Labra 2 Case Kybereo

Ryhmä 13

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Hyökkäykset- ja puolustus menetelmät

17.10.2024

Tieto- ja viestintätekniikka

Sisältö

[1 Johdanto 3](#_Toc179828654)

[2 Tunnistaminen ja tutkiminen 3](#_Toc179828655)

[3 Tutkimus- ja hyökkäyspolku 8](#_Toc179828656)

[4 Auditointi 10](#_Toc179828657)

[4.1 Skannaukset 11](#_Toc179828658)

[4.1.1 Haavoittuvuuksista 14](#_Toc179828659)

[5 Pohdinta 15](#_Toc179828660)

[Lähteet 17](#_Toc179828661)

Kuviot

[Kuvio 1. Tietojenkalastelusähköposti 3](#_Toc180056657)

[Kuvio 2. Viestin hälytysmerkit 4](#_Toc180056658)

[Kuvio 3. Sähköpostiosoitteet 5](#_Toc180056659)

[Kuvio 4. Kalastelusivusto 5](#_Toc180056660)

[Kuvio 5. Kybereon oikea intra 6](#_Toc180056661)

[Kuvio 6. WordPress hallintapaneeli 6](#_Toc180056662)

[Kuvio 7. WordPressin skriptat 7](#_Toc180056663)

[Kuvio 8. Kalastelusivuston kävijät 7](#_Toc180056664)

[Kuvio 9. Käyttäjän luonti SQL-injektiolla 8](#_Toc180056665)

[Kuvio 10. Hyökkääjän luoma käyttäjä WordPress hallintapaneelissa 8](#_Toc180056666)

[Kuvio 11. Tutkimuspolku 9](#_Toc180056667)

[Kuvio 12. Hyökkäyspolku 9](#_Toc180056668)

[Kuvio 13. Kirjautumislomakkeen heikkous 10](#_Toc180056669)

[Kuvio 14. Avoimet portit 11](#_Toc180056670)

[Kuvio 15. Lisätietoa avoimista porteista 12](#_Toc180056671)

[Kuvio 16. Nmapin löytämät haavoittuvuudet 12](#_Toc180056672)

[Kuvio 17. Portin 80 skannaus 13](#_Toc180056673)

[Kuvio 18. Portin 443 skannaus 13](#_Toc180056674)

[Kuvio 19. MariaDB versio 15](#_Toc180056675)

# Johdanto

Kyberhyökkäyksen analysointi on oleellinen vaihe tilanteen vakavuuden ymmärtämiseksi sekä haavoittuvuuksien tunnistamiseksi ja korjaamiseksi. Kyberrikolliset käyttävät usein monivaiheisia hyökkäyksiä, joissa hyödynnetään teknologisia heikkouksia tai ihmisten alttiutta erehtyä sosiaalisen manipuloinnin kautta. Kalasteluhyökkäyksessä käyttäjille lähetetään viestejä, joiden on tarkoitus näyttää aidoilta, organisaation lähettämiltä viesteiltä. Niillä pyritään huijaamaan käyttäjiä paljastamaan henkilökohtaisia tietojaan. Tällaiset hyökkäykset voivat johtaa laajoihin tietovuotoihin ja aiheuttaa merkittävää vahinkoa yrityksen maineelle ja toiminnalle.

Tutkimuksen tavoitteena on analysoida tapahtunut kuvitteelliseen Kybereo-yliopistoon kohdistunut kalasteluhyökkäys, kartoittaa käytetyt tekniikat ja hyökkäyksen kulku sekä paljastuneet heikkoudet.

# Tunnistaminen ja tutkiminen

Kuva, joka sisältää kohteen teksti, elektroniikka, kuvakaappaus, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 1. Tietojenkalastelusähköposti

Ensimmäisenä tehtävänä oli tunnistaa kuvion 1 viestistä merkit, jotka viittaavat tietojenkalasteluviestiin. Kuviossa 2 on ympyröitynä selkeitä hälytysmerkkejä viestistä. Lähettäjän sähköpostiosoite on [ict@kybeneo.ch](mailto:ict@kybeneo.ch), ja viestin lopussa allekirjoituksena on ”Best regards, Kyberoo ICT”. Molemmissa kohdissa Kybereo on kirjoitettu väärin ja kummallakin kerralla eri tavalla.

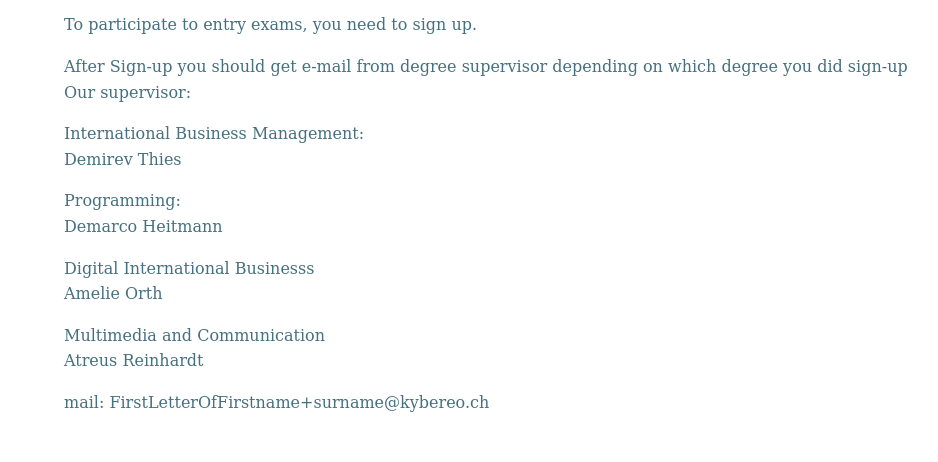
Viestissä oleva informaatio on suppeaa ja lyhytsanaista, eikä sen tarkoitusta ei ole selitetty tarkemmin. Tämä johtaa epäilyyn, jos henkilöstö saa viestejä usein ICT tuelta, voisi hän huomata eron kirjoituksessa. Tärkeää infoa ja klikkaa linkkiä on viestin sanoma, joka luo vähän kiireellisyyden tuntua, mutta ei liian aggressiivisesti. Epähuomiossa ja/tai kiireessä viestin avaaja saattaa klikata linkkiä, jos hän ei tiedosta sen tietoturvauhkaa. Viestin loppuosa on epäilyttävän lyhyt, vain organisaation nimi ja sen jälkeen ICT. Jos viesti tulisi aidolta Kybereon ICT-tiimiltä, voisi kuvitella kirjoittajan laittavan oman nimensä ja muuta lisäinfoa viestin loppuun esim. puhelinnumeron tai "Ystävällisin terveisin!". Lähettäjän tiedot on kuitenkin aina oltava selkeästi näkyvissä, jotta sähköpostiin voi mitenkään luottaa.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Verkkosivusto, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 2. Viestin hälytysmerkit

Hakkeri löysi Kybereon työntekijöiden sähköpostiosoitteet osoitteesta https://www.kybereo.ch/remote-entry-exams/. Osoitteen muoto on työntekijän etunimen ensimmäinen kirjain ja sukunimi. Työntekijän Amelie Orth sähköposti on aorth@cybereo.ch. Tietojenkalasteluviesti on lähetetty ainakin tähän osoitteeseen. (Kuvio 3).



Kuvio 3. Sähköpostiosoitteet

Tietojenkalasteluviestin linkki vie väärennetylle Kybereon intranet sivulle, jossa pyydetään heti kättelyssä yritystunnuksia (Kuvio 4). Sivuston osoite ei herätä epäilyksiä, mutta sivusto näyttää erilaiselta, kuin Kybereon intran kirjautumissivu, johon päästään Kybereon etusivulta (Kuvio 5). Lisäksi kalastelusivun kirjautumislomake kysyy käyttäjänimen ja salasanan erikseen, eikä samalla lomakkeella, kuten yleensä on tapana. Epäilyksiä herättää myös se, että kirjautumislomakkeessa kaikki on kirjoitettu pienillä alkukirjaimilla, joten sivusto ei vaikuta ammattimaiselta.

Kuva, joka sisältää kohteen kuvakaappaus, teksti, ohjelmisto, Multimediaohjelmisto

Kuvaus luotu automaattisesti

Kuvio 4. Kalastelusivusto

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Käyttöjärjestelmä

Kuvaus luotu automaattisesti

Kuvio 5. Kybereon oikea intra

Kirjatumalla Kybereon WordPress hallintapaneeliin voimme nähdä, että hyökkääjän tekemä kalastelusivusto on lisätty pages-välilehdelle. (Kuvio 6).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Tietokonekuvake

Kuvaus luotu automaattisesti

Kuvio 6. WordPress hallintapaneeli

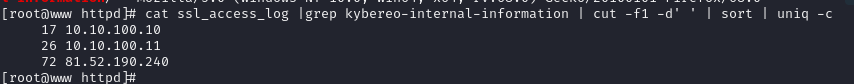
Sivun scripts-osioon on lisätty seuraava skripta, joka välittää käyttäjänimen ja salasanan osoitteeseen <https://www.kyberoo.ch/index.php>. (Kuvio 7).

Kuva, joka sisältää kohteen teksti, Fontti, kuitti, algebra

Kuvaus luotu automaattisesti

Kuvio 7. WordPressin skriptat

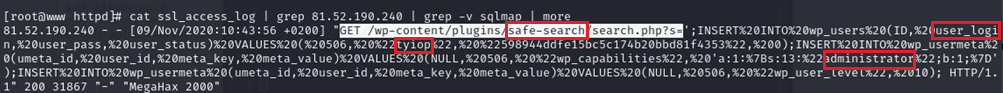
Tarkastellaksemme käyttäjien käyntiä tietojenkalastelu sivustolla tarvitsimme yhteyden palvelimelle, josta pystyimme tarkastella käyttäjien toiminta lokeja. Otimme SSH-yhteyden Kalilta WordPressin palvelimelle ja kuvion 8 komennolla saimme tulosteen, jonka perusteella kolmesta eri IP-osoitteesta on kirjauduttu sivustolle, joista yksi on ulkopuolisesta verkosta (hyökkääjä). Ensimmäisestä IP-osoitteesta on kirjauduttu 17 kertaa ja toisesta 26 kertaa.



Kuvio 8. Kalastelusivuston kävijät

Yksi kolmesta ip osoitteesta on selvästi ulkoverkosta eli 81.52.190.240, voimme suodattaa tämän osoitteen access lokista ja tarkastella toimia.

Hyökkääjä on hyödyntänyt WordPressin Safe Search lisäosaa, joka on altis SQL-injektioiden avulla tapahtuville hyökkäyksille. Sen avulla hyökkääjä on onnistunut luomaan itselleen käyttäjätunnuksen nimeltä tyiop ja antamaan sille administrator-oikeudet. (Kuvio 9)



Kuvio 9. Käyttäjän luonti SQL-injektiolla

Käyttäjä löytyy myös WordPressin hallintapaneelista. (Kuvio 10)

Kuva, joka sisältää kohteen teksti, ohjelmisto, numero, Fontti

Kuvaus luotu automaattisesti

Kuvio 10. Hyökkääjän luoma käyttäjä WordPress hallintapaneelissa

Luotujen tunnusten avulla hyökkääjä on luonut tietojenkalastelusivuston, joka lähettää käyttäjätunnukset eteenpäin hyökkääjän omalle palvelimelle.

# Tutkimus- ja hyökkäyspolku

Kuviossa on kuvattuna tutkimuspolku, jonka mukaan etenimme tutkiessa hyökkäystä. (Kuvio 11)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, viiva

Kuvaus luotu automaattisesti

Kuvio 11. Tutkimuspolku

Hyökkäyspolun hahmottamisessa voimme käyttää apuna Lockheed Martinin Cyber Kill Chain mallia. (Kuvio 12)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, viiva

Kuvaus luotu automaattisesti

Kuvio 12. Hyökkäyspolku

# Auditointi

Aloitetaan ympäristön auditoiminen tarkastelemalla Nessus skannaus tuloksia, josta löytyy 4 keskitason haavoittuvuutta.

Suoritimme ympäristöön myös verkon skannauksia työkaluilla kuten nmap. Tutkimme apachen, mysql ja wordpressin versioiden tunnettuja haavoittuvuuksia Nist NVD (National Vulnerability database) tietokannasta.

Ympäristön suurimpina uhkina voimme pitää vanhentuneita järjestelmiä. Niissä on paljon tiedossa olevia heikkouksia, joita hyökkääjät voivat käyttää helposti hyväkseen. Järjestelmässä ei myöskään ole käytössä kaksivaiheista tunnistautumista, mikä helpottaa hyökkääjän toimia.

Kybereon Intraan kirjautuessa olemassa olevilla tunnuksilla, kuten admin, ja väärän salasanan syöttämällä kerrotaan, että admin käyttäjä löytyy, mutta salasana on väärä. Yrittäessä kirjautua tunnuksella, jota ei ole olemassa kirjautumisportaali kertoo, että käyttäjätunnus on väärä. Tämä on heikkous tietoturvassa, koska se antaa mahdolliselle hyökkääjälle tietoa olemassa olevista käyttäjistä. (Kuvio 13)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

Kuvio 13. Kirjautumislomakkeen heikkous

## Skannaukset

Aloitetaan tutkimalla palvelinta nmap -verkonhaistelutyökalulla. Löysimme ensimmäisellä skannauksella palvelimen avoimet portit 22, 80 ja 443. (Kuvio 14).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, muotoilu

Kuvaus luotu automaattisesti

Kuvio 14. Avoimet portit

Kun skannaamme parametrillä -A (agressive), saamme tietoon porteissa toimivat palvelut ja niiden versiot. Kuten Apache httpd 2.4.37 vuodelta 2018 ja WordPress 5.3 vuodelta 2019 (Kuvio 15). Näin vanhoissa versioissa on tunnettuja haavoittuvuuksia, joita hakkeri voi hyödyntää hyökkäyksessään.

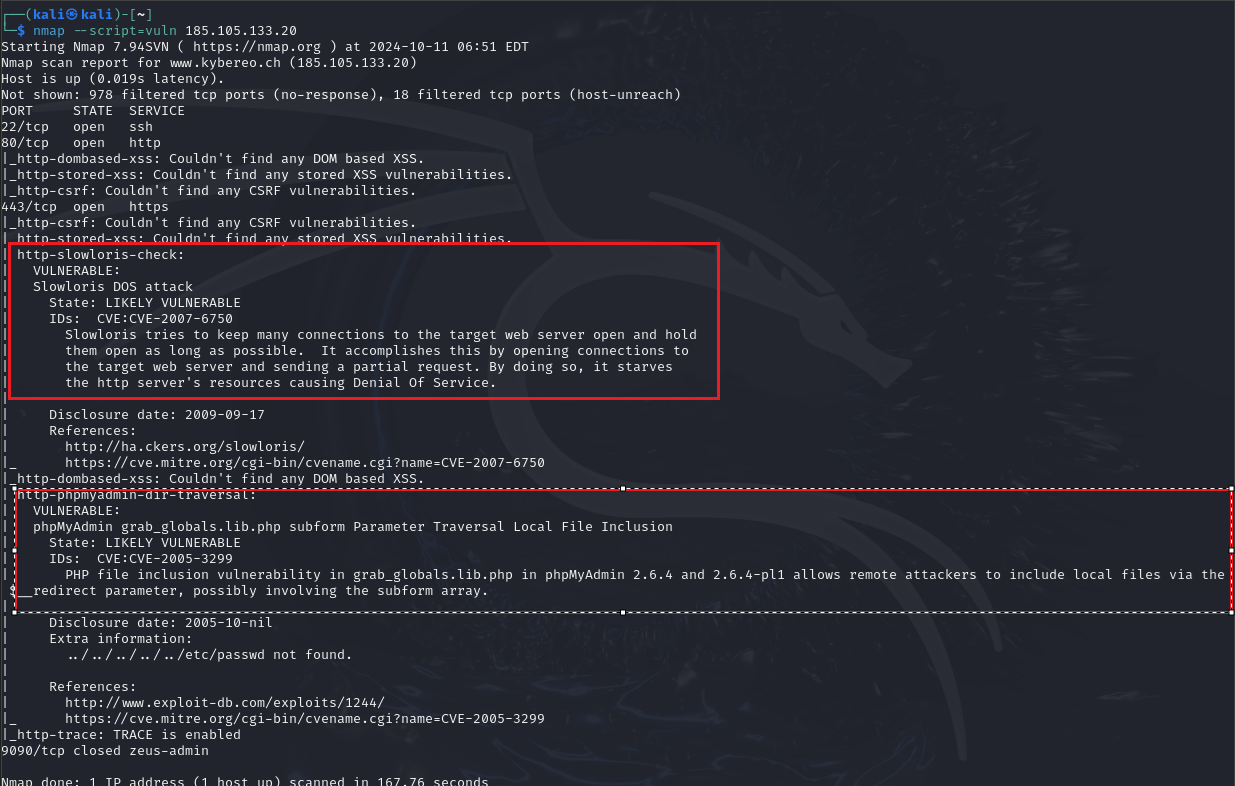
Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, ruokalista

Kuvaus luotu automaattisesti

Kuvio 15. Lisätietoa avoimista porteista

Nmapista löytyy ominaisuus etsiä tunnettuja haavoittuvuuksia. Työkalulla voidaan skannata kohteen IP-osoitteen kaikista porteista haavoittuvuuksia "--script vuln" parametrin avulla. Komento hyödyntää Nmapin oletus skriptejä etsiessään kohteesta tietoturvaheikkouksia. (How To Use Nmap for Vulnerability Scanning: Complete Tutorial. 2023)

Kuviossa 16 näkyy skannauksen tulokset.



Kuvio 16. Nmapin löytämät haavoittuvuudet

Skannattiin vielä erikseen kiinnostavat portit. Ensin portti 80 jossa pyörii apache palvelin. Portti 80 käyttää http protokollaa. (Kuvio 17)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 17. Portin 80 skannaus

Skannataan vielä porttia 443 jota apache myös käyttää, mutta 443 käyttää https protokollaa. (Kuvio 18)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 18. Portin 443 skannaus

### Haavoittuvuuksista

**Apache 2.4.37** versiosta havaittu 15 kriittistä haavoittuvuutta. **Wordpress 5.3** versiosta havaittu 8 kriittistä haavoittuvuutta.

Apache HTTP Server 2.4.37 haavoittuvuuksiin kuuluvat mm. CVE-2024-38476 ja CVE-2024-38474, nämä NVD (National Vulnerability Database) osumat liittyvät tietojen paljastamiseen, skriptien suorittamiseen ja sääntöjen muunteluun mod\_rewrite-moduulissa. Haavoittuvuus on kriittinen (CVSS-arvo 9.8). Apache haavoittuvuus CVE-2023-25690 HTTP-pyyntöjen käsittelyyn (smuggling), hyökkääjä voi tehdä omia (GET, POST ym.) pyyntöjään, ja ohittaa todennuksen. (Apache NVD. 2024)

WordPress 5.3 kriittisiä haavoittuvuuksia on 8 NVD:n mukaan, kuten CVE-2020-36326 haavoittuvuus, jota hyväksikäyttämällä hyökkääjä voi suorittaa haitallisia skriptejä ja löytää arkaluontoisia tietoja kohteesta. CVE-2020-36327 haavoittuvuuden avulla hyökkääjä voi manipuloida käyttäjätietoja ja saada järjestelmänvalvojan oikeudet. (Wordpress NVD. 2024)

**Mysql** **version 10.3.11-MariaDB** selvitimme palvelimella kuvion 19 mukaisesti. NVD:stä löytyi 1 kriittinen haavoittuvuus: CVE-2020-15180. Kyseinen haavoittuvuus altistaa tietokannan mielivaltaisten komentojen ajamiselle järjestelmässä koska wsrep\_sst\_method ei käsittele syötettä oikein.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 19. MariaDB versio

# Pohdinta

Harjoituksessa pääsimme tutustumaan Kybereoon kohdistuneeseen tietojenkalasteluhyökkäykseen. Tämä oli mielenkiintoista, koska tämän kaltaiset hyökkäykset ovat hyvin yleisiä, ja niitä tapahtuu jatkuvasti. Tapausta tutkiessa kävi hyvin nopeasti ilmi, että Kybereolla oli käytössä vanhentuneita palvelimia ja ohjelmistoja, joissa on paljon tunnettuja heikkouksia. Näitä hyödyntämällä hyökkääjä pääsi suhteellisen vaivattomasti luomaan itselleen admin-oikeuksilla olevan käyttäjän ja tekemään Kybereon sivuille oman alasivun, joka lähettää tunnukset hyökkääjälle. Käyttäjätunnusten vuotaminen olisi ollut estettävissä hyvällä sisäisellä koulutuksella, jossa käydään läpi kalasteluviestejä ja niihin liittyviä uhkia sekä oikeita tapoja reagoida niihin.

Tapausta tutkiessa opimme, että järjestelmien päivittämisellä on iso rooli kyberturvallisuuden hallinnassa. On myös tärkeää pitää henkilöstön kyberosaaminen ajan tasalla ja kouluttaa henkilöstöä jatkuvasti siitä, miten mahdollisiin kyberuhkiin tulee suhtautua ja reagoida. Tapauksen aikaleimoja tutkimalla huomasimme, että samankaltainen hyökkäys on nopea toteuttaa, joten niihin on tärkeää myös pystyä reagoimaan nopeasti.

Lähteet

Apache NVD (National Vulnerability Database). Apache 2.4.37 haku Keyword (text search): cpe:/a:apache:http\_server:2.4.37. Viitattu 11.10.2024. <https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&query=cpe%3A%2Fa%3Aapache%3Ahttp_server%3A2.4.37&search_type=all&isCpeNameSearch=false>

How To Use Nmap for Vulnerability Scanning: Complete Tutorial. Nmap ohjesivusto. 2023. Viitattu 14.10.2024. [https://www.esecurityplanet.com/networks/nmap-vulnerability-scanning-made-easy/](https://www.esecurityplanet.com/networks/nmap-vulnerability-scanning-made-easy/%20)

Wordpress NVD (National Vulnerability Database). Wordpress 5.3 haku Keyword (text search): cpe:/a:wordpress:wordpress:5.3. 2024. Viitattu 11.10.2024. <https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&query=cpe%3A%2Fa%3Awordpress%3Awordpress%3A5.3&search_type=all&isCpeNameSearch=false>