Uhka-arvio DefendByVirtual

Ryhmä 13

Leevi Kauranen, AC7750
Samir Benjenna, AD1437
Eelis Suhonen, AA3910
Juho Eräjärvi, AD1276
Mikke Kuula, AC7806

Hyökkäykset ja puolustusmenetelmät sekä suojaaminen TTC6040-3009
4.12.2024
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

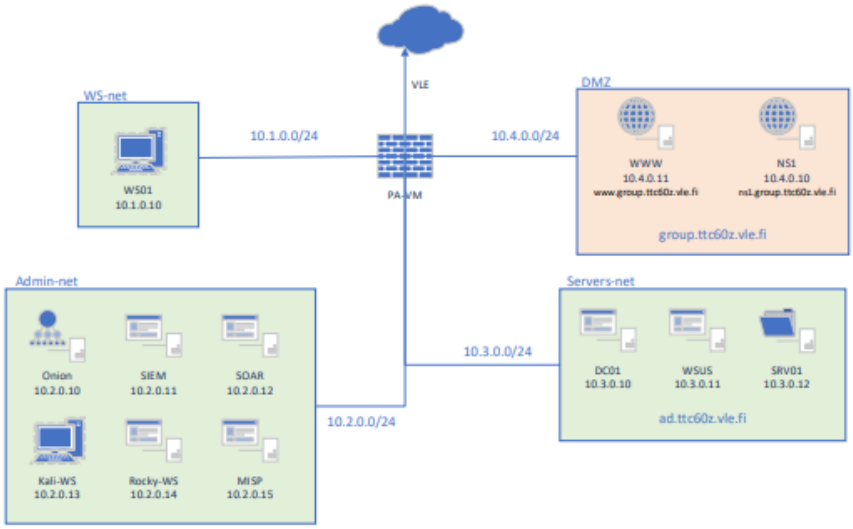
Kuviot

Taulukot

1 Johdanto

Tämän harjoitustyön tehtävänä on toteuttaa uhka-arvio DefendByVirtual yritykselle. Työ tulee pitämään sisällään uhkahypoteesin, analyysin uhkien lieventämisen nykytilanteesta sekä uhkamallinnuksen.

DefendByVirtual on yritys, joka keskittyy kyberpuolustusmenetelmien kehitykseen ja yritysten kouluttamiseen sekä konsultointiin. Yrityksen ympäristö on kuvattu kuviossa 1.



Kuvio 1. VLE

2 Suojattava omaisuus

Kuviossa 2 on tehtynä suojattavan omaisuuden kategorisointi ja luokittelu. Omaisuuden suojauksessa tulee tietää ensinnäkin, mitä omaisuuksia organisaatiolla on, ja myös, miten tärkeitä ne ovat liiketoiminnan kannalta. Omaisuuksien läpikäyminen auttaa myös uhka-arvion tekemisessä niin, että yritys näkee, mitkä omaisuuserät ovat niitä kohteita, joihin kyberrikolliset voisivat yrittää päästä käsiksi. Excel taulukko kuviossa 2, pohjautuu DefendByVirtualin aiempiin dokumentteihin, joissa käydään läpi yrityksen omaisuuksia ja niiden hallintaa.

Omaisuus	Omaisuustyyppi	Käyttö/riskiseuraus	Kriittiset kohteet intrassa	Ensisijainen / tukiomaisuus	Mahd. hyödyntämistapa
Käyttäjätiedot	Informaatio	Luottamuksen menetys, asiakastietojen menetys	WS01-työasemat	Ensisijainen	Tietojenkalastelu (Phishing)
Ohjelmistot	IT	Toiminnan keskeytyminen, tietoturvariski	WS01, SRV01	Tukiomaisuus	Haittaohjelmat (Malware injection)
Palomuurit	IT	Toiminnan keskeytyminen, tietoturvauhkien esto	Intra, SRV01	Tukiomaisuus	Konfiguraation kierto (Misconfig)
Palvelimet	IT, OT	Toiminnan keskeytyminen, tietojen menetys	SRV01	Ensisijainen	Etäyhteyksien hyväksikäyttö (RCE)
Henkilötiedot	Informaatio	Luottamuksen menetys, asiakastietojen seuraukset	WS01	Ensisijainen	Tietovuoto (Data exfiltration)
Järjestelmät	IT	Toiminnan keskeytyminen, tietojen menetys	Intra, WS01	Ensisijainen	Käyttövaltuuksien väärinkäyttö
Asiakastiedot	Informaatio	Luottamuksen menetys, asiakastietojen menetys	SRV01, WS01	Ensisijainen	Arkaluontoisten tietojen kaappaus
Päätelaitteet	IT	Toiminnan keskeytyminen, tietojen menetys	WS01	Tukiomaisuus	Endpoint-suojausten ohittaminen
Verkot	IT, OT	Verkon hallinnan menetys, tietoturvariskit	Intra	Tukiomaisuus	Verkkoliikenteen tarkkailu
Laitteisto	IT, OT	Tietojen menetys, fyysisen pääsyn riski	SRV01	Tukiomaisuus	Laitteiden fyysinen manipulointi

Kuvio 2. resurssit

2.1 Käyttäjätiedot

Käyttäjätiedot sisältävät yrityksen sisäisiä tunnuksia, joiden käyttöoikeudet määräytyvät työtehtävän ja tarpeen perusteella. Niiden käyttötarkoitus on yrityksen sisäisiin laitteistoihin ja järjestelmiin kirjautuminen, kuten WS01, DC01, KALI-WS ja ElasticSIEM. Käyttäjätietojen joutumista vääriin käsiin tulee ehkäistä erilaisten säädösten, tietoturvakulttuurin, järjestelmien ja monitoroinnin avulla.

Intraan kuuluviin kriittisiin kohteisiin kuuluu esimerkiksi Servers-net ja Admin-net verkkoalueiden käyttäjätunnukset.

2.2 Palvelimet

Ympäristömme palvelimet koostuvat Servers-net ja DMZ verkkoalueiden laiteista, kuten WWW-palvelin, DC01, NS1, WSUS, SRV01. Käyttötarkoituksiin sisältyy Windows Active Directory ympäris-

tön hallinta, Nimipalvelin, verkkosivustojen isännöinti, ja päivitysten hallinta. Palvelimet ovat kriittisessä osassa yrityksen verkkoa ja niitä täytyy suojata erilaisin menetelmin kuten pääsynhallinta, tietoturvajärjestelmät ja liikenteen monitorointi.

2.3 Verkot

Yrityksen verkkorakenne on monipuolinen. Se sisältää työasemaverkon (WS-net) jossa käyttäjien päälaitteet sijaitsevat. Se on eristetty muista verkoista turvallisuuden takaamiseksi. Hallintaverkkona käytämme Admin-nettiä, joka sisältää tietoturvan ja hallinnan työkalut, kuten SIEM, SOAR ja Kali Linux -työasemat. Tämä verkko on rajattu tietenkin vain ylläpitäjille. Demilitarisoitu vyöhyke DMZ sisältää julkisesti saavutettavat palvelut, kuten verkkosivut ja nimipalvelimet (WWW ja NS1). Servers-net on palvelinverkkomme, joka on vahvasti suojattu, sillä se toimii yrityksen sisäisten palveluiden ytimenä ja sisältää tärkeimmät palvelimet (DC01, WSUS ja SRV01). Kaikkien segmenttien välillä toimii Palomuuri (Palo Alto VM).

2.4 Asiakastiedot

Asiakastiedot koskevat yrityksen sisäisiä ja ulkoisia sopimuksia, liikesalaisuuksia, yhteystietoja ja projektitietoja. Asiakastiedot ovat pääsääntöisesti arkaluonteista tietoja, joten kaikkia asiakastietoja säilytetään SRV01-tiedostopalvelimella. Palvelimella on oltava vahva salaus ja sitä on valvottava erityisen tarkasti välttyäkseen esimerkiksi tietomurroilta. Tietoihin pääsee käsiksi vain ne yrityksen työntekijät, joilla on siihen oikeus. Työntekijät käsittelevät asiakastietoja omilla WS01-työasemilla. Sen takia yrityksen liikennettä on rajoitettava ja valvottava vahvasti palomuurilla ja erillisillä monitorointityökaluilla. Asiakastiedot ovat luokiteltu kriittisyyden mukaan, jonka perusteella suojaustasot määritellään.

2.5 Palomuurit

Palomuurin käyttö on keskeinen osa yrityksen tietoturvastrategiaa. Yrityksen sisäistä ja sinne saapuvaa liikennettä valvotaan Palo-Alto palomuurilla. Palomuurilla verkon segmentointi on tärkeä

osa yrityksen suojausta ja valvontaa. Verkot jaetaan sääntöjen avulla loogisiin alueisiin, jotka vähentävät sivuttaisliikenteen riskiä (lateral movement) hyökkäyksissä. Säännöillä määritetään myös kuka ja mikä voi käyttää tiettyjä resursseja. Palomuuri suojaa ympäristöä tunnetuilta hyökkäyksiltä ja esimerkiksi estää palvelunestohyökkäyksiä havaitsemalla epäilyttävä suuren liikenteen ja suodattamalla sen. Palomuuri toimii yrityksen ensimmäisenä puolustuslinjana.

3 Uhka-arvio

3.1 Uhkahypoteesi APT 28

APT 28 (tunnetaan myös muilla nimillä, kuten Fancy Bear tai Sofancy) on Venäjällä jo pitkään toiminut kyberuhkaryhmä (APT). Se on ollut tiedetysti aktiivisena ainakin 2000-luvun puolesta välistä lähtien. Tämän uhkatoimijan ensisijaiset kohteet ovat länsi- ja NATO-maiden hallitukset, armeijat ja geopoliittiset toimijat. APT28:n uskotaan olevan yhteydessä Venäjän armeijan tiedustelupalveluun (GRU), ja sen toiminnan uskotaan olevan valtion tukemaa. Sen resurssien tulee olla niin suuret (perustuen aiempaan toimintaan), ja toimintatavat niin edistyksellisiä, että ryhmä saa mitä luultavimmin tukea Venäjän valtiolta toimiinsa. Kun ymmärrämme uhkatoimijan motiivit ja toimintatavat, voimme tämän pohjalta tehdä arvion, mihin APT28 voisi kohdistaa kyberhyökkäyksensä organisaatiossa. (Understanding APT28: A Full Recap of Notorious Cyber Threat. 2024)

- **Geopolitiikka:** APT28 tavoitteena on heikentää NATO:n ja EU:n poliittista vakautta, koska nämä ovat Venäjän vastaisia toimijoita.
- **Kybervakoilu ja tietovuodot:** APT28 tekee kybervakoilua, jonka kautta se saa tietoja esimerkiksi tärkeiltä länsimaisilta organisaatioilta.
- **Liittoutumien murtaminen ja vaikutusvalta:** APT28:n toimet länsimaisten liittoumien (EU, NATO) heikentämiseen ja yleisesti Venäjän vaikutusvallan lisäämiseen Euroopassa. (Understanding APT28: A Full Recap of Notorious Cyber Threat. 2024)

On arvioitu, että APT 28 saattaa lisätä Suomeen kohdistuvaa toimintaansa presidentinvaalien yhteydessä. Tämän vuoksi on tärkeää valmistautua mahdollisiin ryhmän vaikuttamisyrityksiin.

Kohdennettu kalastelu: APT28 yrittää saada jalansijaa verkossamme käyttämällä kohdennettuja kalasteluviestejä, jotka on räätälöity yrityksen ylimmälle johdolle. Viestit sisältävät haitallisia liitetiedostoja, jotka hyödyntävät nollapäivähaavoittuvuuksia Microsoft Office -ohjelmissa.

Kirjautuminen oikeilla tunnisteilla: APT28 on saanut käsiinsä käyttäjätunnuksia kohdennetuilla sähköpostiin lähetetyillä kalasteluviesteillä ja pystyy kirjautumaan yrityksen järjestelmiin. Ryhmä on käyttänyt myös laitevalmistajien asettamia vakio salasanoja esimerkiksi tulostimiin kirjautumiseen.

Verkon haistelu: APT28 saa kaapattua käyttäjänimiä ja salasanojen hasheja käyttämällä NetBIOS nimipalvelun myrkyttämistä. Ryhmä voi käyttää myös Wi-FI pineapple työkalua kaappaamaan Wi-Fi signaaleja.

Palvelunestohyökkäys: APT28 pyrkii häiritsemään organisaation toimintaa ja verkkopalveluita toteuttamalla laajamittaisen hajautetun palvelunestohyökkäyksen (DDOS) käyttäen bottiverkkoa. Tämä voi olla osa laajempaa häirintätoimenpidettä, jonka tarkoituksena on estää organisaation toiminta ja luoda sekaannusta.

Julkisen palvelun haavoittuvuuksien hyödyntäminen: APT28 hyväksikäyttää julkisesta osoitteesta löytyvää haavoittuvuutta, kuten CVE-2020-17144, jonka avulla APT28 pääsee käsiksi kaikkiin Microsoft Exchange palvelimiin ja saavat järjestelmänvalvojan oikeudet.

Tunnistetietojen kaappaus: APT28 käyttää Mimikatz ohjelmaa saadakseen salasanoja muistista, joiden avulla he saavuttavat sivuttaisliikettä ympäristössämme.

Proxyjen käyttö (Proxying): APT28 voi käyttää Proxy-palvelimia, eli sisäverkon laitetta, jonka kautta hyökkääjä kerää tietoa ja ajaa komentoja. Näin hyökkääjän oikea osoite pysyy salassa, koska kaikki liikenne näyttää tulevan sisäverkossa olevalta laitteelta. C2-liikenne voidaan salata ja peittää proxyjen avulla. Haittaohjelmat, kuten CHOPSTICK voivat hyödyntää tätä tiedonsiirrossa.

C2 palvelimelle yhdistäminen: APT28 luo yhteyden komentopalvelimelleen käyttäen CHOPSTICK haittaohjelmaa. CHOPSTICK on kehittynyt, moduulirakenteinen haittaohjelma, jonka avulla APT28 voi etäohjata tartunnan saaneita laitteita, välittää tietoa, varmistaa pysyvyyden kohdeympäristössä ja hallita muita hyökkäyksen vaiheita. Yhteyden avulla APT28 pystyy siirtämään lisämoduuleja ja hyötykuormia tartunnan saaneeseen ympäristöön tarpeen mukaan.

Tiedon kerääminen: APT28 käyttää FPT tai HTTP/HTTPS protokollaa lähettämään tietoa heidän palvelimilleen.

3.2 STRIDE-luokittelu:

Taulukko 1. STRIDE-luokittelu

Tyyppi	**APT28 esimerkki**	**Kontrolli**
Identiteettivarkaus (Spoofing)	Kohdennettu kalastelu, Väärennetty käyttäjätili	Henkilöstön koulutukset, Monivaiheinen tunnistautuminen (MFA), Kirjautumisen seuranta
Peukalointi (Tampering)	Haittaohjelmien (Malware) asentaminen, Konfigurointien muutokset, Tietokantojen muutokset	Tärkeiden tiedostojen eheyden tarkistus (checksum), Admin-oikeuksien vaatiminen, Sovellusten käyttöoikeuksien hallinta, Virus ja Malware torjuntaohjelmat

Jäljitettävyys (Repudiation)	Lokitietojen manipulointi tai poistaminen jälkien peittämiseksi	Lokien muutoksien esto, keskitetty lokien hallinta, hälytykset lokitietojen manipuloinnista
Tietovuoto (Information disclosure)	Luottamuksellisten tietojen vuotaminen palvelimilta (SR1) ja työkoneilta (WS1)	Tietoliikenneverkon siirtojen seuranta (SIEM), Tietoliikenteen salaaminen
Palvelunesto (Denial of service)	Palvelunestohyökkäykset palvelimia (Servers-net) kohtaan.	Tulvinnan esto (Palo Alto), Epäilyttävien (Malicious) IP-osoitteiden esto, DDoS-suojauspalvelut?
Käyttövaltuuksien laajentaminen (Elevation of privilege)	Käyttöoikeuksien nostaminen järjestelmässä	Vähimpien oikeuksien periaate, Admin kirjautumisen seuranta

3.3 Tehtyjen kontrollien lieventävä vaikutus

DefendByVirtualin ympäristöön on tehty useita kovennuksia ja kontrolleja osana muiden opintojaksojen tehtäviä. Näiden avulla pystytään torjumaan mahdollisia uhkia, joita APT28 luo yrityksen toiminnalle.

Palo Alto palomuuri: Palomuuriin on tehty sääntöjä, jotka estävät väärinkäyttöyrityksiä. Palomuuri on integroitu Active Directoryyn. Tällä voidaan luoda erilaisia tunnistus ja valtuutusmekanismeja, jotka parantavat käyttäjänhallintaa ja helpottavat epäilyttävän toiminnan havaitsemista.

Active Directory: DC01-palvelimella olevaa Active Directorya on kovennettu. Active Directoryyn on luotu sääntöjä, jotka rajoittavat eri käyttäjäryhmien toimintaa. Esimerkiksi PowerShellin käyttöä on rajoitettu siten, että ainoastaan järjestelmänvalvojat pystyvät käyttämään sitä.

Tiedostopalvelin: Tiedostopalvelin on kovennettu poistamalla käytöstä turhat palvelut, jotta niiden mahdollisia heikkouksia ei voida hyödyntää hyökkäyksissä. Lisäksi eri käyttäjäryhmillä on oikeus ainoastoaan niihin tiedostopalvelimen levyihin, joihin heillä on tarve päästä.

ElasticSIEM: Windows-työasemat ja -palvelimet sekä WWW-palvelin ovat integroitu ElasticSIEM-järjestelmään. SIEMin avulla voidaan monitoroida järjestelmissä tapahtuvaa liikehdintää. SIEM antaa hälytyksiä, jos järjestelmässä tapahtuu jotain normaalista poikkeavaa. Näin mahdollisiin hyökkäyksiin voidaan reagoida nopeasti ja ne voidaan estää, ennen kuin suurta haittaa on tapahtunut.

WSUS: DefendByVirtualilla on käytössä WSUS (Windows Server Update Services) päivitysten hallintatyökalu. WSUS:ksen avulla hyväksytään ja jaetaan ympäristön Windows-laitteisiin uusia päivityksiä, jotka parantavat tietoturvallisuutta ja vaikeuttavat hyökkääjän toimia.

Koulutukset: Henkilöstölle on annettu tietoturvakoulutusta. Tietoturvakoulutuksen tarkoituksena on kehittää henkilöstön taitoja ja tietoisuutta havaitsemaan, raportoimaan ja ehkäisemään tietovuotoja.

3.4 APT28 hyökkäyspolku

Tavoite: Varastaa liikesalaisuudet

1. **Vaihtoehto 1: Hyökkäys WS01-työasemien kautta**
   - **Taktiikka:** Alkuperäinen pääsy (Initial access)
     - **T1566 (Phishing):** Työntekijälle lähetetään kohdennettu sähköposti, joka sisältää haitallisen linkin tai tiedoston.
       - Työntekijä napsauttaa linkkiä ja haittaohjelma lataa itsensä työasemalle.

   - **Taktiikka**: Haittaohjelman toteutus

- **T1204.002 (User Execution – malicious file):** Haittaohjelma suoritetaan käyttäjän toimesta.

- **Taktiikka:** Sivuttaisliike (lateral movement)
  - **T1021.002 (Remote Services – SMB/Windows Admin Shares):** Hyökkääjä liikkuu esimerkiksi WS01 ja SRV01 välillä käyttäen yhteisiä resursseja.
  - **T1563 (Remote Service Session Hijacking):** Hyökkääjä voi ottaa haltuunsa jo olemassa olevia istuntoja käyttäen esimerkiksi SSH ja RDP yhteyksiä liikkuakseen ympäristössä sivuttaisliikkeessä

2. **Vaihtoehto 2: Hyökkäys suoraan SRV01-palvelimelle**
   - **Taktiikka:** Alkuperäinen pääsy (Initial Access)
     - **T1133 (External Remote Services):** Hyökkääjä käyttää etäyhteyttä päästäkseen palvelimelle (esimerkiksi haavoittuva VPN-yhteys).

   - **Taktiikka:** Haavoittuvuuksien hyväksikäyttö (Exploitation of vulnerability)
     - **T1190 (Exploit Public-Facing Application):** Hyökkääjä hyödyntää palvelimessa mahdollisesti olevaa heikkoutta päästäkseen sisään verkkoon. Heikkouksia voi olla esimerkiksi ohjelmistovika, tilapäinen häiriö tai virheellinen konfigurointi.

   - **Taktiikka:** Tietojen varastaminen (Exfiltration)
     - **T1041 (Exfiltration over C2 Channel):** Palvelimen tiedostot varastetaan salaamalla ne komento- ja valvontakanavan kautta.

3.5 STRIDE Varautumiskeinot:

Taulukko 2. Varautumiskeinot

Uhkatyyppi	**Varautumiskeinoja**
Identiteettivarkaus (Spoofing)	1. Palo Alto palomuuriin on luotu sääntöjä, jotka estävät väärinkäyttöyrityksiä ja auttavat tunnistamaan epäilyttävän toiminnan. 2. Active Directoryyn on kovennettu käyttäjien tunnistamista ja valtuutusta. 3. Koulutukset henkilöstölle tietoturvasta ja kalasteluviestien tunnistamisesta.

Peukalointi (Tampering)	1. Active Directoryssä rajoitetaan PowerShellin käyttöä vain järjestelmänvalvojille, estäen mahdolliset konfiguraatiomuutokset. 2. Tiedostopalvelimella on käytössä tiivistefunktioita, joilla estetään tiedostojen manipulointi. 3. Virustorjunta ja haittaohjelmien torjuntaohjelmat, kuten Palo Alto, suojaavat järjestelmiä.
Jäljitettävyys (Repudiation)	1. ElasticSIEM-järjestelmän avulla monitoroidaan käyttäjien ja laitteiden liikkeitä, mikä varmistaa, että kaikki toimenpiteet ovat jäljitettävissä. 2. Lokitiedot ja tapahtumatarkistukset ovat keskeinen osa kyberturvallisuutta, ja lokit ovat suojattu manipuloinnilta. 3. Aikaleimat ja digitaalisten allekirjoitusten käyttö varmistavat toimenpiteiden aitouden.
Tietovuoto (Information Disclosure)	1. Käyttöoikeudet on rajoitettu vain tarvittaviin tiedostoihin ja palvelimiin, jotta estetään luottamuksellisten tietojen vuotaminen. 2. Tiedon salaaminen on käytössä sekä tiedostopalvelimilla että viestiliikenteessä (esimerkiksi HTTPS). 3. Koulutuksessa painotetaan salaisen datan suojaamista ja oikeaa käyttöoikeuksien hallintaa.
Palvelunesto (Denial of Service)	1. Palo Alto palomuuri tarjoaa DDoS-suojauksen ja suodattaa epäilyttävän liikenteen. 2. WSUS-päivitystyökalu takaa, että kaikki järjestelmät ovat ajan tasalla, estäen mahdolliset haavoittuvuudet.

	3. Palvelutason takaaminen (Quality of Service) tekniikat varmistavat, että tärkeät palvelut pysyvät toiminnassa jopa hyökkäysten aikana.
Käyttövaltuuksien laajentaminen (Elevation of Privilege)	1. Käyttöoikeudet on mallinnettu ja toteutettu vähimmän oikeuden periaatteen mukaisesti, jotta käyttäjät voivat suorittaa vain tarvitsemaansa toimintaa. 2. Järjestelmänvalvojien kirjautuminen ja käyttöoikeuksien seuranta estävät oikeuksien väärinkäytön.

4 Pohdinta

Tämä harjoitustyö tarjosi hyödyllistä oppimista käytännön sekä teorian tasolla kyberturvallisuuden keskeisistä osa-alueista. Työn aikana perehdyimme uhka-arvion laatimiseen, hyökkäyspolkujen analysointiin sekä puolustusmekanismien suunnitteluun ja arviointiin DefendByVirtual-yrityksen kontekstissa. Opimme, että kyberturvallisuus on monitasoinen ja jatkuvasti muuttuva kokonaisuus, jossa ennaltaehkäisevät toimet, reaaliaikainen monitorointi ja selkeät toimintasuunnitelmat ovat ratkaisevassa roolissa. Myös erilaisten dokumenttien, kuten uhka-arvion jatkuva ajan tasalla pitäminen ja kehittäminen ovat tärkeässä roolissa organisaation kyberturvallisuutta kehitettäessä.

Saimme myös hyvän mahdollisuudet tutustua APT28:n käyttämiin hyökkäyspolkuihin ja kuinka niiltä voisi suojautua. Tämä osoitti myös hyvin kuinka monimutkaisia ja kehittyneitä nykyaikaiset hyökkääjät voivat olla. Hyökkäyspolkua analysoidessamme ymmärsimme, kuinka hyökkääjät voivat yhdistellä eri tekniikoita, kuten nollapäivähaavoittuvuuksien hyödyntämistä ja C2-palvelimien käyttöä, saavuttaakseen tavoitteensa.

Keskeisiin oppeihin kuuluu myös tieto siitä, miten teknisten ratkaisujen rinnalla ihmisten toiminta on usein kriittinen tekijä tietoturvassa. Tämä korostui henkilöstön koulutuksen merkityksessä: vaikka järjestelmät olisivat teknisesti hyvin suojattuja, ihmisten tekemät virheet, kuten kalastelusähköpostien avaaminen, voivat avata tien hyökkäyksille. Siksi tietoturvakulttuurin vahvistaminen on yhtä tärkeää kuin tekniset ratkaisut.

Kaiken kaikkiaan tämä harjoitustyö tarjosi erinomaisen mahdollisuuden soveltaa teoriassa opittuja asioita käytännön ongelmanratkaisuun ja antoi meille syvemmän ymmärryksen siitä, miten kyberturvallisuutta toteutetaan ja ylläpidetään organisaatiotasolla.

Lähteet

Understanding APT28: A Full Recap of Notorious Cyber Threat. The SOC Labs artikkeli. 2024. Viitattu 14.11.2024. https://thesoclabs.com/understanding-apt28-a-full-recap-of-cyber-threat/