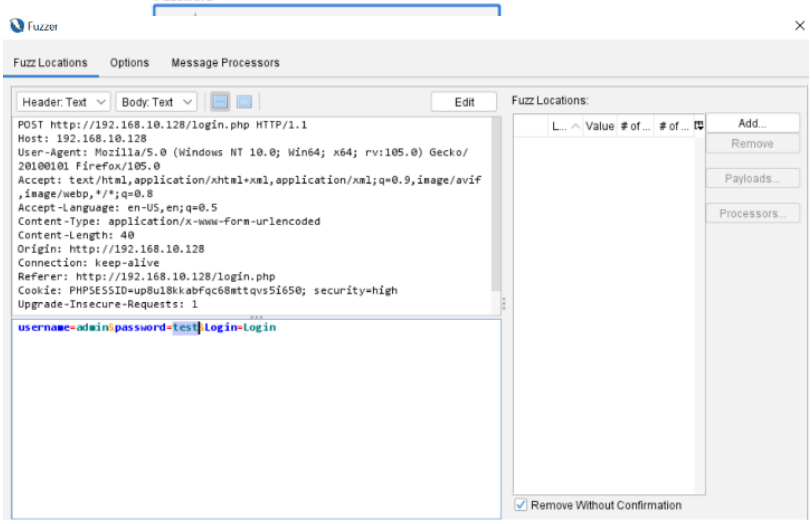
Praktisk del

Oppgave 1

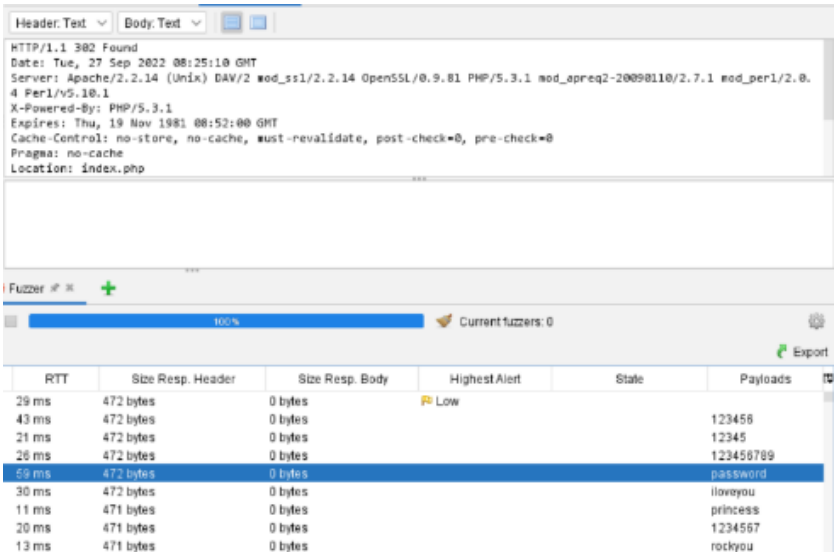
Vedlegg 1: Åpner DVWA VM en og skriver inn i «ifconfig» og får ip- adressen: 192.168.10.128



Vedlegg 2: Åpner deretter en nettleser og får opp en login side.



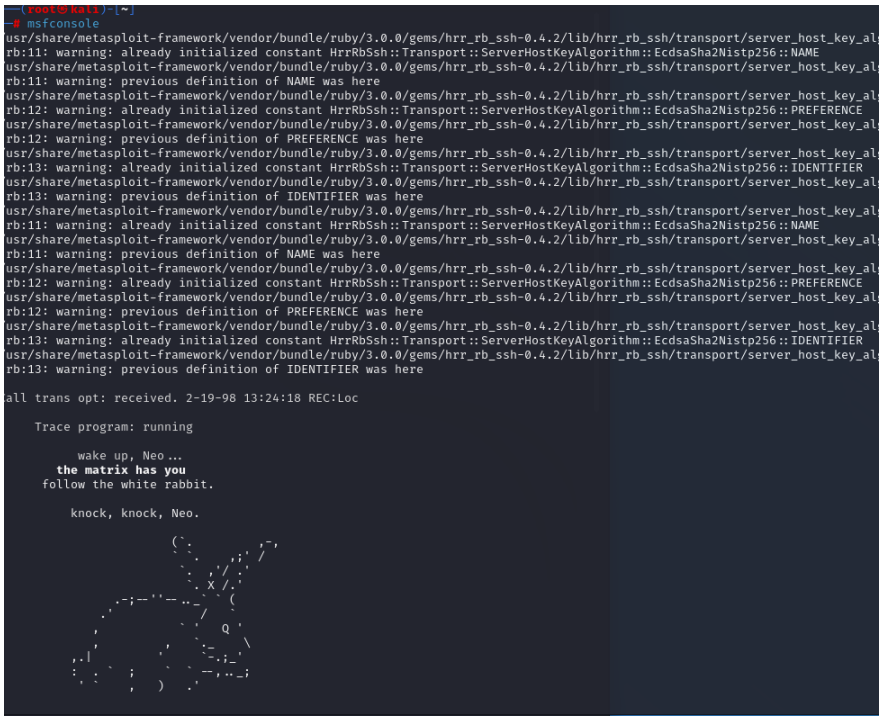
Vedlegg 3: Går tilbake i zap starter active scan og høyre klikker på POST forespørselen og kjører fuzzer. Deretter markerer jeg passordet og legger til passordfilen fra kali inn i «Add»

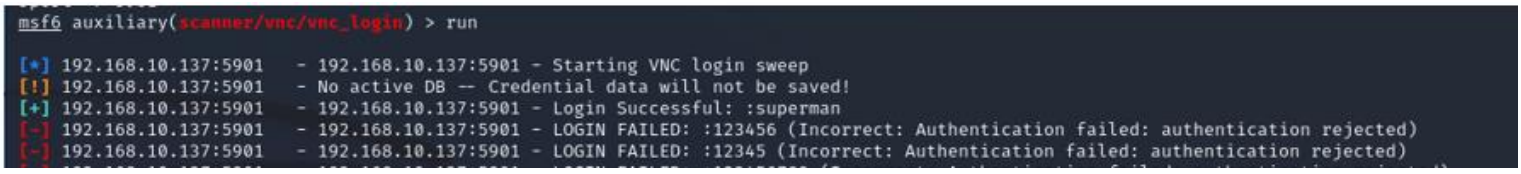


Vedlegg 4: «Password» er det eneste passordet som skiller seg fra andre siden den er den eneste som har location satt til index.php. Så passordet til adminbruker er «password»

Oppgave 2:

DEL A:

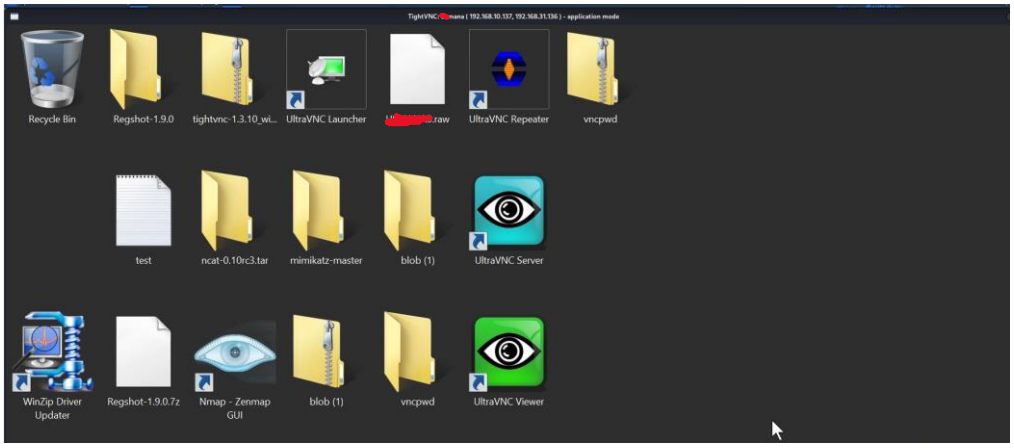




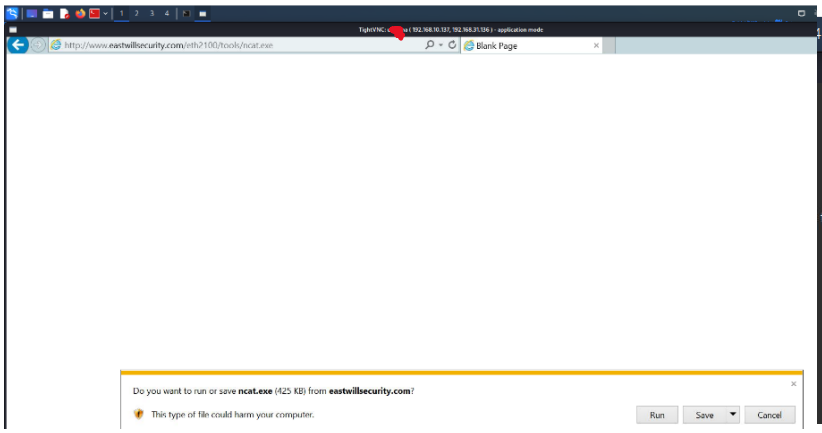
I denne oppgaven setter jeg RHOSTS IP til Windows Serveren=192.168.10.137 og RPORT til 5901, og benytter meg av rockyou5.txt passord-filen. Og finner passordet til VNC serveren «superman».

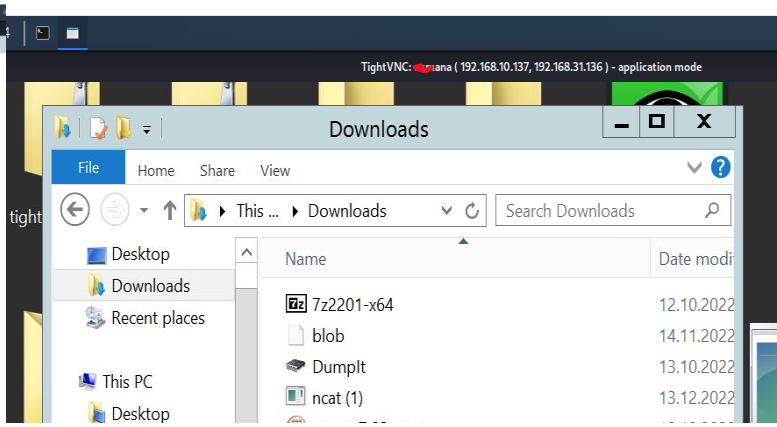
DEL B: Bruker passordet jeg fant i forrige oppgave for å koble meg til serveren. Og kobler meg til windows ip=192.168.10.137 og port 5901 porten.

```
└─# xtightvncviewer 192.168.10.137:5901
Connected to RFB server, using protocol version 3.8
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "[redacted]ana ( 192.168.10.137, 192.168.31.136 ) - application mode"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

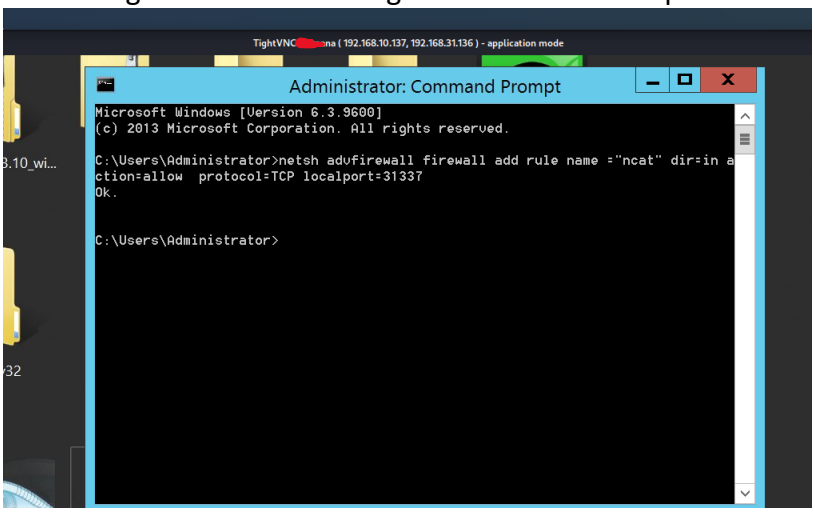


DEL C: Skriver www.eastwillsecurity.com/eth2100/tools/ncat.exe i nettleser og laster ned ncat-filen på serveren.

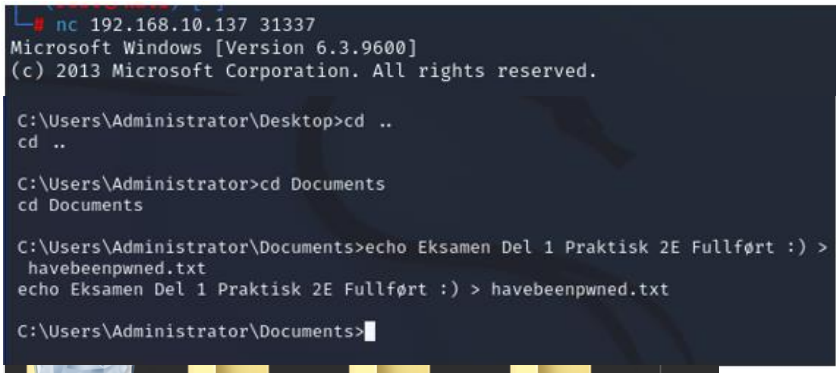


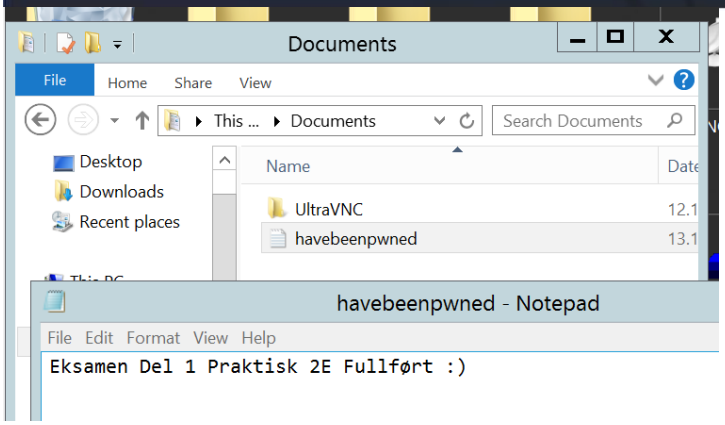


DEL D: Lager netsh firewall regelen i commandline på serveren.



DEL E: Bruker nc i kali og kobler meg til Windows serveren med portnummeret fra forrige oppgave.

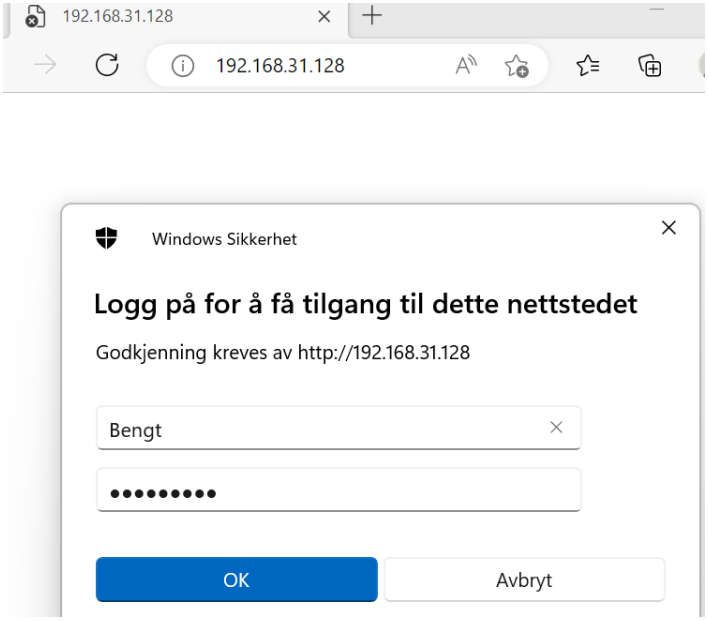




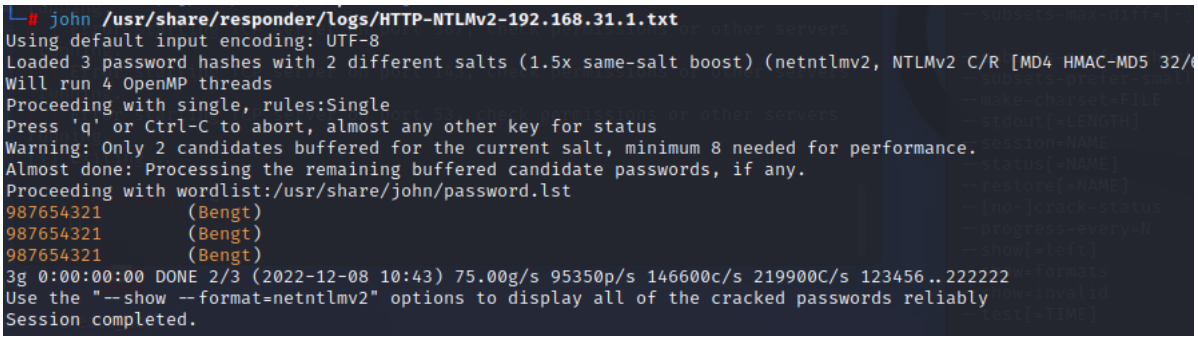
Ser at havebeenpwned.txt filen er opprettet på riktig plassering på serveren.

Oppgave 3:

Vedlegg 1: «Starter responder i kali med kommandoen «responder -I eth0»

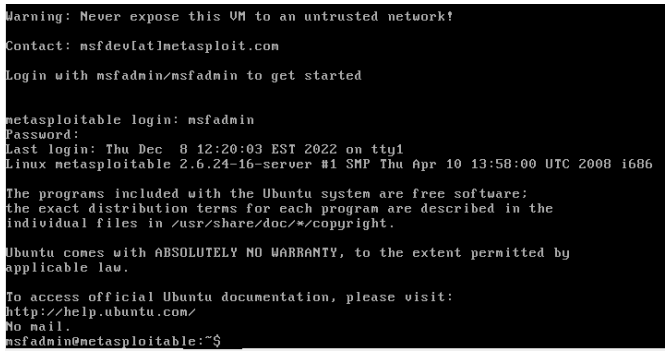


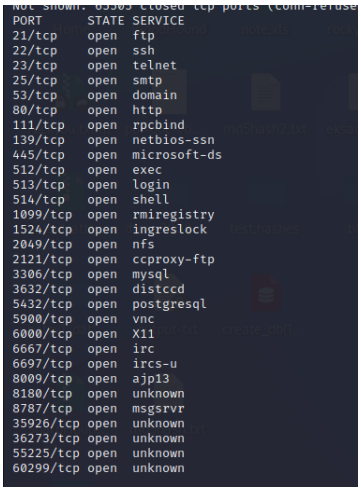
Vedlegg 2: Skriver inn «brukernavnet: Bengt og passordet :987654321 inn i nettleseren»



Vedlegg 3: Knekker passordet med John The Ripper i kali med kommandoen «john /usr/share/responder/logs/http-NTLMv2-192.168.31.1.txt» og får både brukernavnet og passordet i klartekst.

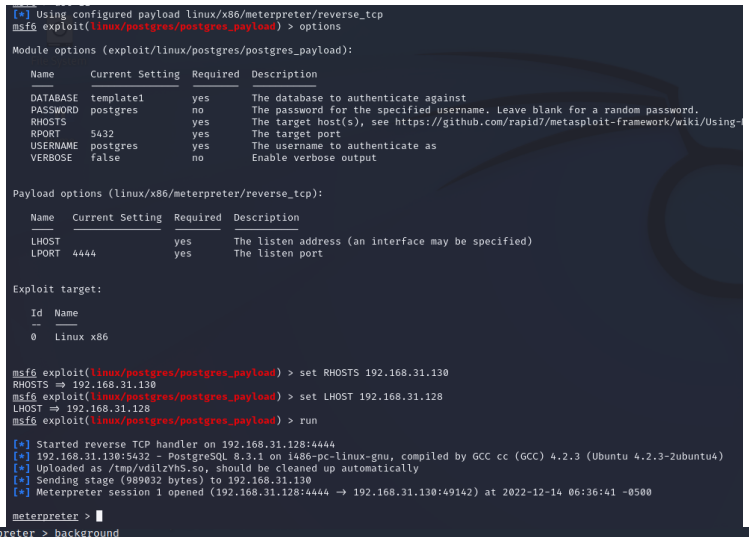
Oppgave 4



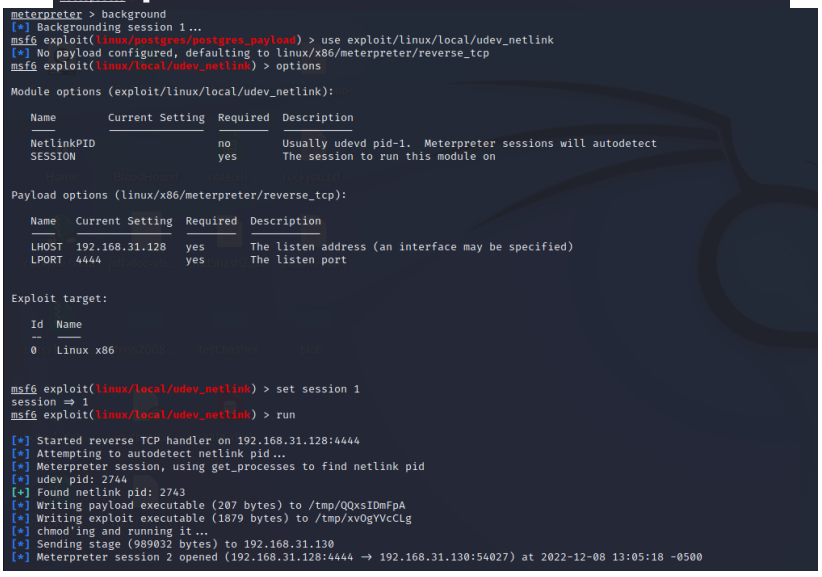


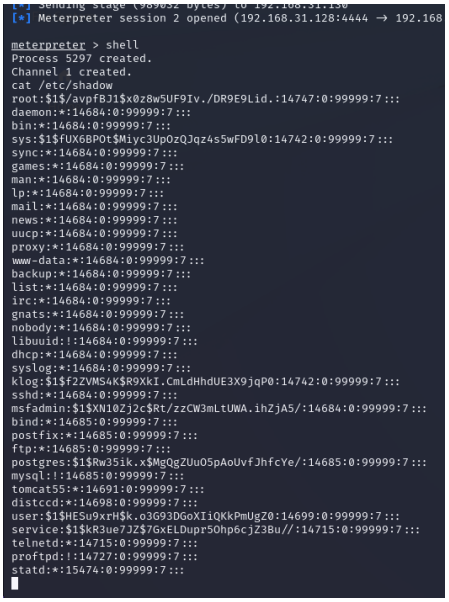
«Vedlegg 1: Åpner Metasploitable VM en og logger inn med brukernavn og passord :msfadmin»

«Vedlegg 2 : kjører kommandoen « nmap -p 1-65535 -T4 -v 192.168.31.130» mot metasploit og finner at postgresql er eksponert på port 5432»



«Vedlegg 3: Åpner en ny terminal skriver msfconsole , søker etter postgres og bruker postgres_payload. Deretter setter jeg RHOST = 192.168.31.130 som er IP adressen til Metasploit og setter Linux IP-Adressen in i LHOST =192.162.31.128. Deretter kjører exploitet»





«Vedlegg 4: Kjører exploit/linux/local/udev_netlink i bakgrunnen som er et «privilege escalation» exploit , deretter setter jeg inn session =1 og kjører exploitet. Deretter kjører jeg

kommandoen shell i meterpreter og skriver kommandoen «cat /etc/shadow» for å printe ut filen direkte inn i terminalen.»

Bibliografi

Avast . (2022 , infecting over 230,000 Windows PCs across 150 countries in a single day). Hentet fra WannaCry : https://www.avast.com/c-wannacry

Bulao, J. (2022, 64% of companies worldwide have experienced at least one form of a cyber attack.). *Techjury.net*. Hentet fra How Many Cyber Attacks Happen per Day in 2022?: https://techjury.net/blog/how-many-cyber-attacks-per-day/#:~:text=64%25%20of%20companies%20worldwide%20have,around%2094%25%20of%20all%20malware

Encyclopedia kaspersky. (2022). Hentet fra A Living off the Land (LotL) attack describes a cyberattack in which intruders use legitimate software and functions available in the system.: https://encyclopedia.kaspersky.com/glossary/lotl-living-off-the-land/

Henriquez, M. (2021). *Security Magazine*. Hentet fra The global average cost of a data breach increased 2.6% from $4.24 million in 2021 to $4.35 million in 2022: https://www.securitymagazine.com/articles/98486-435-million-the-average-cost-of-a-data-breach

hypr.com. (2022). Hentet fra EnternalBlue: https://www.hypr.com/security-encyclopedia/eternalblue

ironnet.com. (2022). Hentet fra What are living off the land attacks: https://www.ironnet.com/blog/what-are-living-off-the-land-attacks

lolbas-project. (u.d.). Hentet fra https://lolbas-project.github.io/

MalwareBytes . (2022, hospitals to schools, banks, and charities, it seems like no organization is immune to ransomware attacks). Hentet fra WannaCry: https://www.malwarebytes.com/wannacry

netsec news . (2019, 05). Hentet fra more than 1million machines still vulnerable to eternalblue exploit: https://www.netsec.news/more-than-1-million-machines-still-vulnerable-to-eternalblue-exploit/

SentinelOne. (2019). Hentet fra (EternalBlue Exploit: What It Is And How It Works) : Deployed in the WannaCry and NotPetya attacks: https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/

Shepherd, A. (2021). *Itpro*. Hentet fra What is NotPetya?: https://www.itpro.co.uk/malware/34381/what-is-notpetya

Techtarget . (2021). Hentet fra A red team is often a group of internal IT employees used to simulate the actions of those who are malicious or adversarial. : https://www.techtarget.com/whatis/definition/red-teaming

The CrowStrike Global Threat Report 2022.pdf. (2022). I *OverWatch Observe a near 45% increase in the number of such campaigns* (ss. 8-9). Texas , USA .

vaultes.com. (2022). Hentet fra Pen tests serve as a way to examine whether an organization's security policies are genuinely effective. : https://www.vaultes.com/why-penetration-testing-is-important/#:~:text=The%20main%20reason%20penetration%20tests,security%20policies%20are%20genuinely%20effective.

Wikipedia.com . (2022). Hentet fra The NSA did not alert Microsoft about the vulnerabilities: https://en.wikipedia.org/wiki/EternalBlue

Østby, B. (2022). ETH2100_U37_Forelesning_03_YourInternetsBelongToUs_Part1.pdf. I *Kali Linux* (ss. 61-62). Oslo , Norge .