Tietoturvalisuuden 101

Nmapin käyttö on tärkeää opetella, sillä siihen pohjautuu ensimmäiset tiedot kyseisestä palvelusta ja siihen pohjautuu kaikki muu tutkimus! Käydään myös läpi Metasploittia, joka on tehty haavoituvuuksien löytämiseen ja hyväksikäyttämiseen. Metasploitissa on myös nmap tuki!

Nmap

Nmapissa on paljon asetuksia ja löydät kaikki ne komennolla "**nmap -h**", selitän ne asetukset ja ominaisuudet mitä itse käytän. Nmapissa komentojärjestys menee siten, että ensimmäiseksi tulee **nmap** ja sitten asetukset kuten esim **–A** ja lopuksi tulee osoite mitä haluat skannata. Tosin tätä järjestystä voi vaihtaa siten että laittaa nmap komennon jälkeen osoitteen ja lopuksi asetukset. Näet tästä esimerkkejä **Valmiita komento esimerkkejä** kohdasta!

Käydään eri asetuksia läpi mitä kannattaa käyttää ja niiden toiminnot!

Huom kun teet nmap skannausta pystyt painamaan space näppäintä terminaalissa, niin näet statuksen skannauksesta!

Automaattinen default skannaus

-A = Agression skannaus eli automaattinen skannaus, tämä käyttää default asetuksia ja scriptejä hyväksi että saa skannatua kohteen.

Palvelun olemassa oleva tarkistus aka ping

"Tämä osio ei ole pakollinen! Yleensä nmap normaalisti tarkistaa pingin avulla onko kohde ylhäällä, että kannattaa käyttää **–Pn** asetusta jos näyttää siltä että nmap katsoo että se palvelu on alhaalla vaikka todelisuudessa ei näin ole!"

-sn = Pelkkä ping skannaus. HUOM! ei sisällä portti skannausta! Eli älä laita portti ja skannaus tekniikka asetuksia

-Pn = on komento, joka kertoo nmapille että ping tai muita tarkistuksia ei tehdä, että onko palvelu ylhäällä vai ei. Tämä asetus voi olla tärkeä silloin kun palomuurista on kielletty ICMP echo eli normi ping.

-PE/PP/PM = ICMP echo asetuksia, normi icmp echo, timestamp ja netmask probit

Porttien valinta ja asetus

-p- = Tämä meinaa kaikkia portteja. Yleisesti haluat mahdollisimman paljon tietoa kohteen palveluista ja järjestelmistä, mutta tämä on hidas, etenkin UDP porttien skannaamiselle. TCP porttiskannaus saatta myös kestää kauan. Jos haluat nopeuttaa prosessia, pystyt määrittämään yksittäiset portit komenolla "**-p80, 443"**. On myös mahdollista käyttää yleisiä portteja komennolla "**--top-ports 1000**". Voit asettaa minkä numeron vain! esimerkiksi vaikka **--top-ports 500**.

-F = on nopea asetus, joka asettaa 100–250 porttia skannattavaksi.

Skannaus metodit

-sS =on skannaus asetus eli tapa millä vahvistat että portit on auki. Eli TCP SYN ACK. **OTA HUOMIOON** että kannattaa vaihdella tätä tekniikkaa koska jotkin palomuurit on voitu asettaa estämään näitä tekniikoita. Jos käytät **-sS** tekniikkaa ja sinulle tulee portti jonka versiossa lukee tcpwrapped, se voi kertoa että siellä on palomuuri eli IDS. Voit vaihtaa skannaus asetukseksi **–sT** joka on TCP CONNECT tai **–sA**. mutta itse olen käyttänyt yleisesti "**-sS, -sT ja -sA**". Muita en oikein ole tarvinnut, mutta kyllä niitäkin kannattaa joskus koittaa!

Huomioitko että jotkut metodit kuten –sS vaati root oikeudet, eli joudut käyttämään sudo komentoa!

Nyt hypätään syvemmälle näihin Skannaus metodeihin että ymmäretään miten nmap toimii!

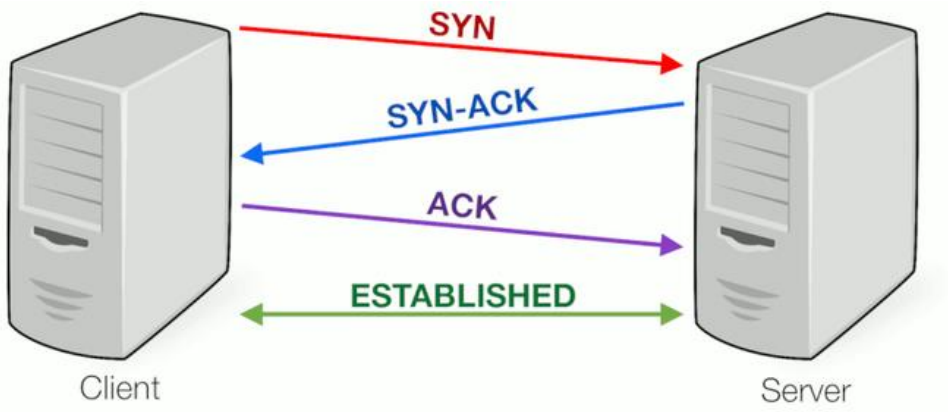
SYN ACK

-sS eli stealth skannaus on kolmen kättelyn prosessi koska se toimii tcp: llä eli se varmistaa että paketti menee perille, jos paketti ei mene perille se lähetetään uudelleen mutta sen sijaan että yhteys muodostuisi palveluun niin syn-ack vastauksen jälkeen nmappi lähettää reset flagin eikä yhdistä palveluun. Voitaisiin ajatella, että tämä olisi paljon hiljaisempi mutta nykyään ei, senpä takia kutsun sitä SYN-ACK skannaukseksi!

Tältä näyttää kun portti skannaus SYN ACK metodilla ei mennyt läpi jostain syystä. Esim. palomuurin takia:

```
PORT    STATE SERVICE    VERSION
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped
```

HUOM tämä on perusteita tcp toiminnasta. Tämä kättely tapahtuu aina mutta eri skannaus metodeissa se on vähän eri.



TCP connect

-sT skannaus tekniikka on melkein muuten sama kuin syn-ack paitsi että se suorittaa kolmen kättelyn loppuun ja yhdistää palvelimelle. Sen jälkeen nmap hakee sieltä bannerin ja merkitsee portin auki, jos nmap ei kuitenkaan pysty yhdistämään tai saa banneria niin kyseinen portti merkataan suljetuksi.

Tässä näkyy sama kohde mutta skannattuna TCP connect tavalla:

```
PORT     STATE SERVICE  VERSION
80/tcp   open  http     nginx
443/tcp  open  ssl/http nginx
554/tcp  open  rtsp?
1723/tcp open  pptp?
```

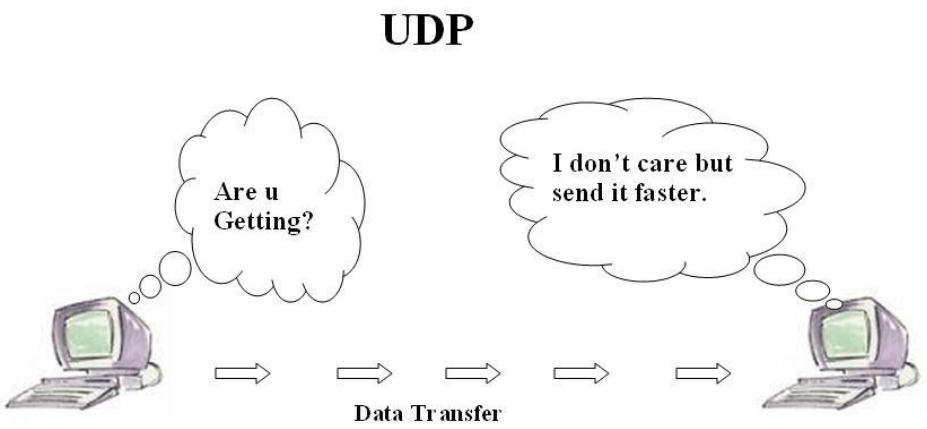
TCP ACK Scan

-sA sama kolmen kättely tapahtuu mutta tällä kertaa paketissa on pelkästään ACK flagi ja aukinaiset portit lähettävät RST paketin takaisin. Täten nmap lukee portin tilaksi unfiltered. Jos nmap ei saa RST vastausta tai hostiin ei saada yhteyttä niin täten portti luetaan filtered eli suodattu, samoin tapahtuu jos ICMP errori koodilla joko 1, 2, 3, 9, 10, 13 tapahtuu.

```
PORT    STATE    SERVICE VERSION
19/tcp  filtered chargen
25/tcp  filtered smtp
179/tcp filtered bgp
```

UDP Scan

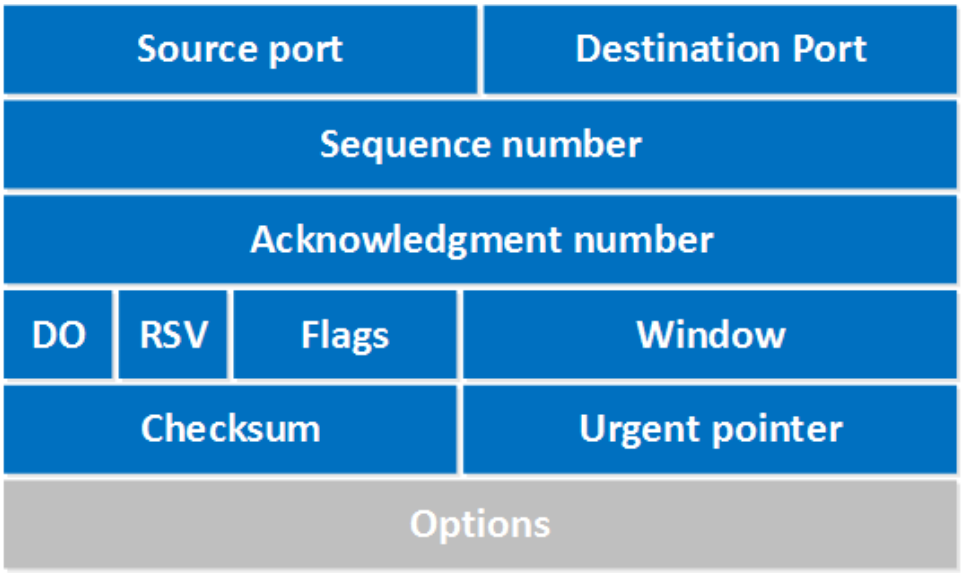
-sU On UDP protokolla joka toimii erillaila kuin tcp, sillä se ei toimi kolmen kättelyn periaatella vaan se lähettää pyynnön ja odottaa vastausta. Se ei tarkista että onko paketti mennyt perille vai ei ja siksi tämä on todella hidas!



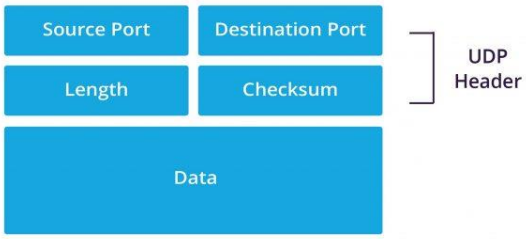
Parhain on vain kokeilla eri metodeita ja tapoja jotta saisi lisää tietoa siitä palvelusta.

TCP ja UDP pakettien sisältö

TCP ja UDP paketit ovat vähän erillaiset ja niistä löytyy samoja asioita mutta myös eri asioita kuten eri hedereitä aloitetaan TCP:stä. TCP paketin hederihin kuulu:



Kun taas UDP hedereihin kuulu:



Hederit ovat paketin tietoja mm mistä se on tulossa, minne menossa ja dataa, mutta esim tcp on paljon erillaisia hedereitä jotka määrittelevät jotakin tietoa siitä paketista!

Palvelun version havaitseminen

-sV = eli Service versionin havainnointi, joka lähettää tietylle portille probeja, jotka määrittelevät palvelun version tai palvelun. Koska jokaisessa palvelussa ja niiden versiossa on sormenjälki mistä nmap yrittää arvioida version siitä palvelusta, yleisesti tämä onnistuu aina mutta toisinaan et välttämättä saa selvitettyä palvelun versiota eli joudut tekemään manuaalisen tarkistuksen sivulle tai käyttäen netcat:tiä että saat joistain palveluista bannerin joka kertoo palvelun version.

Pystyt määrittämään myös nmapin tekemään enemmän probeja:

-sV --version-all

Tämä tarkoittaa sitä että se tarkistaa kaikki mahdolliset versiot mitkä se voi olla. jos muutat all komennosta light se tarkistelee vähemmän versioita!

-sV --version-light

Palomuurin/IDS väistely ja spoofaus asetukset

“Tämä on tärkeä osa koska suurin osa ids ja palomuureista tunnistaa portti skannereita. Nämä asetukset auttavat sinua tarkistamaan palomuurin säännöt ja jopa ohittamaan palomuureja!”

-f / --mtu = Tämä asetus määrittelee millä paketti paloitellaan ja kasataan. Jotkin palomuurit on voitu asettaa niin että se ei suodata paketteja jotka on palasina, tämä on kuitenkin nykyään harvinaista mutta voi olla mahdollista!

-D decoy1,decoy2 = Tämä asetus antaa määritellä monta spoofattua ip-osoitetta mitä nmap sitten käyttää, tämä on hyödyllinen koska sinua ei välttämättä palomuuri flagata liikenteen takia koska skannaus kulkeutuu muitten osotteista!

-S = Tämä asetus antaa sinun vaihtaa ip-osoitetta, tämä asetus on hyvä jos ids tai palomuuri on asetettu suodattamaan tiettyjä osoitteita!

-e = Tämä asetus antaa määritellä mitä fyysistä verkkokorttia haluat käyttää. HUOM voit tarvita tätä joissain asetuksissa!

-g/--source-port <portnum> = Tämä asetus antaa sinun asettaa lähde portin, eli mistä portista liikenne lähtee. Tämä on hyvä silloin kun palomuuri on asetettu väärin suodattamaan portteja vain tietyistä porteista. "Omalla kokemuksella koitan aina käyttää domain porttia eli 53 jos on palomuuri meinaa tämä auttaa yleensä että näkee ne palvelut ;D"

Tein normi syn-ack skannin ja vaihdoin lähde portin 53 ja tulokset on:

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx
```

Tämä tulos ei ollut ihan pelkässä normi syn-ack skannissa koska sielä luki tcpwarped mutta kun vaihdettiin lähde portti se kertoikin siitä palvelusta enemmän!

HUOM Tässä näkee että tietoturvalisuudessa testataan ja kokeilaan erillaisia tapoja rikkoa asioita kunhan on lupa ja tietää mitä tekee, ettei aiheuta mitään ongelmia semmoisille osapuollile tai palveluihin jotka siihen eivät kuulu!

--proxies = Vie liikennettä läpi HTTP/SOCKS4 proxies, tämä asetus auttaa sinun ohjaaman liikennettä jonkin Proxy serverien läpi.

Huom Proxy serverien kautta ohjaaminen on melkein sama asia kun decoy, jopa parempi!

--data-length = Valitse pakettien koko. Tämä asetus voi huijata palomuuria joka on asetettu tietyn paketin kooksi esim. 24bit joka on yleinen nmapille.

--ip-options <options> = Lähetä paketti eri ip asetuksilla.

--spoof-mac = Spooffaa mac osoitteen joko oma valintaisella mac osoitteella tai yhtiön nimellä. Jos jätät nollaksi tämä randomoi sen.

--badsum = Lähettää paketin huonolla hashsummilla niin udp kuin tcp protokollissa, tämä saatta myös toimia joihinkin palomuureihin!

Raportointi

-oA = Luo raporttipohjat kolmella eri pää formaatilla.

-oN = Normaali raportti.

-oX = xml formaatin raportti.

HUOM laita raportin nimi näiden asetusten jälkeen eli jätä tämä mieluiten perälle!

Nopeus ja muut tiedot plus debug

-T 1-5 = Tämä asetus määrittelee portti skannaavuuden nopeutta. Yleisesti se on aina –T4 mutta sen pystyy vaihtamaan, siksi että -T4 on todella aggressiivinen ja käyttää paljon kaistaa joten palomuuri voi estää tämän. Joten on hyvä muistaa käyttää -T4 alaspäin yleisissä palveluissa.

Huom -T5 asetus voi aiheuttaa jopa palvelunesto hyökkäyksen heikkoihin järjestelmiin!

-v 1-5 = Verbosity,tämä kertoo skannauksesta paljon enemmän. Tämä vaihtoehto on yleensä silloin paras kun pitää nähdä mitä takana tapahtuu jos tulokset eivät ole sitä mitä odotit.

--packet-trace = Tällä asetuksella jäljität kaikki paketit ja vastaukset. Tämä on siitä hyödyllinen että pystyt näkemään vastaukset ja pystyt niistä näkemään jos siellä on palomuuri joka häiritsee sinua tehtävässä. Yleisesti pelkkä debug työkalu.

-O = Käyttöjärjestelmän arviointi asetus, tämä yrittää arvata mikä käyttöjärjestelmä on kyseessä. HUOM ei kannata luottaa 100% koska kyseessä on pelkkä arvaus.

Scriptit

Nmapilla on script engine, joka mahdollistaa uusia ominaisuuksia ja automaatioita nmapille!

-sC = suorittaa perus scriptit nmapista. HUOM suorittaa samoja scriptejä kuin ns. automaattinen skannaus!

--script = Tällä asetuksella saat valittua joko scripti kategorian, yhden scriptin tai useamman, kategoriat ovat:

Discovery = Käyttää skriptejä jotka auttavat sinua löytämään enemmän tietoa palvelusta.

Dos = Käyttää skriptejä jotka voivat myös ddos palvelun.

Exploit = Käyttää skriptejä jokka voivat käyttää erillaisia haavoituvuuksia.

Intrusive = Yrittää saada kaiken tiedon.

Safe = Turvalliset skriptit jotka ei kaada palvelua välttämättä.

Vuln = Haavoituvuus skriptit kertoo jos havaitsee haavoituvuuksia mutta tämä on tosi epäluotettava!

HUOM! Varo mitä scriptejä käytät,koska joktut pyrkivät kaataman/murtautumaan sivulle tai palveluihin! Ne voivat olla äänekkäitä ja jäävät Log tiedostoihin. Parhaat kategoriat ovat Vuln ja Discovery!

Valmiita komento esimerkkejä

HUOM et voi käyttää kahta tcp skannaus metodia samaan aikaan. Esim. -sS ja –sA.

Muistathan että kohteen ip-osoitteen voi laittaa joko nmap komennon jälkeen heti tai asetuksien jälkeen. Saat itse päättää mutta ainoa poikkeus on jos teet raportin, tällöin raportti asetus pitää olla lopussa sillä sinun tarvitsee kertoa nmapille raportin tiedoston nimen lopuksi.

nmap –A 192.168.1.1 = Tämä on automaattisen skannauksen esimerkki!

```
┌──(eetu㉿kali-workstation)-[~]
└─$ nmap -A 192.168.101.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 18:22 EEST
Nmap scan report for dna.wifi (192.168.101.1)
Host is up (0.0058s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT    STATE    SERVICE   VERSION
21/tcp  filtered ftp
22/tcp  open     ssh       Dropbear sshd 2017.75 (protocol 2.0)
23/tcp  filtered telnet
53/tcp  open     domain    (unknown banner: DNA)
```

sudo nmap –sS –p- -sV 192.168.1.1 = Tämä käyttää syn ack skannaus metodia, kaikki portit ja version selvitys.

```
┌──(eetu㉿kali-workstation)-[~]
└─$ sudo nmap -sS -p- -sV 192.168.101.1
[sudo] password for eetu:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 18:26 EEST
Nmap scan report for dna.wifi (192.168.101.1)
Host is up (0.041s latency).
Not shown: 65524 closed tcp ports (reset)
PORT      STATE    SERVICE     VERSION
21/tcp    filtered ftp
22/tcp    open     ssh         Dropbear sshd 2017.75 (protocol 2.0)
23/tcp    filtered telnet
53/tcp    open     domain      (unknown banner: DNA)
80/tcp    open     ssl/http
443/tcp   open     ssl/https
27998/tcp open     ssl/unknown
37443/tcp open     upnp        Portable SDK for UPnP devices 1.6.25 (Linux 4.4.197; UPnP 1.0)
37444/tcp open     tcpwrapped
49652/tcp open     upnp        Portable SDK for UPnP devices 1.6.25 (Linux 4.4.197; UPnP 1.0)
49653/tcp open     tcpwrapped
```

sudo nmap –sS –sU -sV –top-ports 800 192.168.1.1 = Tämä käyttää syn ack ja udp skannaus metodeita, version selvitys ja top 800 porttia.

```
┌──(eetu㉿kali-workstation)-[~]
└─$ sudo nmap -sS -sU -sV -top-ports 800 192.168.101.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 18:30 EEST
Stats: 0:05:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 37.95% done; ETC: 18:44 (0:08:14 remaining)
Nmap scan report for dna.wifi (192.168.101.1)
Host is up (0.0012s latency).
Not shown: 797 closed udp ports (port-unreach), 794 closed tcp ports (reset)
PORT     STATE         SERVICE   VERSION
21/tcp   filtered      ftp
22/tcp   open          ssh       Dropbear sshd 2017.75 (protocol 2.0)
23/tcp   filtered      telnet
53/tcp   open          domain    (unknown banner: DNA)
80/tcp   open          ssl/http
443/tcp  open          ssl/https
53/udp   open          domain    (unknown banner: DNA)
67/udp   open|filtered dhcps
1900/udp open|filtered upnp
4 services unrecognized despite returning data. If you know the service/version, please submit
```

nmap –sT -p- -sV 192.168.1.1 = tämä komento tekee skannauksen Tcp Connect metodilla, kaikki portit, version havaitseminen

```
┌──(eetu㉿kali-workstation)-[~]
└─$ nmap -sT -p- -sV 192.168.101.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 18:36 EEST
Nmap scan report for dna.wifi (192.168.101.1)
Host is up (0.043s latency).
Not shown: 65524 closed tcp ports (conn-refused)
PORT      STATE    SERVICE     VERSION
21/tcp    filtered ftp
22/tcp    open     ssh         Dropbear sshd 2017.75 (protocol 2.0)
23/tcp    filtered telnet
53/tcp    open     domain      (unknown banner: DNA)
80/tcp    open     ssl/http
443/tcp   open     ssl/https
27998/tcp open     ssl/unknown
37443/tcp open     upnp        Portable SDK for UPnP devices 1.6.25 (Linux 4.4.197; UPnP 1.0)
37444/tcp open     tcpwrapped
49652/tcp open     upnp        Portable SDK for UPnP devices 1.6.25 (Linux 4.4.197; UPnP 1.0)
49653/tcp open     tcpwrapped
4 services unrecognized despite returning data. If you know the service/version, please submit
```

sudo nmap –sS –Pn –sV 192.168.1.1 -oN localenum = Syn ack metodilla, ei tarkisteta onko hosti ylhäällä, version tarkistus, lopuksi nmap tekee raportin nimeltä localenum

```
┌──(eetu㉿kali-workstation)-[~]
└─$ sudo nmap -sS -Pn -sV 192.168.101.1 -oN localenum
[sudo] password for eetu:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 18:39 EEST
Nmap scan report for dna.wifi (192.168.101.1)
Host is up (0.0061s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE    SERVICE   VERSION
21/tcp  filtered ftp
22/tcp  open     ssh       Dropbear sshd 2017.75 (protocol 2.0)
23/tcp  filtered telnet
53/tcp  open     domain    (unknown banner: DNA)
80/tcp  open     ssl/http
443/tcp open     ssl/https
3 services unrecognized despite returning data. If you know the service/version, please submit
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-TCP:V=7.92%I=7%D=6/3%Time=629A2B2B%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,30,"\0\.\0\x06\x81\x80\0\x01\0\x01\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\x01>c\0\x04\x03DNA");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
```

sudo nmap –sS –source-port 53 –sV –p- 192.168.1.1 = metodina on syn ack, lähde porttina 53, versio tarkistus, kaikki portit

```
┌──(eetu㉿kali-workstation)-[~]
└─$ sudo nmap -sS -source-port 53 -sV -p- 192.168.101.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-03 18:41 EEST
Nmap scan report for dna.wifi (192.168.101.1)
Host is up (0.027s latency).
Not shown: 65524 closed tcp ports (reset)
PORT      STATE    SERVICE     VERSION
21/tcp    filtered ftp
22/tcp    open     ssh         Dropbear sshd 2017.75 (protocol 2.0)
23/tcp    filtered telnet
53/tcp    open     domain      (unknown banner: DNA)
80/tcp    open     ssl/http
443/tcp   open     ssl/https
27998/tcp open     ssl/unknown
37443/tcp open     upnp        Portable SDK for UPnP devices 1.6.25 (Linux 4.4.197; UPnP 1.0)
37444/tcp open     tcpwrapped
49652/tcp open     upnp        Portable SDK for UPnP devices 1.6.25 (Linux 4.4.197; UPnP 1.0)
49653/tcp open     tcpwrapped
4 services unrecognized despite returning data. If you know the service/version, please submit
```

Tietotuvallisuuden ajattelutapa

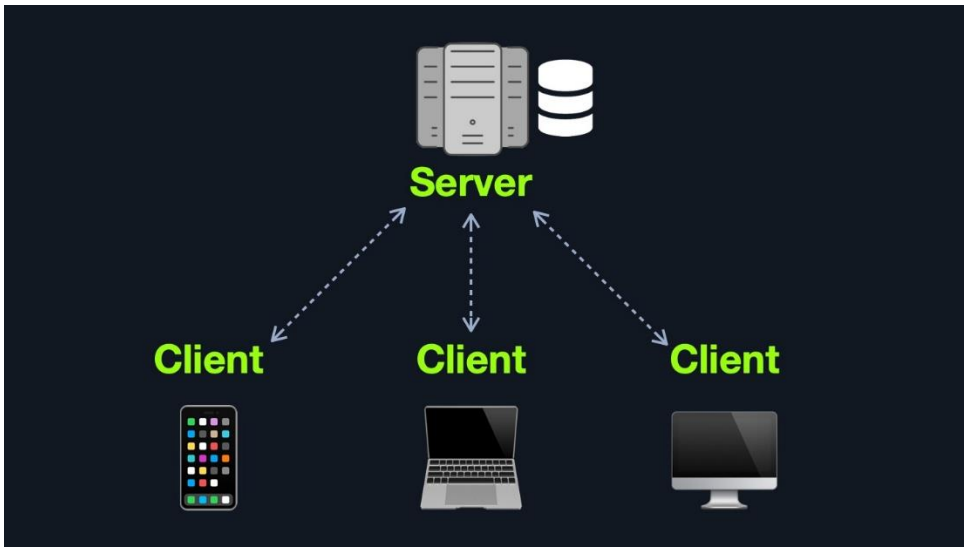
Ajattelutapa on isoin työkalu mitä voi olla, koska kaikki palvelut ovat erilaisia. Sinun tarvitsee kuitenkin tietää mihin keskittyä ja mihin ei. Yritykset voivat olla tosi isoja joten sinunkin tutkimus alue suurenee sen mukaisesti kuinka suuri yritys on tai millainen yritys on kyseessä. Enkä sano sitä että olisi tiettyjä alueita mitä ei kannata edes tutkia vaan se että haluan ohjata sinua katsomaan niihin yleisimpiin paikkoihin mistä saatta löytyä haavoittuvuuksia tai yrityksen tekemiä virheitä.

Yritykset voivat myös näyttää pieniltä mutta oikeasti tutkimus alue on isompi. Tämä on siitä syystä että moni ajattelee että he tekevät pelkän nmapin ja etsivät haavoittuvuuksia versio numeroiden perusteella. Näin ei kuitenkaan ole koska tietotuvallisuudessa ei ole kyse siitä että käyttäisit pelkästään muiden löytämiä haavoittuvuuksia. Tässä vaiheessa huomaatkin että alue on suurentunut koska käyt kaikki palvelut läpi source koodista, pyyntöihin ja tapaa miten palvelin käsittelee liikenettä. Se tuntuu isolta työltä mutta minun ei ole tarkoitus opettaa mten löydät uusia haavoituvuuksia vaan tunnistamaan olemassa olevat, koska siihen menee reilusti monta vuotta jos haluat syventyä asiaan!

Uudella haavoittuvuudella Tarkoitan sitä, että löydät jostain palvelusta haavoittuvuuden mitä ei ole vielä tunnistettu. Niitä sanotaan zerodayexploiteiksi.

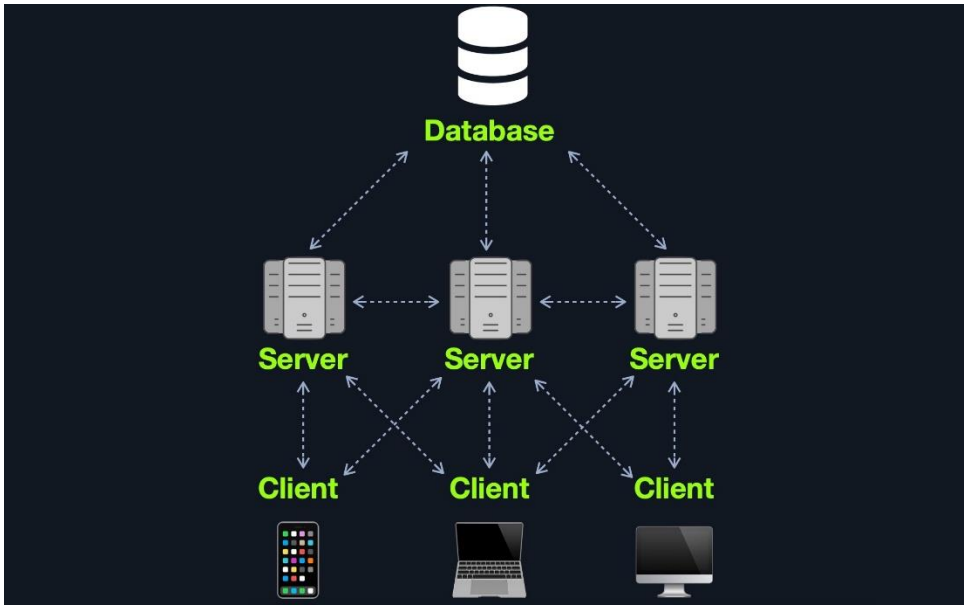
Seuraavaksi kerron yleisiä toteutus tapoja näihin palveluihin:

Tässä on yleinen toteutustapa web-palvelimille, tässä toteutuksessa nähdään se että yksi serveri käsittelee kaikkea mitä web-palvelin tarvitsee mm. tietokantoja, web engine jne. Tämä on huono toteutustapa jos mietitään isoa yhtiötä koska yhteen palveluun murtautuminen aiheuttaisi paljon tuhoa koska kaikki on yhdellä palvelimella!

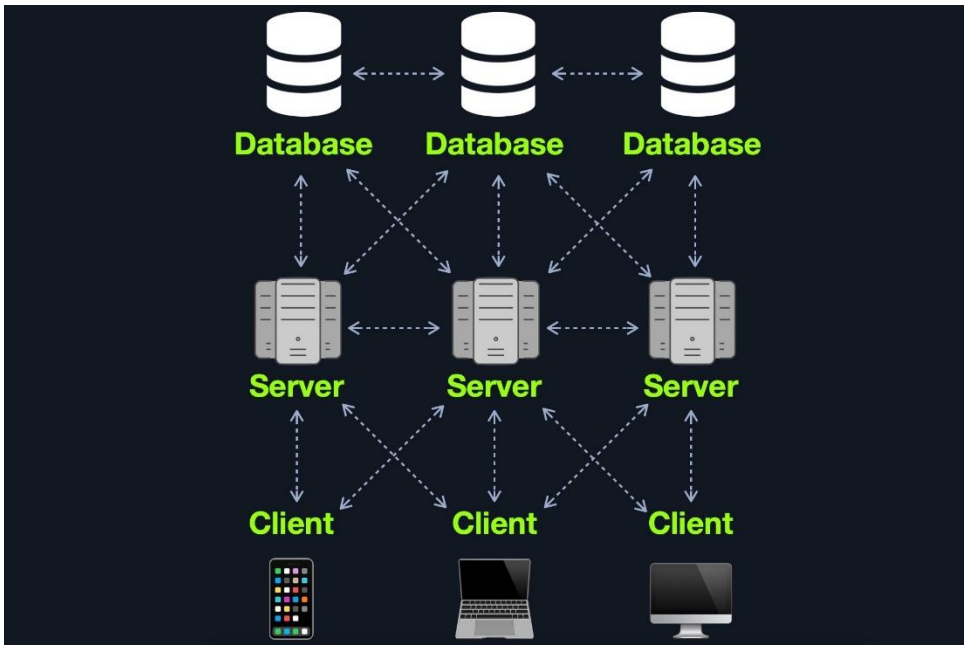


Tämä toinen arkkitehtuuri on paljon turvallisempi ja on yleisesti aika monella yhtiöllä käytössä, mutta virtuaalimuodossa. Sillä tarkoitetaan siis virtuaalikoneita, joista on luotu 4 serveriä: kolme niistä ylläpitää sivua ja ja yksi serveri ylläpitää tietokantaa. Yhden palvelun kompromissi ei aiheuta tuhoa niin paljon kun edellisessä arkkitehtuurissa.

Mutta ota huomioon että yleensä tässä on käytössä loadbalancer joka jakaa liikennettä kolmen serverin välillä. Tämä saatta aiheuttaa hämmennystä tutkimuksessa, sillä voi olla että noista kolmesta palvelimesta vain yksi on haavoittuvainen johonkin hyökkäykseen!



Tämä on kaikista parhain arkkitehtuuri, mutta tässä huomataan, että alue on paljon isompi mikä yleensä tarkoittaa sitä, että mahdollisuus haavoittuvuuksien löydöstä kasvaa!

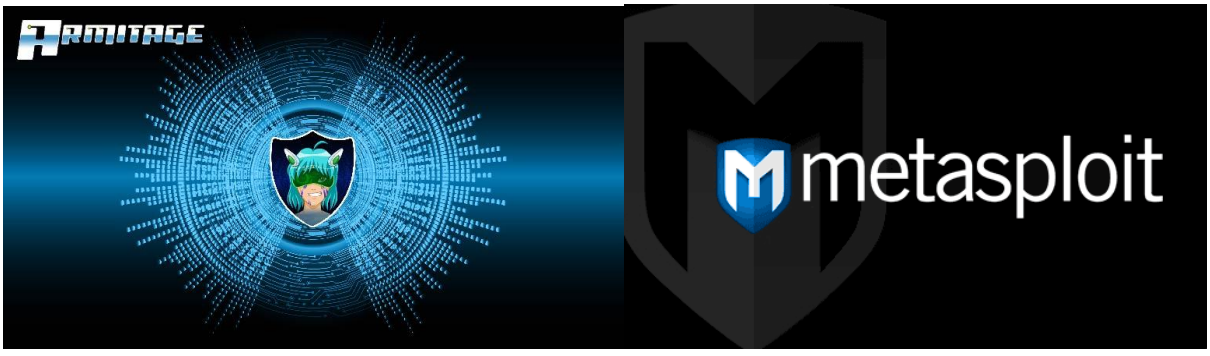


HUOM on siis tärkeää selvittää aluetta mitä tutkia ja tämä onnistuu nmapilla helposti, monet tekee virheen siinä että ei osaa selvittää aluetta mitä tutkia!

Ekstraa nmapista

Nmappi on kehitetty noin 24 vuotta sitten ja se on tähän päivään saakka yksi yleisimmistä työkaluista tietotuvallisuudessa. tästä saamme kiittää sen kehittäjää Gordon Lyonia. nmappi on siis yksi parhaimmista työkaluista mitä voit vain tarvita syystä että siihen perustuu tuhansien eri ihmisten tietotuvallisuus tutkimukset, koska tällä kartoitetaan porttien ja niiden takana olevia palveluita!

Pystyt myös ottamaan lisää selvää nmapin omista sivuista täältä!



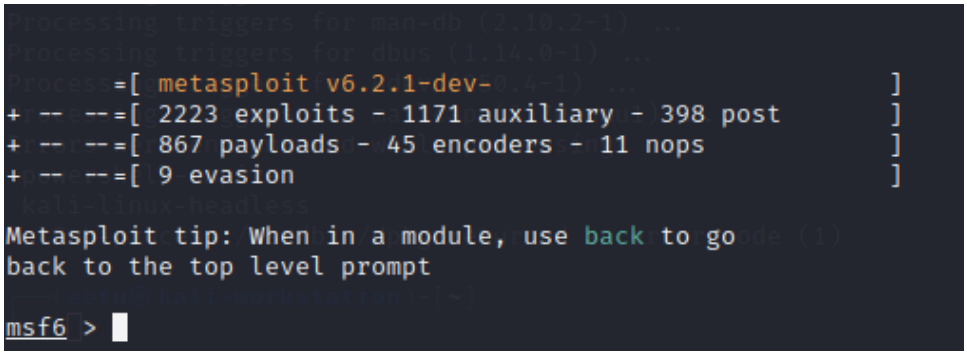
Metasploit

Metasploit on työkalu mikä on suunniteltu auttamaan tietotuvallisuudessa toimivia henkilöitä. Tämä työkalu sisältää mm. exploitteja, skannereita, payloadeja ja muuta. käyttöliittymästä on 2 versioa, toinen on terminaali pohjainen msfconsole ja toinen on armitage joka on tehty GUI versiona metasploitista!

HUOM Armitage vaati metasploitin asentamisen järjestelmään sillä se käyttää metasploitin databasea kommunikaatiossa!

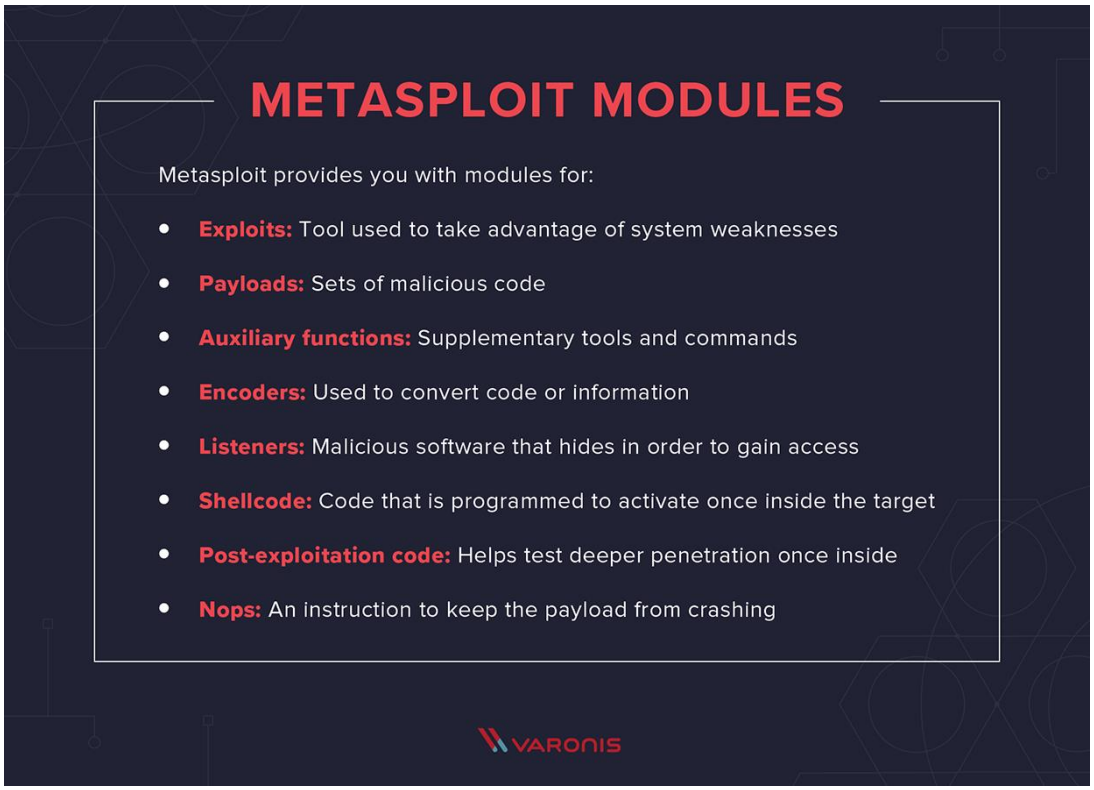
Metasploitin käyttö

Ensiksi tarvitsee ymmärtää metasploittia ja sen toiminta periaatteita. Metasploitin saa terminaalissa avattua **msfconsole** komennolla. olet nyt metasploit konsolessa ja pystyt ohjaaman sillä metasploittia kuten esim kirjotamalla **help** saat apua komennoista!



Metasploitissa ja armitagessa on moduuleita ja näillä tarkoitetaan ominaisuuksia millä pystyy tekemään erillaisia asioita, kuten testamaan onko jokin palvelu haavoittuvainen tai vaikka onko mahdollisuus käyttää skannereita löytämään tietoa lisää eri palveluista!

Moduulit



Metasploitin moduuleihin kuulu:

Exploits = Nämä ovat haavoituvuuksia mitä metasploit voi käyttää hyväksi.

Payloads = Nämä ovat ns. Shellejä, mitkä mahdollistavat sinun saamaan terminaalin hyökättävän kohteen koneeseen esim Meterpreter shelli.

Auxiliary = Näitä kutsutaan skannereiksi. Näiden avulla voi saada lisätietoa palveluista.

Encoders = Näillä pystyt piilottamaan shell koodeja eli puhutaan obfuscatesta. Tämän tarkoitus on sekoittaa koodia niin että ihminen tai antivirus softat ei löytäisi kyseistä ohjelmaa järjestelmästä. Tai se siivoaa shell koodia niin että sinne ei tule huonoja bittejä esim x01.

Listeners = Näillä pystyy luomaan kuuntelioita jota tarvitaan kun luot shelliä ja se suoritetaan kohteen koneessa.

Shellcode = Shellikoodi on koodi mikä suoritetaan kohteen koneessa ja se luo shellin siihen koneesen mistä se yhdistää kuunteliaan jota sinä hallitset.

Post-exploitation = Ovat moduuleita, jotka koittavat auttaa sinua kun pääset Shelliin esim. oikeuksien eskalointia.

Nops = Näillä yritetään estää payloadin kaatumisen eli siivotaan payloadia.

Payloads

Payloadit ovat tapoja miten shelli saa sinun kuuntelijaan yhteyden, payloadilla on 3 eri kategoriaa ne ovat:

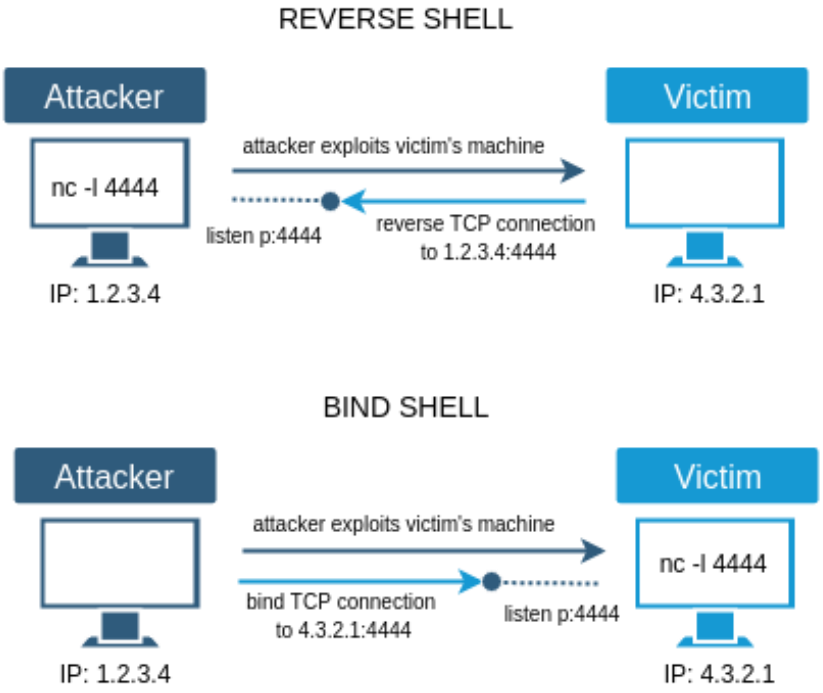
Singles = Ovat itsenäisiä ja ne voivat toimia järjestelmässä käyttäjänä tai exe tiedostona!

Stagers = Asettavat nettiyhteyden hyökkääjän ja kohteen välille. Nämä ovat suuniteltu todella pieniksi ja tasaisiksi, ettei payload kaadu. Mutta on todella vaikeaa tehdä pieni ja vakaa stager payload_joten pystyt valitsemaan kahdesta stagersista jotka ovat Windows NX ja NO-NX stagers.

Stages = Ovat payloadin komponentteja jotka ladataan stage moduuleina. Tämä tarkoittaa sitä että se saa lisäominaisuuksia kuten Meterpreter, vnc injektio ja iphone “ipwn” shelli.

Stages:it ovat hyviä siitä että pystyt lataaman infektion jälkeen siihen lisäominaisuuksia niin paljon kun haluat. Miinuksena on se että lisäominaisuuksien lataaminen voi näkyä log tiedostoissa!

Payload määrittelee miten kyseinen shelli saadaan. Reverse tcp shellin toiminta periaate on se, että hyökkääjä käyttää haavoittuvuutta joka saa kohteen koneen yhdistämään hyökkääjän koneesen. Bind shellissä hyökkääjä vaihtaa sen niin, että kohteen kone kuuntelee ja hyökkääjän kone yhdistää kohteen koneesen joka suorittaa komennot.



HUOM! Reverse shell on parempi kuin bind shell, koska kohde yhdistää sinun koneeseen, silloin palomuuri ei estä suurinta osaa liikennettä mikä menee ulkoverkkoon. Kun taas bind shellissä voi olla ongelmana palomuuri joka estää sinua yhdistämästä kohteesen!

Metasploitin moduulien etsiminen

Metasploitin moduuleita pystyy etsimään search komenolla esim:

```
msf6 > search apache 2.3

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                  2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure
   1   exploit/multi/http/apache_jetspeed_file_upload        2016-03-06       manual     No     Apache Jetspeed Arbitrary File Upl
   2   exploit/multi/http/struts_default_action_mapper       2013-07-02       excellent  Yes    Apache Struts 2 DefaultActionMappe
   3   exploit/multi/http/struts_dev_mode                    2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGN
   4   exploit/multi/http/struts2_namespace_ognl             2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect
   5   exploit/multi/http/struts2_rest_xstream               2017-09-05       excellent  Yes    Apache Struts 2 REST Plugin XStrea
   6   exploit/multi/http/struts2_code_exec_showcase         2017-07-07       excellent  Yes    Apache Struts 2 Struts 1 Plugin Sh
   7   exploit/multi/http/struts_code_exec_classloader       2014-03-06       manual     No     Apache Struts ClassLoader Manipula
   8   exploit/multi/http/struts_dmi_exec                    2016-04-27       excellent  Yes    Apache Struts Dynamic Method Invoc
   9   exploit/multi/http/struts2_content_type_ognl          2017-03-07       excellent  Yes    Apache Struts Jakarta Multipart Pa
   10  exploit/multi/http/struts_code_exec_parameters        2011-10-01       excellent  Yes    Apache Struts ParametersIntercepto
   11  exploit/multi/http/struts_dmi_rest_exec               2016-06-01       excellent  Yes    Apache Struts REST Plugin With Dyn
   12  exploit/multi/http/struts_include_params              2013-05-24       great      Yes    Apache Struts includeParams Remote
   13  exploit/unix/webapp/wp_phpmailer_host_header          2017-05-03       average    Yes    WordPress PHPMailer Host Header Co
   14  exploit/unix/webapp/jquery_file_upload                2018-10-09       excellent  Yes    blueimp's jQuery (Arbitrary) File

Interact with a module by name or index. For example info 14, use 14 or use exploit/unix/webapp/jquery_file_upload
```

Tässä esimerkissä haettiin apache 2.3 moduuleita ja täältä löytyi exploiteja. Pystyt myös etsimään mitä vain moduuleita kuten skannereita komenolla search scanner!

Metasploitin moduulien käyttö

Moduulien käyttäminen on tehty helpoksi. Kun etsit jotain moduulia, pystyt pistämään komennon use ja numeron missä kohdassa sinun haluamasi moduuli on. Esim haluan valita: exploit/linux/smtp/apache_james_exec niin laitan sen numeron, joka on 0.

```
msf6 > use 0
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/smtp/apache_james_exec) >
```

Seuraavaksi haluamme asettaa asetuksia tähän moduulin, asetukset saa esille show options komenolla näin:

```
msf6 exploit(linux/smtp/apache_james_exec) > show options

Module options (exploit/linux/smtp/apache_james_exec):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   ADMINPORT   4555             yes       Port for James remote administration tool
   PASSWORD    root             yes       Root password for James remote administra
   POP3PORT    110              no        Port for POP3 Apache James Service
   RHOSTS                       yes       The target host(s), see https://github.co
   RPORT       25               yes       The target port (TCP)
   SRVHOST     0.0.0.0          yes       The local host or network interface to li
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default
   URIPATH                      no        The URI to use for this exploit (default
   USERNAME    root             yes       Root username for James remote administra


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.101.100  yes       The listen address (an interface may be speci
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Cron
```

Back komenolla pääset pois moduulista. Huomioi myös että kaikissa missä on yes Required on pakko määrittää!

Miten asetukset määritetään? Ennen kun määritetään asetuksia kerron pari asiaa mitkä kannattaa pitää mielessä ja tämä koskee kaikkia moduuleita metasploitissa. RHOST tarkoittaa sitä että siihen laitetaan kohteen osoite, kun taas RPORT on portti mitä metasploit käyttää. LHOST/LPORT tarkoittaa omaa osoitetta esim omaa julkista osoitetta tai yksityistä osoitetta ja sitten lopuksi portti mitä laite kuuntelee!

Asetukset määritetään siten että ekaksi tulee set komento, sitten asetuksen nimi ja lopuksi arvo miksi se halutaan muuttaa esimerkiksi: set rhost 192.168.1.1

```
msf6 exploit(linux/smtp/apache_james_exec) > set rhost 192.168.1.1
rhost ⇒ 192.168.1.1
```

muista myös että metasploittia ei kiinosta onko isot kirjaimet käytössä vai ei, kun asettaa asetuksia!

Seuraavaksi kun olet asettanut moduulin asetukset, pystyt suorittamaan moduulin run tai exploit komenolla:

```
msf6 exploit(linux/smtp/apache_james_exec) > run
[*] Started reverse TCP handler on 192.168.101.100:4444
[-] 192.168.1.1:25 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.1.1:4555) timed out.
[-] 192.168.1.1:25 - Failed to remove payload message for user '../../../../../../../../etc/cron.d' with password 'FhvyGkRffC
[-] 192.168.1.1:25 - Exploit failed: The connection with (192.168.1.1:4555) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/smtp/apache_james_exec) >
```

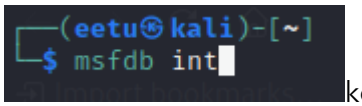
Minulle tuli joissain kohdissa fail koska kohdetta ei ole olemassakaan!

Pystyt tarkistamaan onko kohde haavoittuvainen kyseiselle exploitille, komenolla **check** kun olet asettanut asetukset!

HUOM pystyt metasploitin eri valikoissa kirjoittamaan **help** ja se kertoo sinulle komentoja mitä voit käyttää.

Metasploitin database

Tämä ominaisuus on extraa, mutta se helpottaa tulevaisuudessa sinun metasploitin käyttöä. Tämä databse tuki mahdollistaa nmapin käytön metasploitissa, auttaa sinua löytämään haavoituvuuksia ja automatisoi joitakin metasploitin toimintoja. Se myös auttaa sinua säästämään projektia pidemmäksi ajaksi ja niitä kutsutaan workspaceiksi metasploitissa!

Metasploitin databsen saa luotua ja valmisteltua 

komenolla! Kun olet saanut asetettua databsen, muista salasana ja käyttäjä minkä laitat siihen sillä tarvitse niitä kun yhdistät siihen.

```
MSF web service is no longer running
No data at /home/eetu/.msf4/db, doing nothing
Creating database at /home/eetu/.msf4/db
Starting database at /home/eetu/.msf4/db ... success
Creating database users
Writing client authentication configuration file /home/eetu/.msf4/db/pg_hba.conf
Stopping database at /home/eetu/.msf4/db
Starting database at /home/eetu/.msf4/db ... success
Creating initial database schema
================================================================

================================================================
Running the 'reinit' command for the webservice:
MSF web service is no longer running
[?] Initial MSF web service account username? [eetu]:
[?] Initial MSF web service account password? (Leave blank for random password):
Generating SSL key and certificate for MSF web service
Attempting to start MSF web service ...
```

pystyt käynnistämään databasen komenolla **msfdb start**, msfconsolessa kirjoita **db_connect (käyttäjä)@(salasana)**, pääset sen jälkeen näkemään databasen statuksen komenolla **db_status** tai normaalissa terminaalissa **msfdb status**.

```
msf6 > db_status
[*] Connected to [redacted]. Connection type: postgresql. Connection name: loc
```

Kun näet tämän, olet yhdistettynä metasploitin databseen. Seuraavaksi pystyt luomaan workspacen projektille komenolla **workspace –a** (projektin nimi),

```
msf6 > workspace -a oma projekti
[*] Added workspace: oma
[*] Added workspace: projekti
[*] Workspace: projekti
```

pystyt myös listaaman kaikki workspacet komenolla **workspace –l**

```
msf6 > workspace -l
  default
  oma
* projekti
```

Huom! jos pistät välin (spacebar), luot kaksi eri databsea! eli käytä viivaa tai pistettä nimien erittelyyn!

Pystyt myös poistamaan workspacen komenolla **workspace –d** (Projektin nimi)!

```
msf6 > workspace -d oma
[*] Deleted workspace: oma
```

Metasploit databse nmap integrointi

Metasploitissa on nmap tuki joka tarkoittaa sitä että pystyt msfconsolen sisällä tekemään nmap skannauksen ja lajitella tulokset johonkin workspaceen. Katsotaan miten tämä käytänössä toimii!

Huom! Ilman metasploitin databasea et pysty käyttämään nmap integrointia!

Pystyt tekemään skannauksen **db_nmap (asetukset) (kohde)** esimerkiksi: **db_nmap –A 10.10.51.55**

```
msf6 > db_nmap -A 10.10.51.55
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-31 09:33 EEST
[*] Nmap: Nmap scan report for 10.10.51.55
[*] Nmap: Host is up (0.00021s latency).
[*] Nmap: Not shown: 977 closed tcp ports (conn-refused)
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
[*] Nmap: | ftp-syst:
[*] Nmap: |   STAT:
[*] Nmap: | FTP server status:
[*] Nmap: |      Connected to 10.10.51.82
[*] Nmap: |      Logged in as ftp
[*] Nmap: |      TYPE: ASCII
[*] Nmap: |      No session bandwidth limit
[*] Nmap: |      Session timeout in seconds is 300
[*] Nmap: |      Control connection is plain text
[*] Nmap: |      Data connections will be plain text
[*] Nmap: |      vsFTPd 2.3.4 - secure, fast, stable
```

Seuraavaksi voidaan katsoa miten nähdä lajitellut tulokset. Pystyt tarkistamaan hostit komennolla **hosts.**

```
msf6 > hosts

Hosts
=====

address       mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------       ---  ----  -------  ---------  -----  -------  ----  --------
10.10.51.55                Linux                    server
```

Sitten pystyt tarkistamaan palvelut jotka on tullut nmap skannauksesta komenolla **services**.

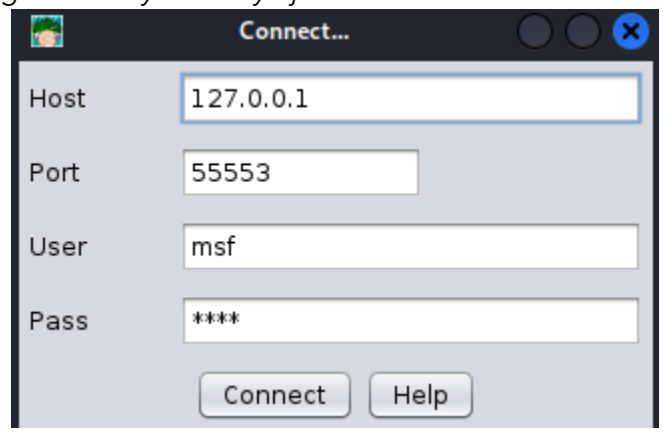
```
msf6 > services
Services
========

host         port  proto  name         state  info
----         ----  -----  ----         -----  ----
10.10.51.55  21    tcp    ftp          open   vsftpd 2.3.4
10.10.51.55  22    tcp    ssh          open   OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
10.10.51.55  23    tcp    telnet       open   Linux telnetd
10.10.51.55  25    tcp    smtp         open   Postfix smtpd
10.10.51.55  53    tcp    domain       open   ISC BIND 9.4.2
10.10.51.55  80    tcp    http         open   Apache httpd 2.2.8 (Ubuntu) DAV/2
10.10.51.55  111   tcp    rpcbind      open   2 RPC #100000
10.10.51.55  139   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.10.51.55  445   tcp    netbios-ssn  open   Samba smbd 3.0.20-Debian workgroup: WORKGROUP
10.10.51.55  512   tcp    exec         open   netkit-rsh rexecd
10.10.51.55  513   tcp    login        open   OpenBSD or Solaris rlogind
10.10.51.55  514   tcp    tcpwrapped   open
10.10.51.55  1099  tcp    java-rmi     open   GNU Classpath grmiregistry
10.10.51.55  1524  tcp    bindshell    open   Metasploitable root shell
10.10.51.55  2049  tcp    nfs          open   2-4 RPC #100003
10.10.51.55  2121  tcp    ftp          open   ProFTPD 1.3.1
10.10.51.55  3306  tcp    mysql        open   MySQL 5.0.51a-3ubuntu5
10.10.51.55  5432  tcp    postgresql   open   PostgreSQL DB 8.3.0 - 8.3.7
10.10.51.55  5900  tcp    vnc          open   VNC protocol 3.3
10.10.51.55  6000  tcp    x11          open   access denied
10.10.51.55  6667  tcp    irc          open   UnrealIRCd
10.10.51.55  8009  tcp    ajp13        open   Apache Jserv Protocol v1.3
10.10.51.55  8180  tcp    http         open   Apache Tomcat/Coyote JSP engine 1.1
```

Vielä on muita komentoja kuten **vulns** joka kertoo tunnistetut haavoittuvuudet. **Creds** joka kertoo tunnuksia mitä metasploit on saanut, **Loot** on lähes sama asia ja viimeiseksi on **notes** eli muistiinpanot, joita pystyt lisäämän eri workspaceihin!

Armitage

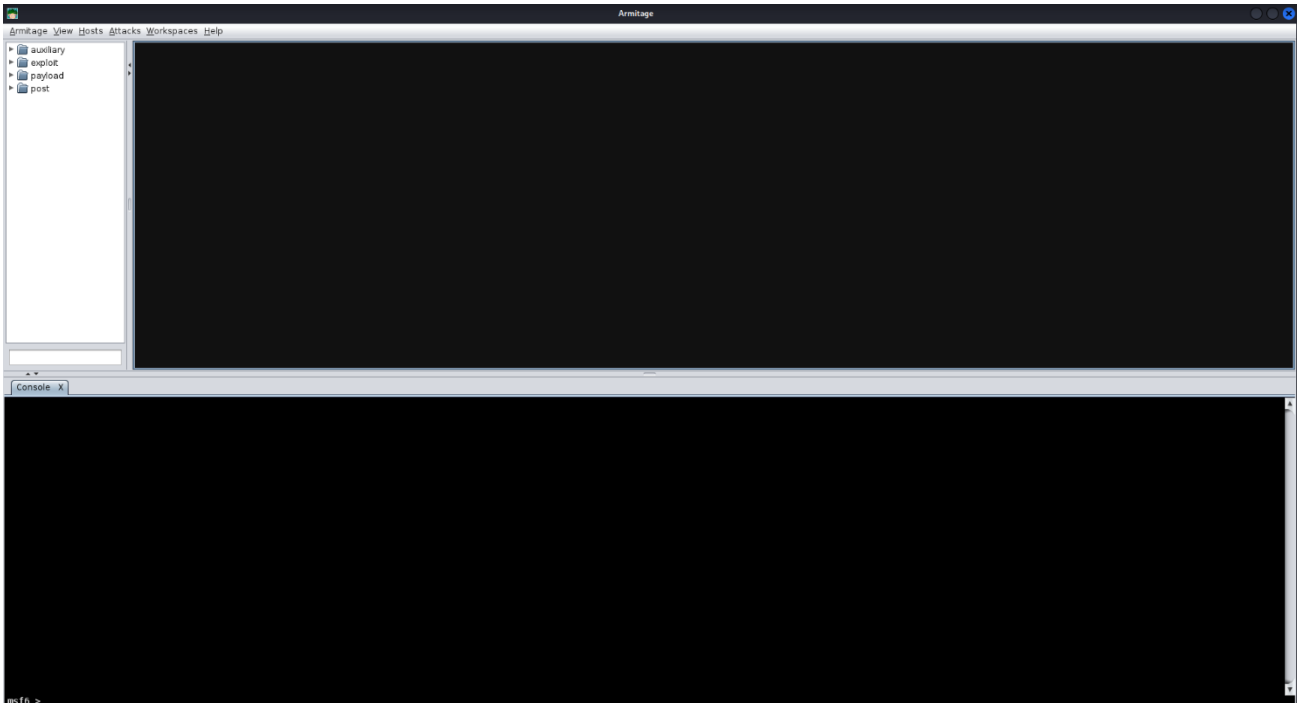
Armitage on gui versio metasploitista ja tässä osiossa katsomme miten sen saa käyttöön ja miten se toimii. Huomioithan että metasploit databse on pakko olla asetettuna ja käynissä sillä se auttaa armitagea ja metasploittia keskustelemaan keskenään!

Armitagen saa käynnistettyä joko terminaalista tai sovelluksena :



User ja pass kohtiin aseta se käyttäjä ja salasana minkä olet asettanut metasploitin databaseen ja sitten paina connect! Sitten sinulle tulee tämän näköinen kysymys:

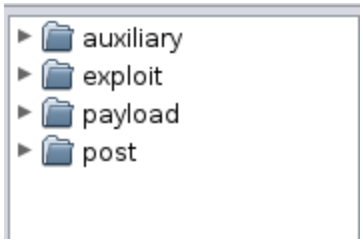
Paina yes niin se luo rpc serverin metasploitille. Tadaa! nyt sinulla on käytössä armitage ja se näyttää tältä:



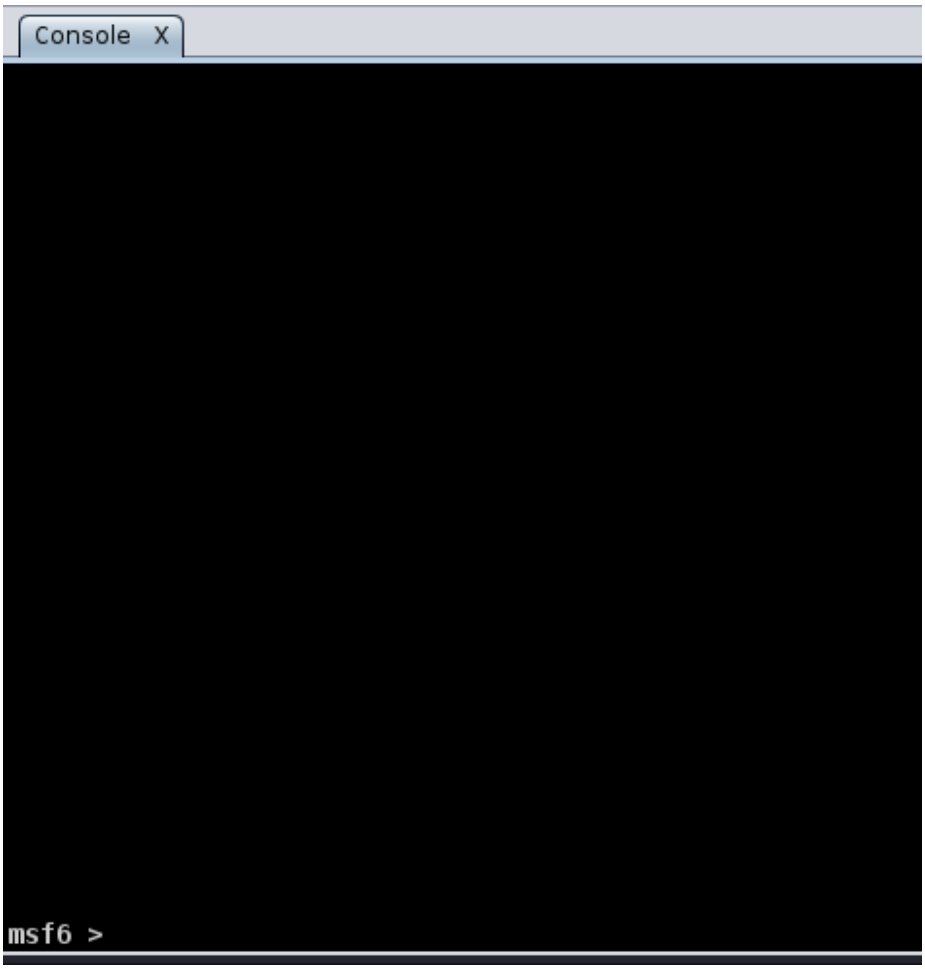
Armitagen käyttö

Armitagen käyttö voi olla monille helpompaa, koska se on gui sovellus. Kaikki toimii samalla tavalla kuin metasploitissa komenoilla ja niitä suoritetaan backendissä metasploitissa!

Armitagessa on samat moduulit kuin metasploitissa. Ne löydät sivupaneelista:



Armitagessa on myös konsoli, missä on metasploitti. Yleensä se on alhaalla:



Armitagessa näet myös hostit keskeltä armitagea!

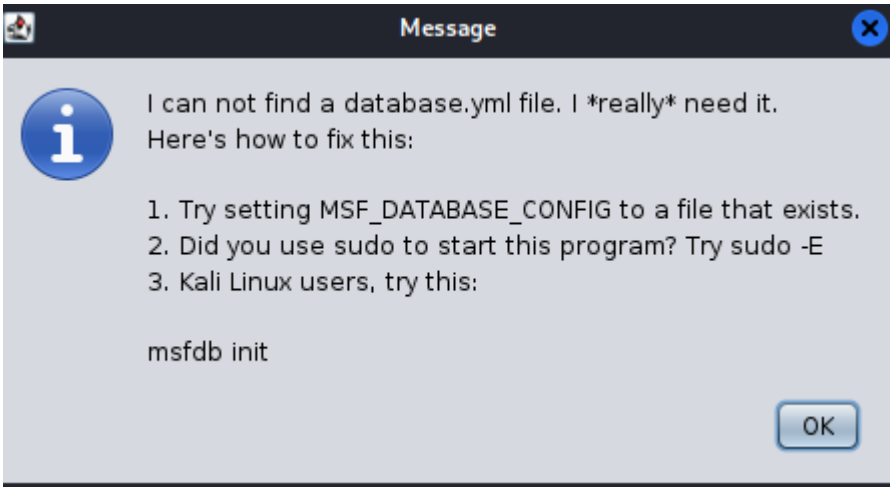
Ylhäältä näet asetuksia ja pystyt hosts osiosta skannamaan joko nmapilla tai metasploitn skanneria käyttäen selvittääksesi portit ja palvelut. Attack menusta voit hakea haavoittuvuudet ja käyttää niitä klikkaamalla hostia ja sieltä attack valikkoa!

Pystyt myös etsimään manuaalisesti moduuleita sivupaneelista. Esim mikä palvelu on käynnissä. Yksi mahdollinen voisi olla ssh!

HUOM kokeile itse käyttää armitagea ja tutki siitä tietoa enemmän, sillä siellä on paljon ominaisuuksia mitä tässä ei ole käyty!

Armitagen korjaus

Minulle tuli tämmöinen errori:



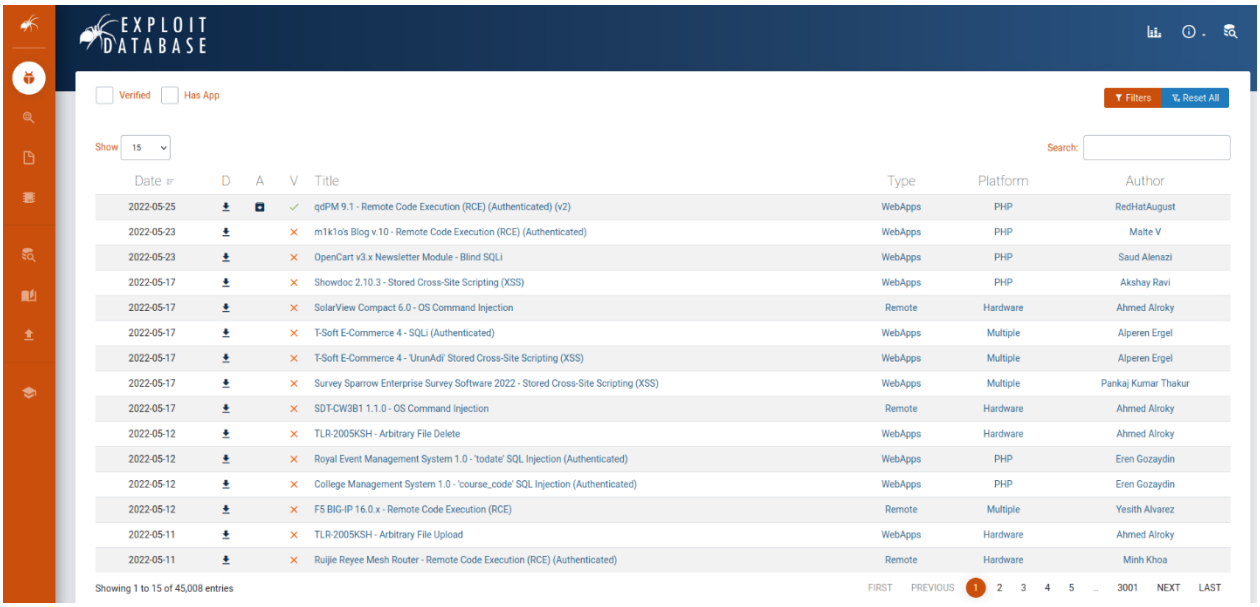
Tämä tarkoittaa sitä että armitage ei löydä sinun metasploit databasen configuraatio tiedostoa. Siihen on olemassa helppo korjaus, joka vaatii sen että kerrot armitagelle missä kyseinen tiedosto on. Se on yleensä polussa: **/usr/share/metasploit-framework/config/database.yml**. Korjaa tämä ongelma komenolla **export MSF_DATABASE_CONFIG= /usr/share/metasploit-framework/config/database.yml** ja käynnistä armitage uudelleen komennolla **sudo –E armitage**!

Extraa! haavoittuvuuksien hakeminen

Haavoittuvuuksia on helppo etsiä joko käyttäen **exploit-DB** tai **searchsploittia**, huomioithan että sinun tarvitsee tehdä palvelu tutkinta ensin, sillä sinun tarvitsee tunnistaa mikä palvelu ja versio on käyttössä. Palvelun versiolla pystyy etsimään olemassa olevia exploitteja!

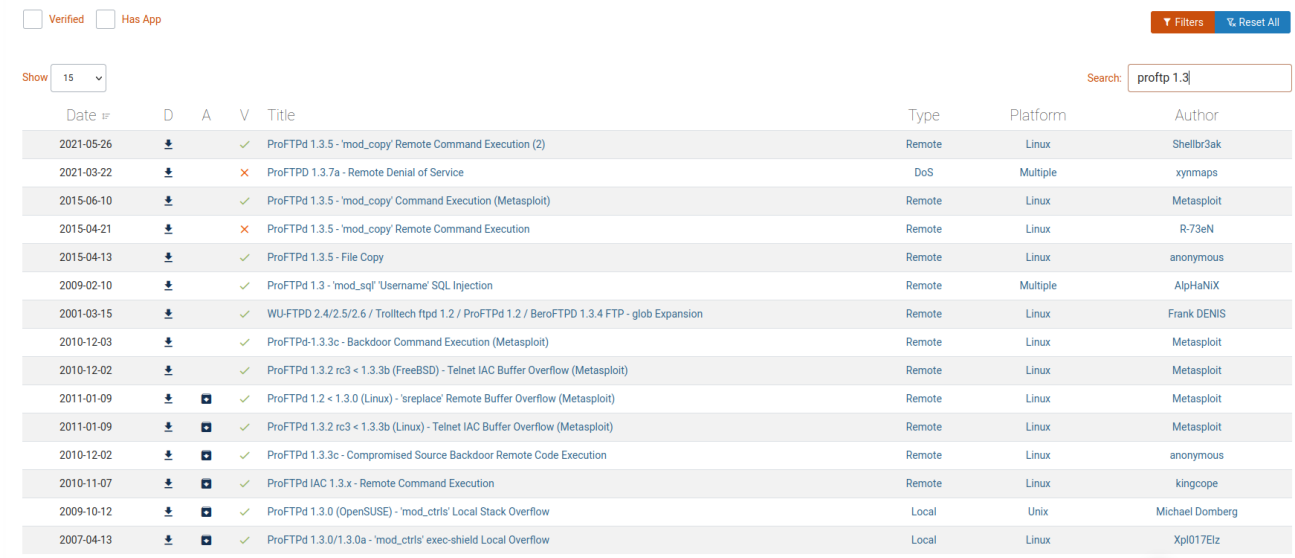
Exploit-DB

Pääset etsimään tältä sivulta voimassa olevia haavoittuvuuksia, katsotaan miten tämä käytännössä toimii!



Kun pääset tähän sivulle, voit etsiä exploitteja search palkista

Pystyt asettamaan suodattimia ja hakea exploitteja. Esimerkiksi käytän metasploitablesta tehtyä skannausta hyväksi ja etsin ssh palveluun exploitteja Proftpb 1.3.1.



Pystyt lataaman exploitteja jos lataus kuva näkyy D osiossa! Huomaathan että lue aina exploiteista mitä suoritat koneella. Jos V osiossa on X niin sitä ei ole tarkistettu!

SearchSploit

Searchsploit on Offensive securityn tekemä työkalu linuxille, joka mahdollistaa exploittien ja shell koodien haun exploit-databasesta ja latauksen terminaalissa. Saat apua komennolla **searchsploit –h**!

Muistathan päivittää searchsploit exploitit komenolla **searchsploit –u**!

Searchsploit on helppo työkalu, sillä pystyt etsimään exploitteja komennolla:

searchsploit (palvelu tai käyttöjärjestelmä)

```
┌──(eetu㉿kali)-[~]
└─$ searchsploit android
```

```
 Exploit Title
```

```
1Password < 7.0 - Denial of Service
Adobe Reader for Android 11.1.3 - Arbitrary JavaScript Execution
Adobe Reader for Android < 11.2.0 - 'addJavascriptInterface' Local Overflow (Metasploit)
AirDroid - Arbitrary File Upload
AirDroid 4.2.1.6 - Denial of Service
AirDroid iOS / Android / Win 3.1.3 - Persistent
AirDrop 2.0 - Denial of Service (DoS)
AirMore 1.6.1 - Denial of Service (PoC)
Allwinner 3.4 Legacy Kernel - Local Privilege Escalation (Metasploit)
Android - 'getpidcon' Permission Bypass in KeyStore Service
Android - 'zygote→init;' Chain from USB Privilege Escalation
Android - ashmem Readonly Bypasses via remap_file_pages() and ASHMEM_UNPIN
Android - Binder Driver Use-After-Free
Android - binder Use-After-Free of VMA via race Between reclaim and munmap
Android - binder Use-After-Free via fdget() Optimization
Android - binder Use-After-Free via racy Initialization of →allow_user_free
Android - Directory Traversal over USB via Injection in blkid Output
Android - getpidcon() Usage in Hardware binder ServiceManager Permits ACL Bypass
Android - Hardware Service Manager Arbitrary Service Replacement due to getpidcon
Android - Inter-Process munmap due to Race Condition in ashmem
Android - sdcardfs Changes current→fs Without Proper Locking
Android 1.x/2.x HTC Wildfire - Local Privilege Escalation
Android 7 - 9 VideoPlayer - 'ihevcd_parse_pps' Out-of-Bounds Write
Android 7 < 9 - Remote Code Execution
```

Näet myös oikella puolella kyseisen exploitin sijainnin järjestelmästä.

```
 Path
```

```
android/dos/46165.txt
android/local/32884.txt
arm/local/33791.rb
android/webapps/37504.py
android/dos/46337.sh
multiple/webapps/37662.txt
android/dos/46445.c
android/dos/46381.py
android/local/40504.rb
android/dos/43996.txt
android/local/45379.txt
android/dos/47921.txt
android/local/47463.txt
android/dos/46357.txt
android/dos/46356.txt
```

Lähteet

Huom kaikki lähteet ovat Englanniksi!

Nmapin sivu: https://nmap.org/

Metasploit tutoriaalit: https://www.offensive-security.com/metasploit-unleashed/

Exploit-DB: https://www.exploit-db.com/

Searchsploit manuaali: https://www.exploit-db.com/searchsploit

Armitage ohjeet: https://www.kali.org/tools/armitage/

Kaikki muu on minun omalla kokemuksellani tullutta tietoa!

Lopputiivistelmä

Osaat perusteita nmapista ja metasploitista, lisäksi osaat käyttää niitä tehokkaasti palvelun tunnistamisessa. Osaat myös ajatella tietotuvallisuutta edellyttävällä tavalla, joka auttaa tulevaisuudessa palveluiden ja verkkojen rakentamiseen. Osaat myös käyttää exploit-db ja searchsploittia niin, että saat exploitteja ja Shell codeja!

Haluat opetella enemmän?

Tässä osiossa kerron miten pystyt opettelemaan lisää tai testata juuri opittuja taitoja turvallisesti ja huolettomasti. Tiedät varmaankin jo, että testaaminen luvattomasti on rikos! Noh, miten pääsen opettelemaan, jos minulla ei ole palveluita tai palvelimia mihin testata taitoja?

On monia palveluita, jotka tarjoavat alustoja missä testata taitoja, nyt kerron minun lempparistani! Hackthebox on palvelu missä on virtuaalipalvelimia mihin voi hyökätä vapaasti! siellä on myös haasteita! Pääset tästä linkistä tutustumaan hackthebox palveluun!

Kaikki haasteet ovat eritasoisille ja ne on merkitty siellä sivulla kun aloitat haasteen!

Haasteet koostuvat eri palveluista ja sinun on saatava flägin, kun olet murtautunut järjestelmään, haaste merkitään suoritetuksi, kun olet palauttanut flägin!

Hyvää! Tietoturvan testaamis matkaa!

By: Eetu Heino