Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2021

Nuutti Jokinen

ONLINE-POHJAISET ALUSTAT TIETOTURVATESTAUKSEN OPISKELUSSA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2021 | 28 sivua

Nuutti Jokinen

ONLINE-POHJAISET ALUSTAT TIETOTURVATESTAUKSEN OPISKELUSSA

Opinnäytetyön aiheena oli tutkia erilaisten tietoturvatestausalustojen käyttöä itseopiskeluun tietoturva-alalla. Lisäksi haluttiin tutkia alustojen sisältöä sekä verrata niiden soveltuvuutta aloittelevan käyttäjän näkökulmasta. Tarkoituksena oli löytää mahdollisimman monipuolinen sekä aloittelijaystävällinen alusta, joka tarjoaa harjoituksia sekä opiskelumateriaalia tietoturva-alan itsenäiseen opiskeluun.

Tutkimuksessa verrattiin online-pohjaisia alustoja tietoturvatestauksen opiskelussa. Opinnäytteen aikana tutustuttiin Internetissä oleviin tietoturvatestausalustoihin, joista tarkempaan vertailuun otettiin HackTheBox- sekä TryHackMe-alustat. Molempien alustojen opetusmateriaalia tutkittiin syksyllä 2020, jolloin ympäristöistä suoritettiin alustojen tarjoamia harjoituksia. Molempien alustojen aloittelijatason harjoituksia läpikäytiin ja niiden sisältöä vertailtiin toisiinsa sekä tutkittiin harjoituksien sisältämiä ohjeita. Lisäksi tutkittiin alustojen kokonaistarjontaa sekä ilmaiskäyttäjien että lisäpalveluista maksavien käyttäjien näkökulmasta.

Alustoista tehtiin esimerkkiharjoitukset, joiden työmäärää ja haastavuutta verrattiin. Lisäksi alustojen sisältöä verrattiin ja vertailun kriteereinä käytettiin ympäristöjen aloittelijaystävällisyyttä, näiden tarjonnan määrää sekä laatua. Lopputulemana koottiin alustojen vahvuudet sekä heikkoudet omiksi listoiksi ja käytiin läpi alustojen soveltuvuutta tietoturvatestauksen itseopiskeluun. Tutkimustuloksista voidaan päätellä TryHackMe -alustan soveltuvan aloittelijatasoiseen itseopiskeluun vahvemmaksi alustaksi tämän tarjoaman opastuksen ja tutoriaalien perusteella. Tutkimusta voidaan jatkaa ottamalla erilaisia vertailunäkökulmia sekä tutustumalla isompaan määrään itseopiskelualustoja.

ASIASANAT:

hakkerointi, opiskelu, tietoturva

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2021 | 28 pages

Nuutti Jokinen

ONLINE-BASED PENETRATION TESTING PLATFORMS IN INFORMATION SECURITY STUDIES

The purpose of this thesis was to compare online-based learning platforms for information security. The research part of the thesis was dedicated to introduce different online platforms for penetration testing studies. HackTheBox- and TryHackMe-platforms were main platforms that were compared during the thesis.

Fall of 2020 was spent to research the chosen platforms by performing their exercises. Beginner-level exercises were completed with their write-up guides from both platforms. In addition the selection of exercises and learning material were studied and compared from both free users and premium users perspective.

After research portion of thesis, example exercises were performed from both platforms from which comparison and conclusions could be made regarding the workload and difficulty of the exercise. After the exercises the selection of exercise on the platforms were compared. The comparison perspective were new user friendliness and selection towards new users.

KEYWORDS:

hacking, information security, studying

SISÄLTÖ

KUVAT

KÄYTETYT LYHENTEET

CTF	Tehtävätyyppi jossa tarkoituksena on murtaa harjoituksen palvelin, josta viedään haluttua asia eli lippu, joka merkkaa harjoituksen suorituksen onnistumisen (Capture The Flag).
VPN	Turvallinen kommunkaatiomuoto laitteiden välillä Internetissä (Virtual Private Network).

1 JOHDANTO

Internet sekä sen käyttö ovat kasvaneet 2000-luvun alusta tähän päivään massiivisesti ja käyttäjämäärä sen mukana. Yksityishenkilöt sekä organisaatiot panostavat näkyvyyteensä internetissä, ja tähän liittyy usein myös oman tietoturvan ylläpito, joka joskus saatetaan laiminlyödä. Tällainen laiminlyönti voi johtaa tietomurtoihin sekä -vuotoihin, joista kärsivät organisaatiot sekä yksityishenkilöt.

Tietoturvaloukkausten määrä Suomessa on ollut erityisesti kasvussa vuonna 2020 kyberturvallisuuskeskus Tarficomin kybersäätiedotusten mukaan. Traficom ylläpitää kuukausittaisia tietoturvaraportteja keräämällä informaatiota Suomessa sijaitsevien yritysten hyväksi ja avustaa tarvittaessa konsultoimalla sekä testaamalla yrityksiä tietoturvan suhteen (Kybersää).

Yritykset voivat pitää organisaatioissaan tietoturvakoulutusta, johon usein kuuluu käyttäjän tietoturva sekä esimerkiksi käyttäjien salasanapolitiikkaan yleiset käyttöohjeet sekä toimintaohjeet tietoturvaloukkauksen tapahtuessa. Tämän lisäksi yritykset voivat hankkia apua muualta, ja vahvistavat yrityksen tietoturvapolitiikkaa esimerkiksi testaamalla yrityksen tietoturvaa.

Kun testataan yrityksen tietoturvaa, lähestytään usein tilannetta haitallisen tekijän näkökulmasta sekä pyritään käyttämään samankaltaisia työkaluja, joita haitalliset tekijät käyttävät. Jotta tällaisia testauksia on mahdollista suorittaa, tarvitaan osaavia ihmisiä, jotka ymmärtävät, millä tavoin haitalliset tekijät toimivat. Siksi on tärkeää oppia, millä tavoin tietoturvaloukkauksia voidaan tehdä hallitussa ja suljetussa ympäristössä, jossa voidaan erilaisten harjoitusten avulla oppia työkalujen käyttöä aiheuttamatta muille haittaa.

Tämän työn päätarkoituksena on verrata online-pohjaisia tietoturvatestaukseen perustuvaa alustoja sekä tutkia tarkemmin HackTheBox- ja TryHackMe-alustoja sekä verrata näiden ominaisuuksia, vahvuuksia sekä heikkouksia.

Opinnäytetyötä alettiin työstämään syksyllä 2020 tutkimustyönä, jolloin tutustuttiin molempien alustojen eri harjoituksiin sekä tutkittiin ilmaisia vaihtoehtoja alustojen harjoitustarjonnasta. Tarjonnan määrä sekä laatu käydään läpi tutkimuksen alustojen esittelyosuudessa. Lisäksi verrattiin molempien ympäristöjen maksullisia versioita ja niiden tarjonnan laajuutta toisiinsa.

Teoriaosuudessa esitellään online-pohjaisia tietoturvatestausalustoja. Lisäksi suoritettiin vertailua, jossa kriteereinä käytetään alustojen aloittelijaystävällisyyttä, niiden tarjonnan määrää sekä laatua.

Työn käytännön osuudessa suoritettiin molempien ympäristöjen aloittelijatason harjoitukset. Näiden harjoitusten työmäärää sekä vaikeusastetta vertaillaan keskenään.

2 TIETOTURVATESTAUS

Tietoturvatestauksessa simuloidaan oikean maailman kyberhyökkäystä kohteisiin, jotka halutaan testata mahdollisten heikkouksien varalta. Tietoturvatestausta suoritetaan yleisesti www-palvelimiin sekä yritysten verkkoihin, jotka ovat näkyvillä ulkoverkkoon, josta haitallinen tekijä kykenee suorittamaan kyberhyökkäyksen. Tietoturvatestauksesta on useita erilaisia vaihtoehtoja testausmetodeista riippuen. Tällaisia metodeja ovat esimerkiksi ulkoinen sekä sisäinen testaus, sokkotestaus ja kaksoissokkotestaus (Imperva, n.d.).

Ulkoinen testaus

Ulkoisessa testauksessa kohteena on ulkoverkkoon näkyvä omaisuus, johon voidaan suorittaa kohdennettuja hyökkäyksiä ulkoverkkoa pitkin. Tällaisia kohteita ovat yleisesti web-applikaatiot, verkkosivut sekä sähköposti- ja web-palvelimet. Testauksen tarkoituksena on pyrkiä saamaan pääsy sisään järjestelmään sekä viemään ulos arvokasta informaatiota sekä dataa (Imperva, n.d.).

Sisäinen testaus

Sisäisessä testauksessa testataan verkon sisäpuolella sijaitsevaa omaisuutta, joka on suojattu ulkoverkolta usein palomuurien avulla. Tällä testauksella voidaan simuloida tilannetta, jossa käyttäjän tiedot ovat vuotaneet haitalliselle toimijalle (Imperva, n.d.).

Sokkotestaus

Sokkotestauksen tarkoituksena on testata kohdetta niin, ettei testaajalle anneta muuta informaatiota, kuin esimerkiksi yrityksen nimi. Tällä tavoin voidaan selvittää, mitä tietoa yrityksestä saadaan skannaamalla ja tiedustelulla (Imperva, n.d.).

Tuplasokkotestaus

Sokkotestauspohjan lisäksi tuplasokkotestauksessa ei anneta yritykselle itsessään informaatiota testauksesta. Kyberhyökkäykset tulevat usein yllättäen eikä niiden ajankohtaa kyetä todentamaan etukäteen tarkasti, joten tällä tavoin voidaan testata yleistä valmiutta ja toimiin vastaamista oikeassa skenaariossa (Imperva, n.d.).

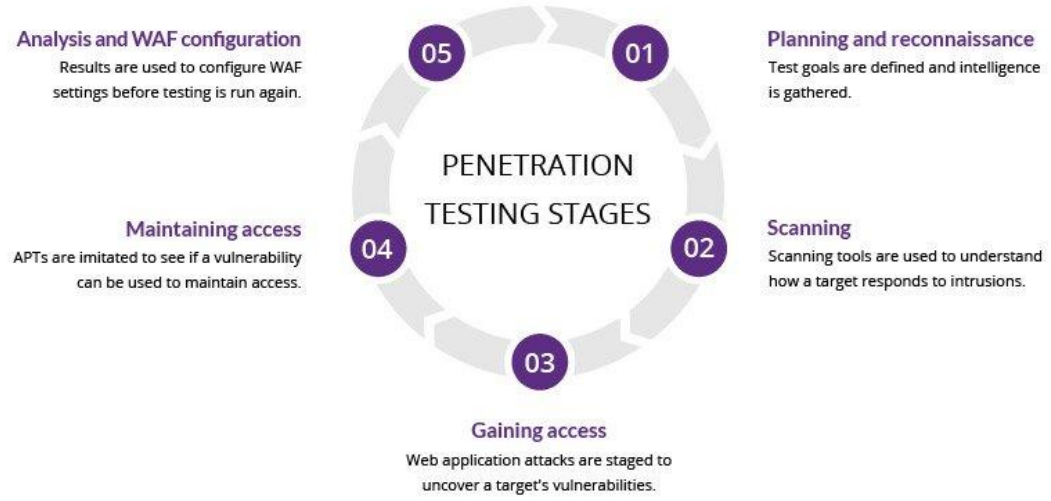
Yritysten tietoturvatestauksessa pyritään todentamaan ympäristöjen tietoturvan todentamista tunnettujen haavoittuvuuksien sekä haittojen osalta. Mahdollisia haavoittuvuuksia

ovat esimerkiksi puutteelliset päivitykset, vahingossa suoritetu virheelliset asetukset ja säädöt sekä heikot salasanapolitiikat sekä oikeussuhteiden määrän liiallisuus (Imperva, n.d.).

Testauksen kohteena voivat olla mm. yrityksen tietojärjestelmät, työasemat, lähiverkko ja tämän aktiivilaitteet, kamera- ja turvajärjestelmät sekä palvelimet, kuten www- ja sähköpostipalvelimet sekä palomuurit. Testauksen alkusuunnittelussa sovitaan yrityksen kanssa tietoturvatestauksen tavoitteista sekä päämääristä, joista raportoidaan yritykselle testauksen päätyttyä.

Tietoturvatestauksen vaiheet

Tietoturvatestaus sisältää viisi eri työn vaiheita, jotka ovat suunnittelu- ja tiedustelu, skannaus, pääsyn saaminen, pääsyn ylläpito sekä analysointi- ja raportointi (Imperva, n.d). (Kuva 1.).



Kuva 1. Tietoturvatestauksen eri vaiheet (Imperva, n.d.)

Suunnittelu- ja tiedustelu

Suunnittelu- ja tiedusteluvaiheessa määritellään ja rajataan yhdessä kohdeorganisaation kanssa testauksen laajuus, tavoitteet, testausalueet sekä metodologiat. Samalla suoritetaan alustavaa tiedonkeruuta kohteista.

Skannaus

Skannausvaiheessa suoritetaan kohdepalvelimien analysointia joko manuaalisesti sekä erilaisten skannaustyökalujen kuten Nmap-porttiskannerin avulla. Näin luodaan tulevia vaiheta varten kuva asiakasorganisaation ulkoverkosta sekä mahdollisista aukoista, joita mahdollinen haitallinen toimija voisi hyödyntää varsinaisessa hyökkäyksessä.

Pääsyn saaminen

Pääsyn saamiseksi suoritetaan erilaisia hyökkäysmetodeja käyttämällä skannausvaiheessa ilmenneitä mahdollisia haavoittuvuuksia, joilla pyritään saamaan kohteisiin jalansija.

Pääsyn ylläpito

Pääsyn ylläpitovaiheessa pyritään saamaan syvempi pääsy kohteisiin esimerkiksi korkeamman tason käyttäjällä, jolla on enemmän hallintaoikeuksia kohdeympäristössä. Lisäksi pyritään mahdollistamaan myöhempi huomaamaton pääsy mahdollista haitallista käyttöä varten.

Analysointi ja raportointi

Viimeisessä vaiheessa kerätään saatu data sekä tieto raportoitavaksi yritykselle, jossa läpikäydään testauksessa esille tulleet asiat, joita parantamalla voidaan parantaa yrityksen tietoturvapolitiikkaa sekä verkkoa. Lisäksi usein sovitaan jatkotarkastus, jossa tarkastetaan edellisen testauksen johdosta tehtyjen toimenpiteiden toimivuus.

3 OPETUSALUSTAT

Tietoturvatestaukseen on luotu erilaisia online-pohjaisia alustoja, joissa käyttäjät voivat suorittaa erilaisia harjoituksia sekä haasteita. Nämä alustat tarjoavat aiheen opiskeluun runsaasti eritasoisia harjoitustehtäviä, opetusmoduuleita sekä ympäristöjä, joihin kuka tahansa voi liittyä helposti ilman suurta panostusta.

Osa alustoista on pyrkinyt tarjoamaan myös suurempiin harjoituskokonaisuuksiin heidän omia työkaluja, jotka tarjoavat yleiset tietoturvatestaukseen vaadittavat ohjelmistot hyökkäyskoneella, jota ylläpidetään alustojen virtuaalipalvelimilla. Näihin hyökkäyskoneisiin saadaan yhteys käyttäjän omasta laitteesta, jolloin konetta voidaan ohjata normaalin tietokoneen tavoin etäyhteyden avulla.

Osa näistä on ilmaisia, osa taas on tilauspohjaisia, joissa maksetaan kuukausi- tai vuosimaksu alustan käytöstä. Maksullisten alustojen tarjonta on laajempaa verrattuna ilmaisalustoihin sekä ne ovat suunnattu enemmän alan osaajille. Esimerkiksi Virtual Hacking Labs on maksullinen tietoturvatestausalusta, joka tarjoaa eritasoisia harjoitteita, joiden suorittamisesta tarjotaan sertifikaatteja.

Ilmaisalustoja on esimerkiksi Vulnhub, HackTheBox sekä TryHackMe. Vulnhub alustana perustuu harjoitteiden jakeluun, jonne tekijät voivat ladata omat harjoitteensa virtuaalikoneen muodossa. Käyttäjä voi ladata virtuaalikoneen omalle laitteelleen ja ajaa harjoitusta omassa ympäristössään virtuaalisesti.

HackTheBox sekä TryHackMe ovat online-alustoja, joiden tarkoituksena on pitää kaikki testaukseen liittyvä samassa paikassa. Näiden alustojen harjoitukset pyörivät heidän omilla palvelimillaan, joihin otetaan yhteys joko omalta laitteelta VPN-yhteyden avulla, tai harjoituksia voidaan tehdä alustojen tarjoamilla virtuaalikoneilla, josta löytyy testaukseen hyödyllisiä työkaluja. Molemmat alustat tarjoavat ilmaiskäyttäjille runsaasti harjoitusmateriaalia sekä opetusmoduuleita, mutta jatkavat tarjontaa pidemmälle, mikäli käyttäjä sitoutuu maskulliseen tilausmuotoon lisäsisällöstä. Tällöin käyttäjällä on tarjolla enemmän materiaalia sekä hänelle annetaan pääsy vanhempiin harjoituksiin, jotka ovat poistuneet aktiivisesta ylläpidosta.

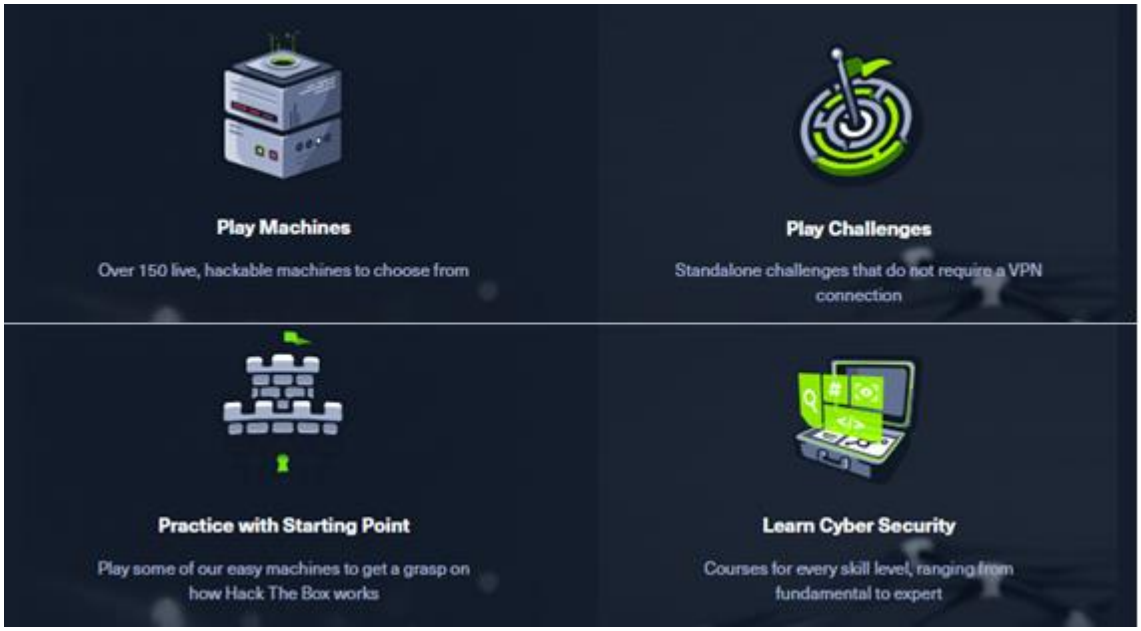
3.1 HackTheBox

HacktheBox on vuonna 2017 perustettu opetusalusta, jonka tarkoituksena on antaa työkalut hakkeroinnin sekä tietoturvantestauksen opiskelulle. Alusta tarjoaa käyttäjälle erilaisia harjoitteita, kuten opiskelumoduuleita eri aiheista sekä labrapalvelimia, joissa voidaan tehdä tietoturvatestausta liittymällä labraverkkoon VPN-avaimien avulla (HackTheBox LinkedIn).

HacktheBox-alustan neljä päämäärää ovat luoda huippuluokan hakkerointisisältöä, tietoturvaopiskelun pelillistäminen, käytännönläheiset testausharjoitukset sekä käyttäjän oman opiskelutahdin määrittäminen. Alustaan tuodaan uutta materiaalia viikoittain vaihdellen vaikeusasteeltaan helpoista harjoituksista haastaviin, oikean maailmaan reflektoiviin labrapalvelinympäristöihin. Opiskelun pelillistämistä luodaan tekemällä pisteytysmekanismi alustaan, jossa pisteitä kerätään suorituksista sekä taitotason kehittämisestä. Käytännönläheiset testausharjoitukset tuovat interaktiivisen puolen tietoturvaopiskeluun, jollaista ei esimerkiksi aiheesta lukemalla välttämättä voida saavuttaa. Oman opiskelutahdin määrittämisellä tarkoitetaan alustan harjoituksien olevan aikaan sitoutumattomia. Käyttäjä voi itse määrittää oman tahtinsa sekä milloin suorittaa harjoitteita (HackTheBox).

Tarjonta

HackTheBox sisältää eri harjoituskategorioita (Kuva 2.), joista suurimmat ovat Machines-harjoitukset sekä CTF-tyyliset Challenges-haasteet. Machines-harjoitukset sisältävät eniten sisältöä, sillä yhteisön jäsenet voivat esittää alustalle omia harjoituksiaan, joita HackTheBox valikoi ja ottaa käyttöönsä tasaisin väliajoin. Yhteisön käyttäjät voivat myös luoda omia Challenges-haasteita, ladata ne HackTheBoxin alustalle, josta muut käyttäjät voivat ratkoa ilman erillisiä vaatimuksia.



Kuva 2. HackTheBox -alustan harjoituskategoriat (HackTheBox).

HackTheBox on myös aloittanut erillisen Academy-alustan, jossa on tarjolla erilaisia opiskelumoduuleita (Kuva 3.). Moduulit vaihtelevat sisällöltään, ja osa on maksullisia.

Kuva 3. Esimerkkitarjontaa HackTheBox Academy -alustasta.

Pääideana Academy-alustalla on tienata cube-pisteitä, joilla voi avata kattavampia moduuleita eri aiheista. Nykyisessä mallissa pisteiden keruu ei ole vielä kehittynyt tuotta-

vaan suuntaan, vaan käyttäjän on ostettava pisteitä maksamalla kuukausittainen jäsenhinta. Jokaisesta täysin suoritetusta moduulista tienaataan noin puolet maksetuista pisteistään takaisin, jolla kannustetaan kokonaisten opetusmoduulien suorittamista loppuun asti.

Aloittelijaystävällisyys

HackTheBox tarjoaa aloitteleville käyttäjille Starting point-alueen, jossa ylläpidetään yksinkertaisia harjoituksia, joita voidaan suorittaa opastetuilla läpikäyntidokumenteilla. Harjoitukset toimivat samalla perjaatteella kuin tavalliset Machines-osion harjoitukset, mutta sisältävät vähemmän työvaiheita sekä kirjoitetut läpikäyntidokumentit. Harjoitusten tarkoitus on saada peruskuva haastavimmista harjoitteista, joita HackTheBox tarjoaa.

Varsinaisten Machines-osuuden harjoituksiin HackTheBox ei suoraan sisällytä mitään läpikäyntidokumentteja, joista saisi opastusta. Näihin voi kuitenkin löytää yhteisön kirjoittamia opasteita. HackTheBox kuitenkin toivoo yhteisön käyttäjiltä, ettei nämä luovuttaisi harjoitusten ratkaisuja, ennen kuin nämä ovat vanhenemassa ja siirtymässä arkistoihin, jolloin niihin pääsee käsiksi vain maksullisen jäsenyyden omaavat käyttäjät.

3.2 TryHackMe

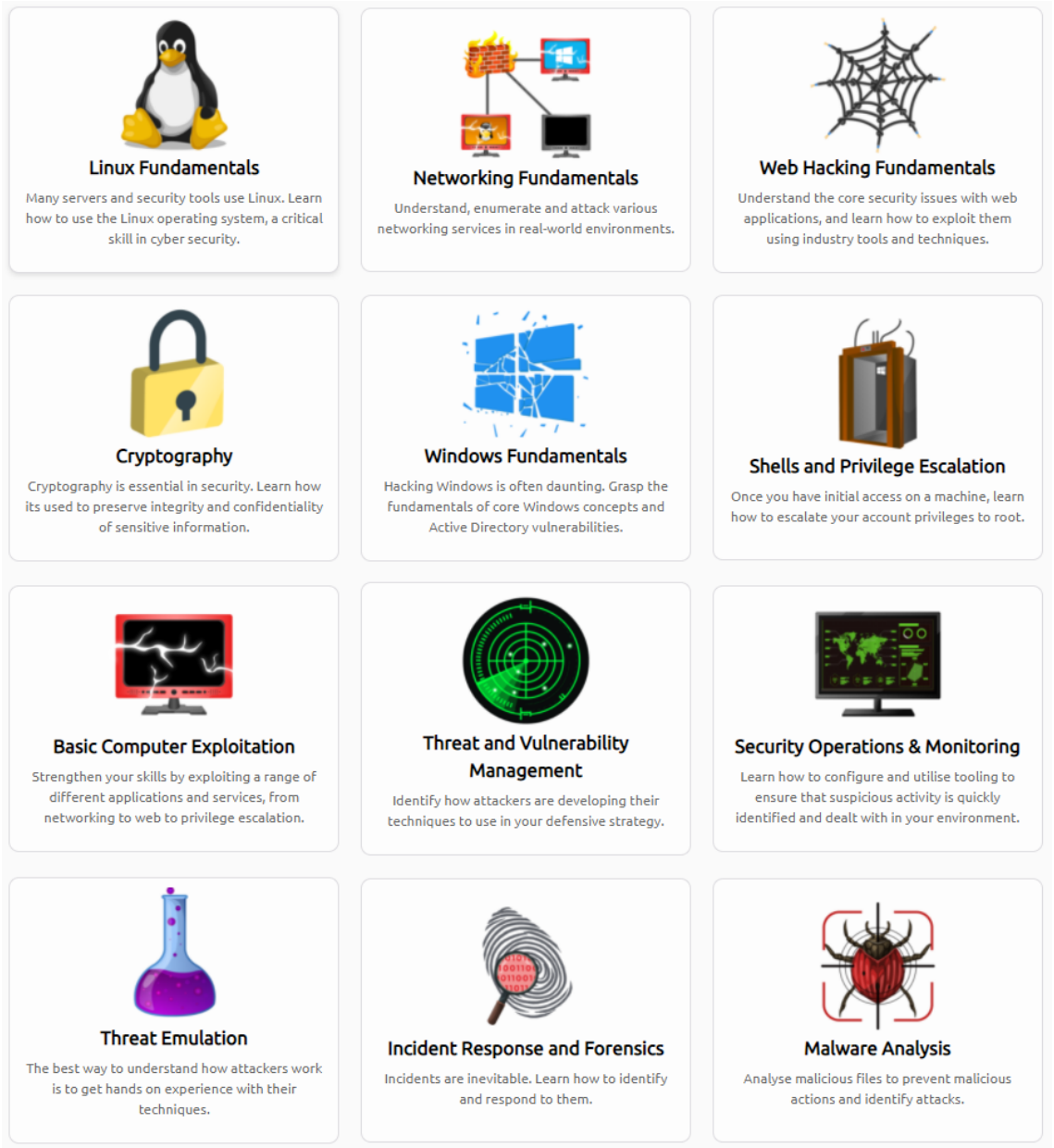
TryHackMe on vuonna 2018 perustettu (TryHackMe) tietoturvatestaukseen erikoistunut opetusalusta. Alusta tarjoaa ympäristöt, joissa voidaan toteuttaa tietoturvaopiskelua opastetusti sekä tarjotaan tenttipohjaisia opetuskokonaisuuksia, joilla varmistetaan että käyttäjä on onnistunut suorituksessaan tarkoitetulla tavalla vastaamalla annettuihin kysymyksiin oikein. Jokaisessa harjoituksessa on listattu joukko siihen liittyviä kysymyksiä, joihin löytyy vastaukset itse harjoituksesta tai siihen tarjotusta opetusmateriaalista.

TryHackMe on HackTheBoxin tavoin pelillistänyt tietoturvaopiskelun, jossa harjoitteita suorittamalla kerätään käyttäjälle pisteitä, joilla pääsee paremmalle sijoitukselle kaikkien nähtävillä olevalla pistetaulukolla. Lisäpisteitä annetaan myös jatkuvan opiskelun ylläpitämisellä palkitsemalla päivittäinen tehtävien tekeminen sekä harjoituskokonaisuuksien kokonaan suorittaminen. Näin varmistetaan käyttäjän aktiivisuus alustalla.

Tarjonta

TryHackMe alustana tarjoaa erityyppisiä harjoituksia, joista käyttäjä kykenee valitsemaan haluamansa helposti valitsemalla harjoituksen (Kuva 3.)., jonka haluaa suorittaa

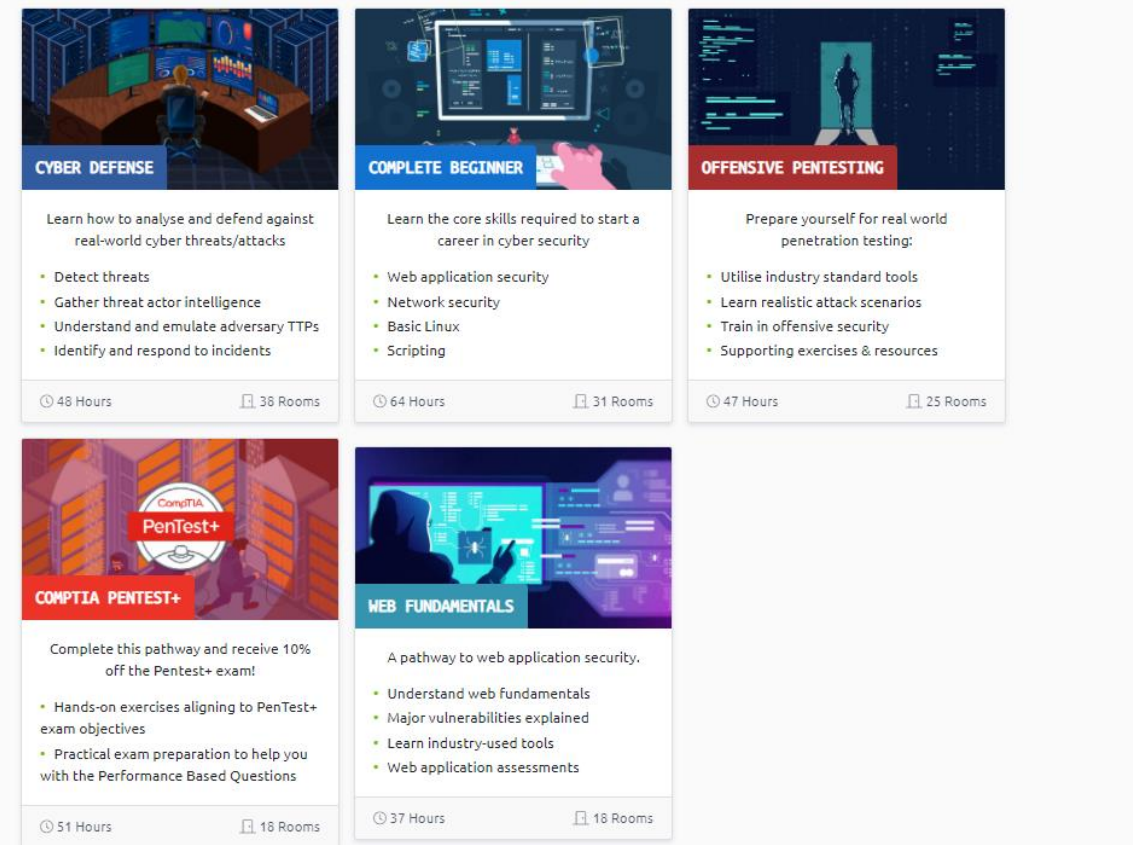
Yksinkertaisimmillaan käyttäjä kykenee suorittamaan ainoastaan yhden harjoituksen haluamastaan mooduulista.



Kuva 4. Esimerkkitarjontaa HackTheBox Academy -alustasta.

Yksittäisten harjoitteiden lisäksi alusta tarjoaa kokoelman erilaisia kurssikokonaisuuksia, joihin sisältyy erilaisten alaan liittyvien työkalujen sekä toimintojen opiskelua (Kuva 4.). Käyttäjä voi halutessaan liittyä kurssikokonaisuuteen ja suorittaa sen sisältämiä osia

omassa mielivaltaisessa järjestyksessä, mikäli käyttäjä katsoo osaavansa tietystä kurssikokonaisuuden osassa käytävät asiat tarpeeksi hyvin.



Kuva 5. TryHackMe -alustan kurssikokonaisuustarjonta.

Aloittelijaystävällisyys

TryHackMe alustalla tarjotaan aloittavalle käyttäjälle eritasoisia harjoituskokonaisuuksia, jotka kasvavat vaikeusasteessa tasaisesti. Jokaisessa harjoituksessa tarjotaan käytännön opastusta esimerkiksi videomateriaalin muodossa, josta voidaan seurata etenemistä sekä ohjaajan kommentaariota harjoituksesta.

TryHackMe-alustan harjoituksista tulee myös selville niiden päämäärät. Jokaisessa harjoituksessa on näkyvillä kysymykset, joihin löytyy vastaus harjoituksen aikana selvitetyistä asioista sekä itse harjoituksesta. Kysymykset sisältävät myös tehtävälista-tyylisiä kohtia, joista on helppo seurata etenemistään.

4 ESIMERKKIHARJOITTEIDEN LÄPIKÄYNTI

Tietoturvatestauksen harjoittelua varten alustat ovat luoneet käytännönläheisiä harjoituksia, joista vertailuun otettiin aloittelijaystävälliset vaihtoehdot, sillä vertailun kohteena tutkimuksessa pidettiin harjoitteiden soveltuvuutta aloittelijatason käyttäjille.

HackTheBox- sekä TryHackMe-alustojen aloittelija-tason harjoitukset otettiin testauksen alle vertailun merkeissä. Näistä luotiin läpikäynnit, joissa selitetään suorituksen eri vaiheet sekä toimenpiteet.

4.1 HackTheBox Archetype -harjoitus

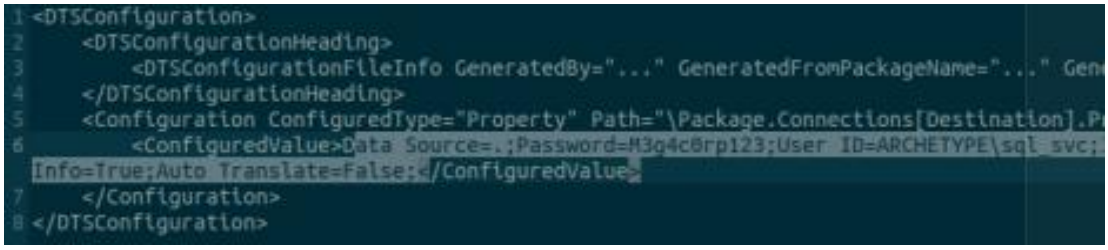
Archetype on HackTheBox-alusta Starting point-osuuden ensimmäinen harjoitus, jossa käyttäjän on tarkoitus päästä käsiksi Windows-palvelimeen ja pyrkiä sisään root-ylläpitokäyttäjänä. Harjoitus todetaan suoritetuksi, kun käyttäjä syöttää root.txt tiedoston sisällön vastauskenttään. Kyseinen tiedosto sijaitsee root-käyttäjän tiedostopolussa, johon vain kyseisellä käyttäjällä on luku- sekä kirjoitusoikeudet.

Harjoitus aloitetaan yhdistämällä hyökkäyslaite suljettuun harjoitusverkkoon VPN-avaimilla, jotka jaetaan käyttäjälle, kun hän rekisteröityy HackTheBox-alustalle. Harjoituksen kohdepalvelin skannataan Nmap-työkalulla. Skannauksesta havaitaan, että palvelin kuuntelee portteja 445 (Microsoft-DS) sekä 1433 (SQL), joita voidaan käyttää hyödyksi (Kuva 6.).

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-20 04:28 UTC
Nmap scan report for 10.10.10.27
Host is up (0.023s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Windows Server 2019 Standard 17763 microsoft-ds
1433/tcp open  ms-sql-s     Microsoft SQL Server 2017 14.00.1000.00; RTM
```

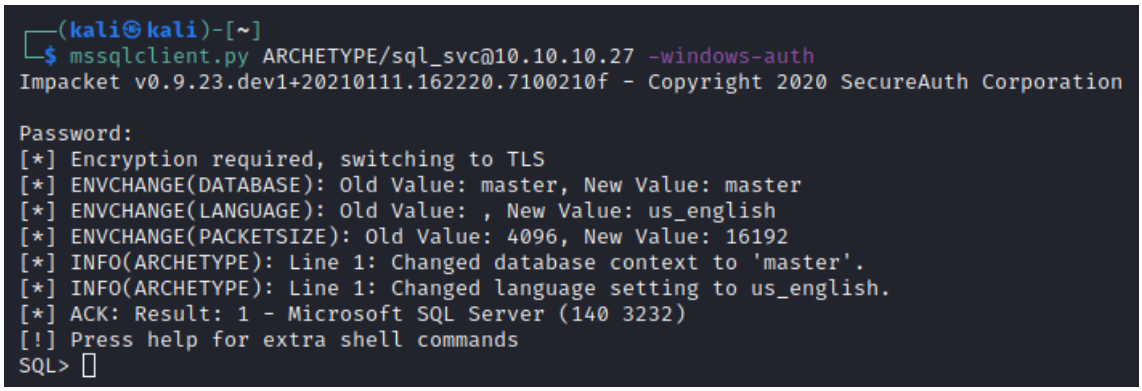
Kuva 6. Archetype harjoitteen Nmap-tulokset.

Porttiin 445 voidaan syöttää smbclient-komento, jolla voidaan anonyymisti tiedustella jaossa olevia tiedostojakoja. Tiedostojaosta löytyvästä backups-polusta löydetään prod.dtsConfig-niminen tiedosto, jonne on kovakoodattu selkokielisessä muodossa kirjautumistiedot Windows-käyttäjälle sql_svc (Kuva 7.).



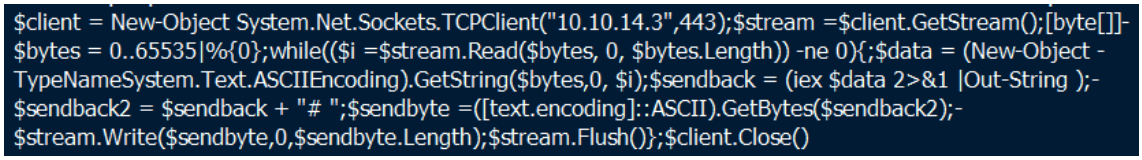
Kuva 7. Selkokielinen salasana kirjattu prod.dtsConfig-tiedostoon.

SQL-palvelimelle päästään käsiksi käyttämällä Impacket-skriptikirjaston mssqlclient.py-skriptiä, jolla saadaan terminaaliyhteys palvelimeen käyttämällä aiemmin saatuja kirjautumistietoja (Kuva 8.).



Kuva 8. SQL-palvelimen terminaaliyhteys.

Käyttäjällä sql_svc varmistetaan olevan sysadmin-tason oikeudet palvelimelle IS_SRVROLEMEMBER-komennolla. Sysadmin-tason oikeudet mahdollistavat etäkoodin ajamisen palvelimelle, joten seuraavaksi pyritään hankkimaan varsinaisen etäyhteyden palvelimelle PowerShell-skriptin avulla (Kuva 9.). Skripti tullaan jakamaan kohdepalvelimelle hyökkäyskoneelle luodusta HTTP-palvelimesta.



Kuva 9. PowerShell-komentosarja etäyhteyden saamiseksi.

Kun komentosarjan jakopalvelin on luotu, ajetaan latauskomento kohdepalvelimelta, jolla ladataan komentosarja ja ajetaan se. Tämä aiheuttaa kohdepalvelimen ottamaan reverse shell-yhteyden hyökkäyslaitteen osoitteen spesifioituun porttiin, joka on asetettu

kuuntelemaan kyseistä porttia yhteydenottojen varalta. Yhteyden muodostuessa vahvistetaan käyttäjä whoami-komennolla (kuva 10.).

```
┌──(kali㉿kali)-[~]
└─$ sudo rlwrap nc -nlvp 8888
listening on [any] 8888 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.27] 49682
id
whoami
# archetype\sql_svc
```

Kuva 10. Reverse shell-yhteyden muodostus.

Nykyisellä sql_svc-käyttäjällä on mahdollisuus ottaa talteen välisuorituksen muodossa olevat user.txt tiedosto, joka merkkaa pääsyn saamisen olevan suoritettu (kuva 11.).

```
more \users\sql_svc\desktop\user.txt
3e7b102e78218e935bf3f4951fec21a3
```

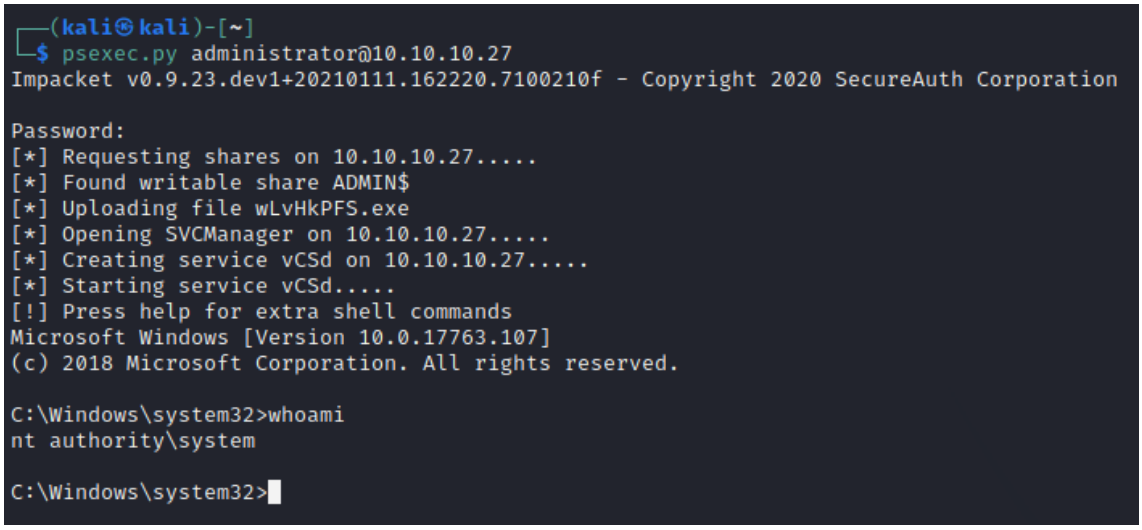
Kuva 11. user.txt tiedoston sisältö.

Seuraavaksi hankitaan lisäoikeuksia poikittaisliikkeellä, jossa pyritään eskaloimaan pääsy järjestelmävalvoja-tason käyttäjälle, jolla on oikeus root.txt tiedostoon. Informaation etsimisessä esiin tuli tallennettu ConsoleHost_history.txt tiedosto, jossa on tallella ote PowerShell-konsolin historiasta, josta löydetään selkokieliset kirjautumistiedot administrator-käyttäjälle (Kuva 12.).

```
type C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit
#
```

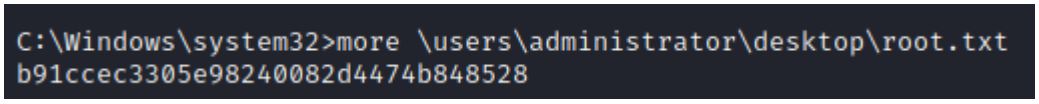
Kuva 12. Administrator-käyttäjän kirjautumistiedot.

Kirjautumistietoja voidaan käyttää uuden terminaaliyhteyden luomisessa, jolloin päästään käsiksi korkeamman käyttöoikeuksien omaavaan käyttäjään. Käyttämällä Impacket-kirjaston psexec.py komentosarjalla saadaan terminaaliyhteys ja varmistetaan käyttäjä whoami-komennolla (Kuva 13.).



Kuva 13. Terminaaliyhteys administrator-käyttäjällä.

Lopulta haetaan haluttu root.txt käyttäjän työpöydän tiedostopolusta. Tiedoston koodi syötetään HackTheBox-alustan harjoitussivustolle, jolloin harjoitus on merkitty suoritetuksi (Kuva 14.).

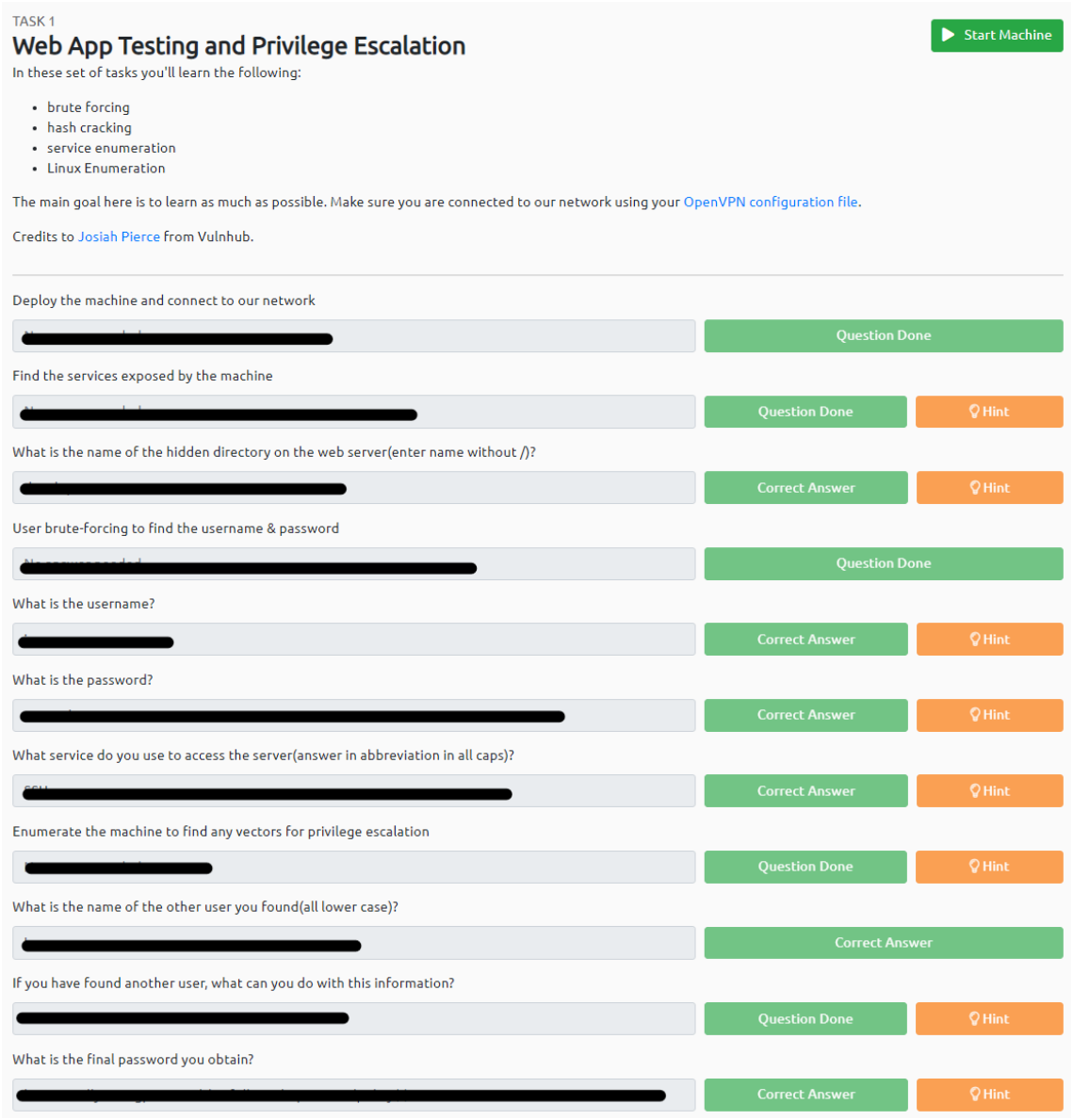


Kuva 14. root.txt sisältö.

4.2 TryHackMe Basic Penetration Testing -harjoitus

Basic Penetration Testing-harjoitus on ensimmäinen harjoitus TryHackMe-alustan Basic Computer Exploitation-moduulissa, jossa käyttäjä oppii tietoturvatestauksen perusteet. Harjoituksessa on tarkoitus pyrkiä sisään järjestelmävalvoja-tason käyttäjälle Linux-palvelimella.

Harjoitus aloitetaan yhdistämällä hyökkäyslaite harjoitusverkkoon VPN-avaimilla, jotka jaetaan käyttäjälle, kun hän liittyy harjoitukseen mukaan. Harjoitteen tavoitteet käydään läpi annetuista kysymys- sekä tehtävälistasta, josta saadaan vinkkejä laitteen sisällöstä (Kuva 15.).



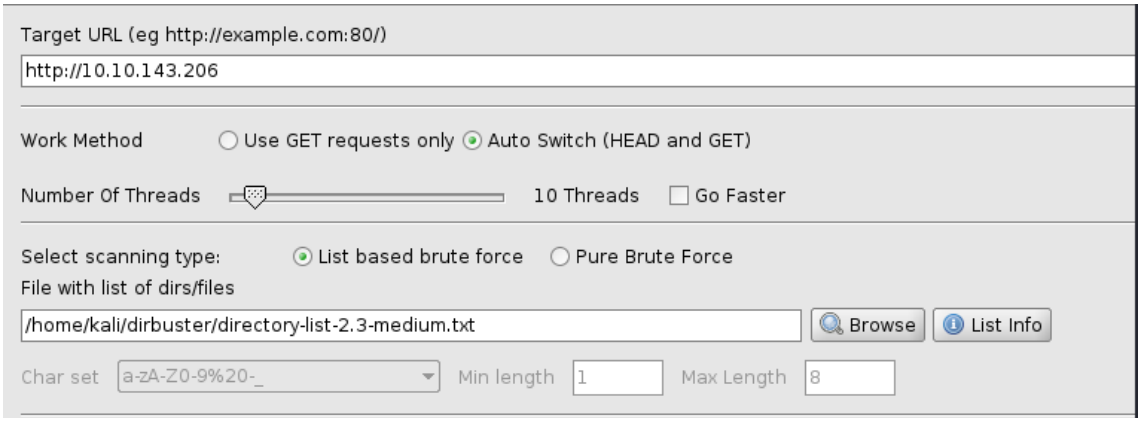
Kuva 15. Basic Penetration testing tehtävälista.

Kun yhdistäminen harjoitusverkkoon on tehty, skannataan kohdepalvelin Nmap-työkalulla. Skannauksesta havaitaan porttien 22 (SSH) sekä 8080 (HTTP) olevan avoimia (kuva 16.).

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 10.10.143.206
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-21 03:25 EDT
Nmap scan report for 10.10.143.206
Host is up (0.049s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

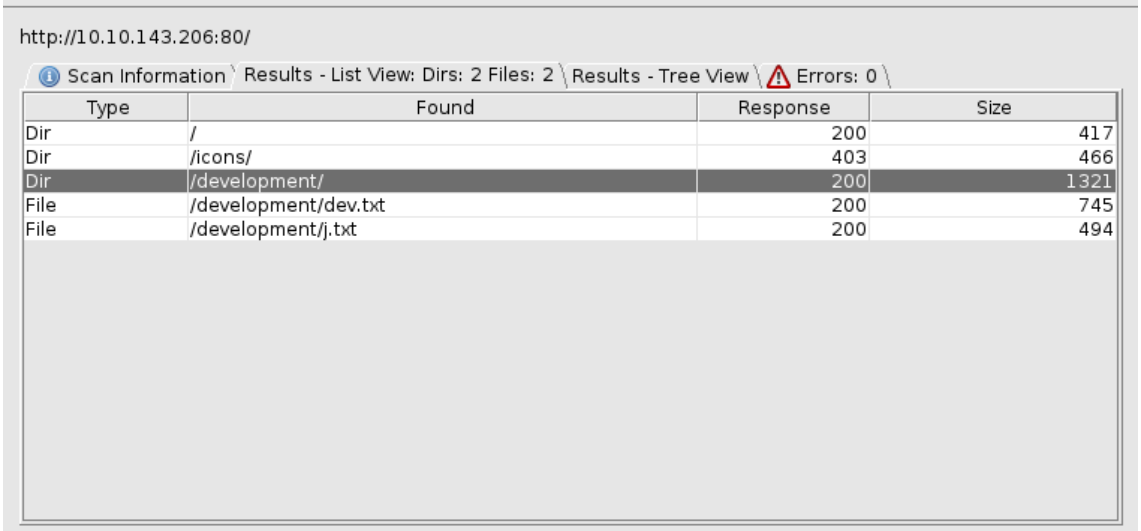
Kuva 16. Basic Penetration Testing Nmap tulokset.

Portin 8080 takana olevasta www-palvelimelta halutaan tietää piilotettu tiedostopolku, joten tätä lähdetään hakemaan DirBuster-työkalulla, jolla voidaan skannata palvelimelta piilotettuja tiedostopolkuja verraten niitä työkalussa käytettyyn sanakirja-tiedostoon. Kohdeosoitteeksi asetetaan kohdepalvelimen osoite 10.10.143.206 ja sanakirja-tiedostona käytetään DirBusterin omaa directory-list-2.3-medium.txt tiedostoa (kuva 17.).



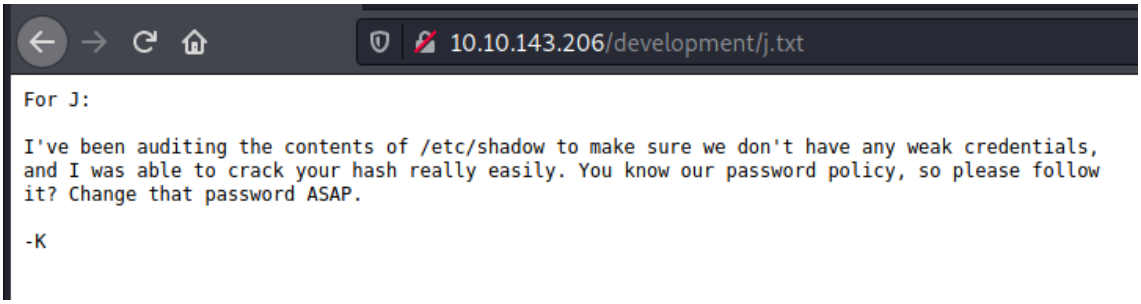
Kuva 17. DirBusterin -käyttöikkuna.

Kun DirBuster on ajettu kokonaan läpi, se listaa tulokset ikkunaan, josta havaitaan development-tiedostopolku, jota ei tavallisesti ole näkyvillä (Kuva 18.).



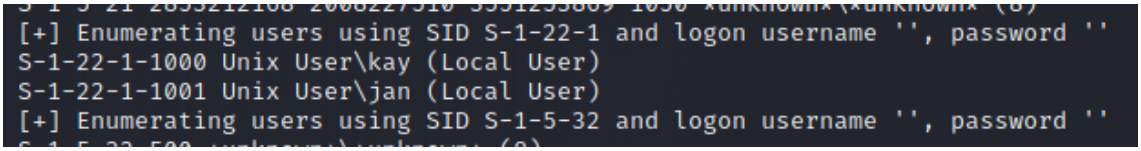
Kuva 18. DirBuster -tulokset kohdepalvelimelta.

Tiedostopolusta löytyneestä dev.txt-tiedostosta löytydetään sivuston kehittäjien välisiä viestejä, joista paljastuu, että yhdellä käyttäjistä on käytössään heikko salasana käytössä (Kuva 19.).



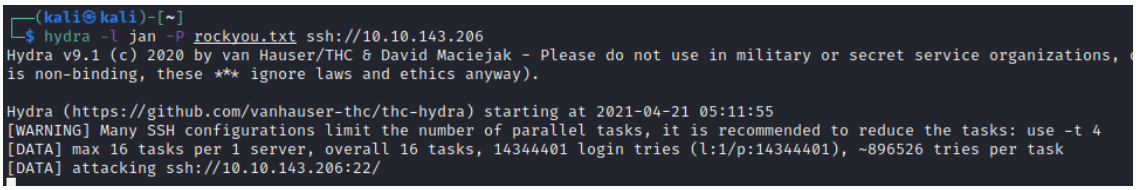
Kuva 19. j.txt sisältö.

Jotta kyseisen henkilön käyttäjä saadaan selville, käytetään enum4linux-työkalua, jolla voidaan listata tietoja kohdepalvelimelta. Listauksessa käy ilmi molempien viestissä mainittujen kehittäjien käyttäjänimet alkukirjaimen perusteella (Kuva 20.).



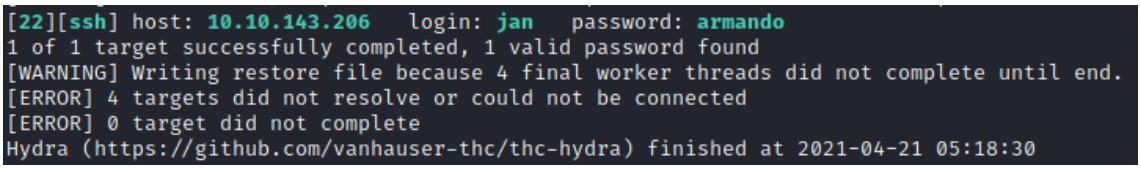
Kuva 20. Enum4linux listaamat käyttäjätunnukset.

Jan-käyttäjän heikon salasanan vuoksi tämän tilille on helpompi pyrkiä ensin, jotta voidaan myöhemmin edetä järjestelmässä. Tilille pääsemiseksi käytetään Kali-linuxissa olevaa Hydra-työkalua, jolla voidaan pakottaa pääsy heikkoja salasanoja arvaamalla tunnettujen heikkojen salasanalistojen avulla (Kuva 21.).



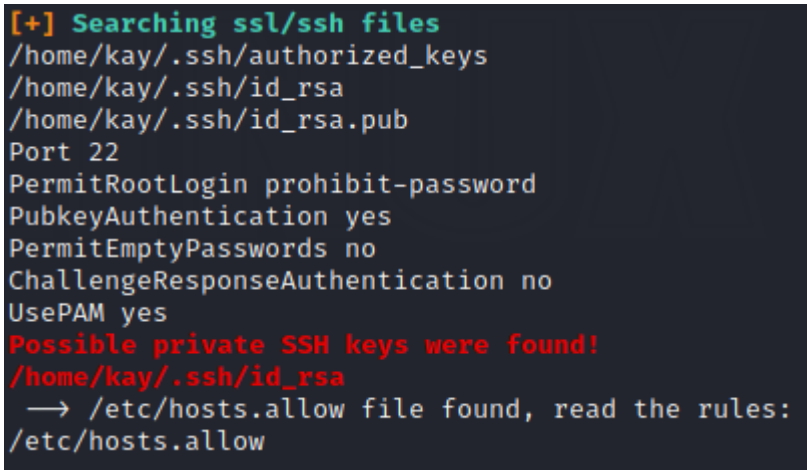
Kuva 21. Hydra-työkalun aktivointi.

Kun Hydra on onnistuneesti löytänyt heikon salasanan, joka täsmää käyttäjän salasanan kanssa, voidaan muodostaa SSH-yhteys kohdepalvelimelle kirjautumalla jan käyttäjänä (Kuva 22.).



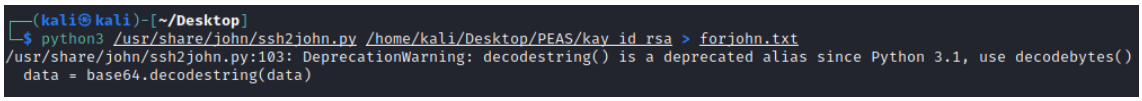
Kuva 22. SSH-yhteys käyttäjällä jan kohdepalvelimelle.

Nykyisellä käyttäjällä ei ole järjestelmävalvojan oikeuksia, joten oikeuksien hankkiminen on seuraava päämäärä. Kohdepalvelimelle ladataan linpeas.sh komentosarja, jolla listataan tietoja kohteesta, joita voidaan hyödyntää lisäoikeuksien hankkimiseksi. LinPEAS on tietoturvayhteisön luoma Linux-palvelimille suunniteltu komentosarja, jolla listataan tietoa kohteesta. Komentosarja merkitsee mahdolliset haitalliset ja huomioonotettavat seikat tulosteesta, jota käyttäjä voi hyödyntää. Komentosarja paljastaa lukukelpoisen RSA-avaimen, jota voidaan käyttää kay-käyttäjällä tehtävään SSH-yhteyden muodostamiseen (Kuva 23.).



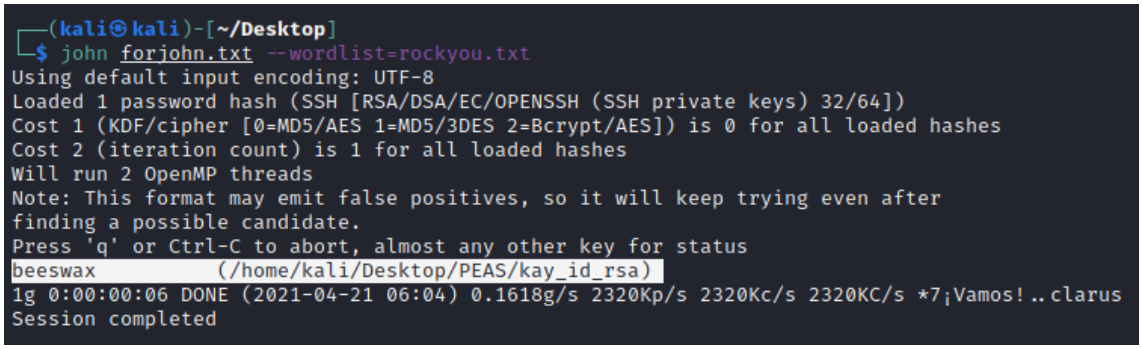
Kuva 23. LinPEAS -komentosarjan havaitsema RSA-avain.

SSH-avain kopioidaan hyökkäyslaitteelle, jossa siitä voidaan ratkoa avaimeen tarvittava salasana ulos John the Ripper -nimisellä salasanan purkutyökalulla. Työkalu ei itsessään ymmärrä RSA-avainta, joten se on vietävä ensin ymmärrettävään muotoon ssh2john.py komentosarjan avulla, joka tulkkaa avaimen muodon John the Ripper työkalulle lukukelpoiseksi (Kuva 24.).



Kuva 24. ssh2john.py komentosarjalla avaimen muunto.

Kun avain on muutettu John the Ripper -työkalun ymmärtämään muotoon, siitä puretaan kay käyttäjän salasana vertaamalla sitä tunneittuihin salasanoihin. Käyttäjän salasanaksi selvitetään beeswax (Kuva 25.).



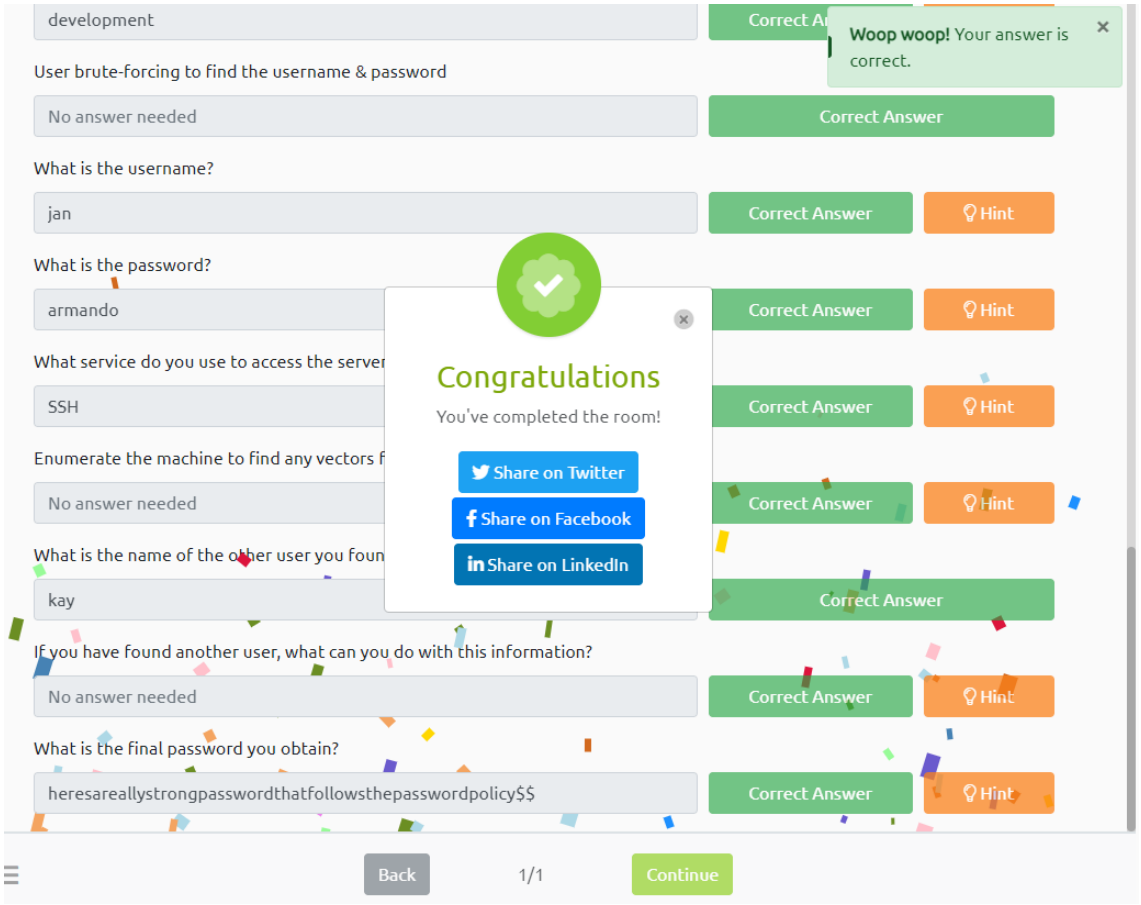
Kuva 25. Käyttäjän kay RSA-avaimen selvitetty salasana.

Selville saatujen kirjautumistietojen avulla voidaan luodan kohdepalvelimelle SSH-yhteys käyttämällä RSA-avainta. Käyttäjällä havaitaan olevan pääsy pass.bak tiedostoon, joka sisältää root-käyttäjän salasanan selkokielisenä (Kuva 26.).

```
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```

Kuva 26. root käyttäjän selkokielinen salasana pass.bak tiedostossa.

Salasanan saaminen päättää tarvittavat tekovaiheet, ja voidaan siirtyä vastaamaan annettuihin kysymyksiin. Harjoitus merkataan suoritetuksi, kun viimeisen kysymykseen on vastattu oikein, jolloin käyttäjälle tulevat pisteet sekä suoritusmerkintä käyttäjäprofiiliin (Kuva 27.).



Kuva 27. Harjoituksen suorituksen merkintä.

5 ESIMERKKIALUSTOJEN VERTAILU

Molemmat esimerkkialustat HackTheBox sekä TryHackMe tarjoavat kattavaa sekä informatiivista materiaalia tietoturvatestauksen opiskeluun. Alustojen päätarjonta ja ennemmistömäärä sisällöstä on ilmaista, joka laskee huomattavasti kynnystä aloittaa näiden alustojen käyttö, kun halutaan aloittaa itsenäinen tietoturvan opiskelu.

5.1 HackTheBox -vahvuudet

HackTheBox alustana tarjoaa kaksi eri osiota, jotka jakavat teoriapuolen omaan Academy-osioonsa sekä varsinaiset Machines- ja Challenges-harjoitukset omaan puoleensa. Näiden välille ei luoda vaatimusta suorittaa toista suoritusten etenemiseksi, joten käyttäjä kykenee keskittymään omaan kiinnostuksenkohteeseensa opiskellessaan alustan tarjontaa. Alustalla ei myöskään vaadita aloittelija-tasoisten tai helpompien harjoitusten suorittamista, joka helpottaa alasta tietävien käyttäjien etenemistä nopeampaan tahtiin.

HackTheBoxin vahvimmaksi puoleksi esiin tulee sen tarjonnan määrä sekä vaihtelevuus. Viikottaiset uudet harjoitukset tuovat käyttäjän takaisin ja koska sisältöä luodaan myös yhteisön toimesta, tarjoaa se myös ajankohtaista harjoitusta tietoturva-alan trendeihin sekä uusiin tekniikoihin.

Aloittelijaystävälliset harjoitukset osoittautuivat helpoiksi, ja näihin tarjottiin sopivasti opastusta tutoriaalien muodossa. Omaa etenemistään on alustalla helppo myös seurata pelillistetystä tasosta, joka käyttäjällä kasvaa suoritusten lisääntyessä. Jokaisen harjoituksen lopputulemana käyttäjä ansaitsee lisää kokemuspisteitä, jolla nostetaan tasoa sekä sijaintia tilastot-listalla. Tämä tuo harjoitteluun ja opiskeluun moraalilisän ja innostuksen jatkaa harjoittelua tasaisesti.

5.2 TryHackMe -vahvuudet

TryHackMe alustan parhaimmaksi vahvuudeksi osoittautui ohjeistuksen määrä harjoituksissa. Läpivientiohjeiden sijaan harjoituksissa oli video-opas, jota pystytäänn seuraa-

maan harjoitusta suorittaessa. Lisäksi alustan tapa mitata käyttäjän onnistumista kysymyksillä auttaa käyttäjää antamalla suuntaa antavia ohjeita, miten edetä harjoituksessa. Mikäli aloitteleva käyttäjä ei osaa edetä harjoituksessa eteenpäin, hän voi turvautua kysymyksiin, joista selviää seuraavan vaiheen tavoite sekä halutessa vinkki, josta voidaan hyötyä tavoitteen läpäisemiseksi.

Alustan tarjonta on jaoteltu aihealueittain, joka helpottaa harjoitusten sisällöntarkastelua, sekä mieleisten valitsemista. Aihealueiden pääpuolet ovat jaettu offensiivisen puolen sekä defensiivisen puolen harjoituksiin, sekä opiskelumateriaaliin. Käyttäjän on helppo tehdä valinta näistä aihealueista, sekä tarkastella jokaisen opetusmoduulin sisältöä etukäteen.

5.3 HackTheBox -heikkoudet

Suurin heikkous HackTheBox-alustalla on sen harjoitteiden haastavuuden skaalautuvuus sekä haastavien harjoitteiden ohjeistusten puutteellisuus. Harjoitusten päätarkoitus on simuloida oikean maailman skenaarioita sekä toimia kykyjen testauksena, joten varsinaisia ohjeita ei tarjota näihin harjoituksiin. Tämä saattaa aiheuttaa työskentelyn hitautumista ja pahimmillaan voi johtaa harjoituksen keskeytykseen mielenkiinnon puutteesta taikka osaamisen puuttumisesta. Yhteisön tekemiä läpivientiraportteja löytyy harvakseen hakemalla internetistä, mutta näistäkään ei välttämättä tule esiin haluttuja ohjeistuksia, vain muiden suoritusten tuloksia.

HackTheBox ympäristössä Academy-puolella tarjonta on myös toistaiseksi vähäinen, ja aloittelijatason opiskelumateriaali on ainoa ilmainen osuus. Advanced-tason opiskelumateriaali on suljettu maksumuurin taakse, joka estää käyttäjän pääsyn materiaaliin, jolloin tätä ei voida edes tarkastella yleiskatsaukseltaan. Lisäksi käyttäjähallinta HackTheBox-alustalla on haasteellista, sillä alusta on kokenut muodonmuutoksen aiemmin, jolloin legacy-puolen käyttäjät eivät ole rekisteröityneet Academy-puolelle. Tämä pakottaa käyttäjän luomaan vähintään kaksi käyttäjää koko alustalle ja pahimmillaan tämä vaatii kahden eri sähköpostin käyttöä, jottei systeemissä synny virhetilanteita.

5.4 TryHackMe -heikkoudet

TryHackMe alustana on keskittynyt akateemiseen tietoturvatestauksen opiskeluun, joka rajaa esimerkiksi yhteisön tarjoamien harjoitusten määrän. Harjoituksien kokonaismäärä on pienempi verrattaen HackTheBox-ympäristöön, ja harjoitusten julkaisijat ovat joko TryHackMe itse tai heidän yhteistyötoimijat, jotka ovat valikoituja tietoturva-alan osaajaryhmiä.

Lisäksi TryHackMe rajaa osan opetusmoduuliensa sisällöstä maksumuurin taakse, jolloin käyttäjältä vaaditaan premium-tasoista tiliä, jotta pääsee käsiksi lisäharjoituksiin tietyistä aiheista. Aloittelijatasoisten harjoitusten sisältöä ei ole rajattu maksumuurien taakse, mutta haastavamman sisällön käyttämiseksi vaaditaan premium-tasoista tiliä, joka saavutetaan kuukausittaisella jäsenmaksulla.

5.5 Yhteiset -heikkoudet

Sekä HackTheBox- että TryHackMe-alustoilla oli heikkouksena niiden omien työkalujen tarjonta. Harjoitusten tekemiseen vaaditaan usein hyökkäystyökaluilla varustettu tietokone, joka on helppo luoda itselleen esimerkiksi virtuaalikoneena. Alustat ovat kehittäneet asiaan myös oman ratkaisunsa ja tarjoavat käyttäjien käyttöön aikarajalla varustettua virtuaalikonetta, joka pyörii alustojen omilla palvelimilla. Käyttäjä ottaa yhteyden virtuaalikoneeseen, ja saa käyttöönsä tämän harjoituksen ajaksi. Ongelma virtuaalikoneilla on niiden pyöriminen web-alustan lävitse, joka luo testauksen harjoitteluun hidasteita ja teknisiä pulmia.

Suurin ongelma on ajankäyttö. Molemmat alustat tarjoavat tunnin ilmaista aikaa käyttää virtuaalikonetta, mutta HackTheBox vaatii premium-tasoisen käyttäjän, jotta aikaa voidaan pidentää yhtäjaksoisesti. TryHackMe-alustalla ei vaadita suoraan premium-tasoista käyttäjää, mutta aikaa on pyydettävä manuaalisesti lisää aina viimeisillä käyttöminuuteilla, joka voi johtaa toimenpiteen vahingolliseen tekemättä jättämiseen.

6 LOPPUPÄÄTELMÄT JA JATKOSUUNNITELMAT

Työn tavoitteena oli löytää aloittelijaystävällinen ja itseopiskeluun soveltuva tietoturvatestausalusta, jota voidaan käyttää tietoturva-alan itsenäiseen opiskeluun. Vertailuun otettiin mukaan erilaisia alustoja, ja niiden sisältöä tutkittiin ja käytiin läpi. Näistä alustoista päädyttiin tarkastelemaan kahta esimerkkialustaa tarkemmin.

Molemmat esimerkkialustat soveltuvat aloittelijatasoiseen tietoturvatestauksen opiskeluun. Ne sisältävät runsaan määrän opetusmateriaalia taitojen kehittämiseen sekä aloittelijatasoisille käyttäjille että kokeneille tietoturva-asiantuntijoille. HackTheBox alustan erillisellä Academy-osalla on suuri määrä opetusmoduuleita, joita voidaan käydä läpi uudelleen suorituksen jälkeenkin. Tämä osoittautuu käteväksi tavaksi hakea informaatiota, kun harjoitteessa ei ole tarjolla suoraa opastusta.

Esimerkkialustojen harjoitukset, jotka suoritettiin vertailussa, on luokiteltu aloittelijatasoisiksi vaikeusasteeltaan. Molemmat tarjoavat yksinkertaisia harjoituksia työkalujen käytöstä, joita tietoturvatestauksissa voidaan käyttää. Harjoitukset eivät vastaa oikeita palvelimia, vaan on luotu enemmän opetuspohjaisiksi esimerkkipalvelimiksi. Ne ovat helposti ratkaistavissa kirjoitettuja ohjeistuksia hyödyntämällä.

Alustojen aloittelijaystävällistä sisältöä tarkasteltiin aloittelevan käyttäjän näkökulmasta ja listattiin molempien alustojen vahvuuksia sekä heikkouksia.

HackTheBox-alustan tarjonta on kattavaa, mutta sisältää vähemmän opastettuja harjoituksia. Harjoitusten on tarkoitus lähennellä oikean maailman esimerkkejä, joille ei löydy suoraa opastusta. Lisäksi HackTheBox toivoo, ettei ohjeita julkaista harjoitusten ollessa aktiivisessa tilassa, joten käyttäjän on itse otettava selvää harjoitteiden käyttämistä palveluista sekä sovelluksista.

Suurin ongelma aloittelijalle HackTheBox -alustalla on suoran opastuksen puutteellisuus harjoitteissa. Starting point -harjoitteiden jälkeen seuraavat harjoitukset ovat pidempiä ja hankalampia. Ilman opastusta tai opetusmateriaalia opiskelu vaikuttaa aloittelevalle käyttäjälle haasteelliselta, ja mielenkiinto voi loppua ennen varsinaisen osaamisen sekä itsevarmuuden kehittymistä käyttäjässä. Myös virheen havaitseminen voi hankaloitua, kun harjoitteiden koko kasvaa ja osaamista vaaditaan enemmän. Tämä voi johtaa usein harjoitteen keskeyttämiseen.

TryhackMe alustana soveltuu helpommin aloittelevalle käyttäjälle, sillä jokainen harjoite sisältää opastusmateriaalia sekä vihjeellisiä kysymyksiä, joista voidaan päätellä seuraava harjoituksen tavoite. Mikäli ratkaisua ei löydetä, on mahdollista pyytää vihjettä, jolla ohjataan käyttäjää oikeaan suuntaan.

TryHackMe -alustan heikkous on sen suppeampi tarjonta. Ilmaiskäyttäjälle tarjotaan koko tarjonnasta noin puolet saatavilla olevista harjoitteista ja materiaalista. HackTheBoxissa on uusi sisältö kaikille, ja se siirtää vanhemmat harjoitteet myöhemmin arkistoihin. Niitä pääsee kuitenkin VIP-tason käyttäjät suorittamaan. HackTheBox tuo myös käyttäjilleen suurempia haastekokonaisuuksia, joihin kuuluu useita palvelimia, joita normaaleissa harjoitteissa on vain yksi.

TryHackMe -alustan vahvin puoli on harjoitteiden opetuksellisuus. Jokaisessa harjoituksessa on mukana kysymyksiä, joihin on vastattava oikein. Kysymysten vastaukset löytyvät, kun etenee harjoituksessa.

Tutkimuksen tuloksena todettiin molempien esimerkkialustojen olevan soveltuvia aloittelijan käyttöön, ja näiden tarjoamien harjoitusten olevan kattavia sekä yksinkertaisia. Syvemmän tarkastelun ansiosta selvitettiin myös TryHackMe-alustan olevan tietoturvan opiskelun jatkon kannalta suotuisampi alusta, koska tämä tarjoaa opastusta harjoituksiin vaativimmillakin tasoilla.

Vertailusta sekä tutkimuksesta jäivät ulkopuolelle maksulliset alustat, joka kavensi tutkittavien alustojen tarjontaa. Lisäksi ajankäytön vuoksi jätettiin esimerkkialustojen määräksi kaksi. Tämä vaikuttaa tutkimuksen loppupäätelmiin, sillä maksullisia alustoja löytyy useita, ja näiden sisältöä ei päästy tutkimaan millään tasolla.

Tutkimusta ja vertailua tullaan jatkamaan eri alustojen kesken, ja päämäränä on löytää mahdollisimman monipuolinen tietoturvatestausalusta, josta aloittelijan on hyvä lähteä liikkelle. Lisäksi alustan on tarjottava tarpeeksi sisältöä, jotta aloittelijatasoisten harjoitusten jälkeen on vielä tarjontaa työskentelyssä ja taitojen hiomisessa. Tulevaisuudessa tutkimusta sekä testausta tullaan suorittamaan alusta kerrallaan, ja vertailu alustojen kesken korvataan logiikalla, jossa alusta arvostellaan erilaisten kriteerien perusteella. Tällä tavoin tuodaan tutkimukseen enemmän puolia ja voidaan keskittyä alustojen uniikkeihin ominaisuuksiin tarkemmin.

Harjoitusten läpivientejä eri alustoilta tullaan työstämään lisää, sillä näistä saa usein selkeän kuvan haastavuudesta sekä tehtävien työmäärästä. Tarkoitus on julkaista suoritettujen harjoitusten läpivientiraportit omalla alustallaan, josta halukkaat kykenevät tarkastelemaan raportteja. Raportteihin ei kuitenkaan sisällytetä vastauksia, kuten opinnäytetyössä. Tämä tehdään sen takia, että HackTheBox- sekä TryHackMe-alustojen harjoitukset ovat ns. aktiivisia tietyn periodin ajan, jonka jälkeen ne eläköityvät, jolloin ne eivät ole pistetytyskelpoisia alustojen pisteytystalukossa. Oikeden vastausten piilottaminen ehkäisee näiden väärinkäyttöä.

Aion jatkaa tutkimustyötä, ja tavoitteenani on luoda kokoelman erilaisten tietoturvatestausalustojen harjoitusten läpivientiraporteista, jotka toimivat omana taidonnäytteenäni. Kunnianhimoisempana ideana on tuottaa täysimittainen vertailututkimus kaikista mahdollisista alustoista, sekä suorittaa käyttäjäkokeiluja alustoilla. Käyttäjäkokeiluissa testattaisiin aloittelijatasoisien käyttäjien suoriutumista harjoituksista, jolloin saataisiin aikaiseksi realistisia kokeiluja aloittelijaystävällisten harjoitusten toimivuudesta sekä niiden ohjeistusten toimivuudesta.

LÄHTEET

DirBuster (n.d.). DirBuster Package Description. Viitattu 20.03.2021 https://tools.kali.org/web-applications/dirbuster

HackTheBox (n.d.). Viitattu 20.03.2021 https://www.hackthebox.eu/

HackTheBox LinkedIn (n.d.). HackTheBox Company info. Viitattu 18.05.2021 https://www.linkedin.com/company/hackthebox/about/

Hydra (n.d.). Hydra Package Description. Viitattu 20.03.2021 https://tools.kali.org/password-attacks/hydra

Imperva (n.d.). Penetration testing stages. Viitattu 20.03.2021 https://www.imperva.com/learn/application-security/penetration-testing/

Impacket (SecureAuth Corporation). What is Impacket. Viitattu 20.03.2021 https://github.com/SecureAuthCorp/impacket

Kybersää (Kyberturvallisuuskeskus Traficom). Kybersää. Viitattu 20.02.2021 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa

LinPEAS (carlospolop). LinPEAS - Linux Privilege Escalation Awesome Script. Viitattu 20.03.2021 https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS

Nmap (n.d.). Nmap: the network mapper. Viitattu 20.03.2021 https://nmap.org/

TryHackMe (n.d.). Viitattu 20.03.2021 https://tryhackme.com/

TryHackMe LinkedIn (n.d.). TryHackMe Company info. Viitattu 18.05.2021 https://www.linkedin.com/company/tryhackme/about/

Virtual Hacking Labs (n.d.). Viitattu 20.03.2021 https://www.virtualhackinglabs.com/