**Pentesthez**

fontos portok: 22-ssh, 53-dns, 25-smtp, 21-ftp, 80/443-http(s)

össz. portok : 65,535

Gyors Billentyűk:

(http://sugo.ubuntu.hu/16.04/shell-keyboard-shortcuts.html)

Alt + Print Screen - Képernyőkép készítése egy ablakról

Ctrl + Alt +N yílbillentyűk - Váltás a munkaterületek között

Ctrl + Alt + Shift+Nyílbillentyűk - Az aktuális ablak áthelyezése másik munkaterületre

Ctrl + Alt + Delete - Kijelentkezés

Ctrl + Super + D - Minden ablak elrejtése, és az asztal megjelenítése. Nyomja meg újra az ablakok visszaállításához.

Ctrrl + C - folyamat megszakítása

Ctrl + Alt + T - terminál

Ctrl + Shift + +/- - nagyítás / kicsinyítés terminálban

Ctrl + Shift + W - tálcára helyez

Helymeghatározás:

ls - aktuális hely fájljai/mappái

cd - helyváltoztatás

pwd - aktuális hely kiírása

Fájl létrehozás / szerkesztés:

cat / less - kiírja a file tartalmát

touch - létrehoz egy üres file-t

echo - tartalmat adhatunk a file-nak

nano - file-t hozunk létre és szerkesztőablakban tartalmat adhatunk neki

Mappa kezelés:

mkdir - mappa létrehozása

mv - mozgatás

cp - másolás

rm - törlés (könytár törlése pl: rm folder1 -r)

Egyeb:

man / help - segédlet

cal - naptár

date - dátum

information Gathering:

Whatweb - info kérés egy weboldalról

--verbose - az info rendezése (olvashatóbb lesz)

--log--verbose=file1 - eredmény mentés fileba

--no-errors - ne írja ki a hibákat

TheHarvester - DNS-ről public info szerzés (név, username, email, stb.)

RED\_HAWK - 14 féle scan (nmap,dns,geo-ip,whois,sqli,mx,stb.)

Scanning:

Arp -

-a - felderítés hálózaton belül

https://www-geeksforgeeks-org.translate.goog/arp-command-in-linux-with-examples/?\_x\_tr\_sl=en&\_x\_tr\_tl=hu&\_x\_tr\_hl=hu&\_x\_tr\_pto=sc

Netdiscover - host felderítés hálózaton belül

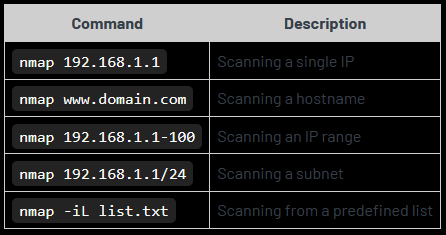
https://www-kali-org.translate.goog/tools/netdiscover/?\_x\_tr\_sl=en&\_x\_tr\_tl=hu&\_x\_tr\_hl=hu&\_x\_tr\_pto=sc

Netstat -

-nr - sajátgép gateway

Nmap –

https://zerotomastery.io/cheatsheets/nmap-cheat-sheet/?utm\_source=udemy&utm\_medium=coursecontent#nmap\_overview



|  |  |  |  |
| --- | --- | --- | --- |
| Parancs | Leírás | SUDO | Észlelhetőség |
| nmap -sS <\_target> | Ez egy TCP SYN SCAN, más néven lopakodó vizsgálat. Ez a vizsgálat csak SYN csomagot küld, és SYN/ACK választ vár. Ha az nmap SYN/ACK üzenetet kap egy adott vizsgált porton, az azt jelenti, hogy a port létezik a gépen, és nyitva van. Ez egy gyors és meglehetősen pontos szkennelés, amelyet legtöbbször használni fog. | Kell | Nagyon alacsony |
| nmap -sT <\_target> | Az -sT vizsgálat pontosabb, mint az -sS vizsgálat, de a hátránya, hogy lassabb, több zajt ad, és könnyen észlelhető a jól beállított tűzfalak által. Ennek az az oka, hogy teljes háromirányú kézfogást (vagy jobban mondva teljes TCP-kapcsolatot) hoz létre a gazdagéppel. | Nem kell | Közepes |
| nmap -sU <\_target> | Ez a vizsgálat az UDP-portok keresésére szolgál. Ez általában egy lassabb és nehezebb vizsgálat. Bár a legtöbb szolgáltatás TCP-t használ, vannak olyan szolgáltatások is, amelyek UDP-t használnak, például: DNS, SNMP, DHCP. Tehát ez a vizsgálat továbbra is hasznos, mivel még mindig vannak kihasználható UDP-szolgáltatások. Tehát ne essen abba a hibába, hogy kihagyja ezt a vizsgálatot, lehet, hogy talál valamit! | Kell | Közepes |
| nmap -sn <\_target(s)> | Ez egy egyszerű és gyors ping-ellenőrzés annak megállapítására, hogy mely gazdagépek válaszolnak az ICMP ping-csomagokra. Ez akkor hasznos, ha ugyanazon (al)hálózaton van, mint a vizsgált IP-tartomány, és csak azt szeretné tudni, hogy mely eszközök élnek. Ugyanezt az eredményt kaphatja a -Pn használatával is. | Nem kell | Alacsony |
| nmap -sV <\_target> | Ez a szolgáltatás verziójának vizsgálata. Annak érdekében, hogy megtudjuk, milyen exploitok működnek, nagyon hasznos, ha ismerjük a szolgáltatás verzióját a nyitott port mögött. Előfordulhat, hogy egy bizonyos kizsákmányolás csak egy bizonyos szolgáltatás egy adott verziójában működik, mivel előfordulhat, hogy egy új verzióban javítják. | Nem kell | Közepes |
| nmap -O <\_target> | Ez egy távoli operációs rendszer észlelési vizsgálat. Ezt a vizsgálatot arra használjuk, hogy megtudjuk, milyen operációs rendszeren fut a cél. Ez nagyon hasznos, mert képet ad arról, hogy milyen exploitok működhetnek a célponton, és mely exploitok nem. Vegye figyelembe, hogy ez a vizsgálat csak akkor működik, ha van legalább 1 nyitott és 1 zárt port. | Kell | Közepes |
| nmap -A <\_target> | Ez egy agresszív szkennelés. Ez az ellenőrzés végrehajtja az operációs rendszer észlelését, a verzió észlelését, a szkriptvizsgálatot és a nyomkövetési útvonalat. Bár sok információt ad vissza, riasztja a célpontot, mivel valószínűleg ez a legzajosabb keresés. | Kell | Nagyon Magas |

|  |  |
| --- | --- |
| Parancs | Leírás |
| nmap -p <\_port> <\_target> | A -p <\_port> használatával kereshet egy adott portot a célponton. |
| nmap -p <\_port\_range\_begin>-<\_port\_range\_end> <\_target> | A -p-t is használhatja számos port keresésére, a -p 1-20 <\_target> a cél 1-20-as portjait keresi. |
| nmap -p <\_port\_a>,<\_port\_b>,<\_port\_c> <\_target> | Lehetőség van több konkrét port megadására is, vesszővel elválasztva őket. |
| nmap -p U:<\_udp\_port>,T:<\_tcp\_port> <\_target> | Ha UDP- és TCP-portokat is szeretne keresni, használhatja az U:<\_udp\_port> és T:<\_tcp\_port> karakterláncot, vesszővel elválasztva. |
| nmap -F <\_target> | Az -F arra utasítja az Nmap-et, hogy keresse meg a 100 leggyakoribb portot, amelyek nyitva lehetnek egy célponton. |
| nmap -top-ports <\_amount> <\_target> | Ezzel a lehetőséggel megkeresi a # legnépszerűbb portot, attól függően, hogy mekkora összeget ad meg. |
| nmap -p- <\_target> | Ez az opció arra utasítja az Nmap-et, hogy ellenőrizze a célt a világ összes ismert portjára... összesen 655 355 port van. Ez egyértelműen hosszabb ideig tart a beolvasás befejezéséhez. |

Az Nmap lehetővé teszi az "időzítési sablonok" használatát, amelyek lehetővé teszik a felhasználó számára, hogy meghatározza, milyen agresszív akar lenni a vizsgálatokkal, miközben az Nmap maga választja ki a pontos időzítési értékeket. 6 időzítési sablon létezik:

|  |  |
| --- | --- |
| **Parancs** | **Leírás** |
| nmap -T0 <\_target> | A T0 a leglassabb vizsgálat, amelyet "Paranoid" vizsgálatnak is neveznek. Ez az opció jó az IDS-elkerüléshez. |
| nmap -T1 <\_target> | A T1 gyorsabb opció, mint a T0, de továbbra is "Sneaky" sablonként hivatkoznak rá. Ez az időzítési lehetőség az IDS kijátszására is jó választás. |
| nmap -T2 <\_target> | A T2 opció az időszerű vizsgálatra szolgál, és "Udvarias" időzítési opcióként is ismert. Ez lelassítja a vizsgálatot, ami kevesebb sávszélességet és kevesebb célgép-erőforrást eredményez |
| nmap -T3 <\_target> | A T3 alapértelmezett pásztázási időzítőként is ismert. Ennek a sablonnak a használata ugyanaz, mintha egyáltalán nem használná. Az Nmap alapértelmezés szerint ezt használja, ha nincs kiválasztva sablon. |
| nmap -T4 <\_target> | A T4 egy lehetőség a szkennelés felgyorsítására azáltal, hogy feltételezi, hogy Ön egy ésszerűen gyors és megbízható hálózaton van. Ezt az idősablont "Agresszív" sablonnak is nevezik. |
| nmap -T5 <\_target> | A T5 egy őrülten gyors mód, feltételezve, hogy egy rendkívül gyors hálózaton van... vagy ha hajlandó feláldozni némi pontosságot a sebességért. Ezért nevezik „őrült” módnak is. |

Végül, de nem utolsósorban... Az Nmap szkripteket biztosít számunkra. Ezek a szkriptek kategóriákba tartoznak:

auth

broadcast

default. discovery

dos

exploit

external

fuzzer

intrusive

malware

safe

version

vuln

Egy szkriptet a következő módon futtatunk: nmap --script <\_script/\_script\_group> <\_taget>

Néhány forgatókönyv nagyon zajos, néhány egyáltalán nem. Ezért fontos elolvasni, hogy az egyes szkriptek mit csinálnak, és hogy a cél könnyen észlelhető-e vagy sem.

Vegye figyelembe, hogy a --script vizsgálatokat root/sudo-ként kell futtatnia.

Amikor pentesztet végez, hasznos az -oN kapcsoló használata a szkennelés szövegfájlba történő kimenetéhez. Így később bemásolhatja a pentest jelentésébe.

A következőképpen kell csinálni: nmap -oN <\_fájlnév.txt> <\_target>

Egy szkennelés során több opciót is használhat.

Például valószínűleg ez a leggyakrabban végzett vizsgálat: sudo nmap -sS <\_target> -oN <\_fájlnév.txt>

Nmap jegyzet-

--help - kurva sok lehetőség

man nmap - érdemes belenézni a kézikönyvébe (Port Scanning basics bekezdést főleg a rengeteg scan lehetőség miatt)

nmap "targetip" - info(portok/szállításmód + státusz + protokoll) (alapból csak 1k portot páztáz végig a 65k-ból)

nmap 192.168.1.1/24 VAGY 192.168.1.1-255 - adott range/subnet páztázása

nmap -sS "ip" - TCP SYN scan (tűzfal védelem nélküli hálózatokon használható) (ha a cél SYN-ACK-t küld vissza akkor a port nyitva van / ha RST-t akkor zárva / ha semmit attól még szűrtként lesz jelezve azaz meghatározhatatlan a státusza(szűrővel vagy tűzfallal lehet védve))(NINCS teljes TCP kapcsolat)

-sT - infot ad mint az -sS (különbség: Létrehoz teljes TCP kapcsolatot / azaz sok nyomot hagy, lenyomozhatóbb)

-sU - UDP vizsgálat (nagyon lassú viszon sok esetben elhagyják az UDP portok biztonságát azaz sok esetben kihasználhatóak, érdemes lefuttatni) (% lekérdezés - felső nyílbillentyű)

-sA - hasznos a tűzfal feltérképezéséhez

-sV –version-intesity „7” – argumentummal megadhatjuk a lekérdezés intenzitását (argu nélkül alapból 7) (0-9-ig adható meg) (kevésbé használt)

nmap xy xy xy >> file.txt – eredmények mentése

-sF / -G /-F /-S /-D – ezekkel lehetőség van megkerülni a tűzfalat(„filtered”)

-f – kapcsolóval kisebb csomagokra bonthatjuk (halmozható pl: -f -f)(TCP fejlécet több csomagra osztja fel pl:24 bájtosat 3db 8-ra) (megkerüli a tűzfalat NEM rejti el az ip-t )

-D RND:5 --kapcsolóval csali címeket ad hozzá a sajáttal együtt (esetünkben 5db)(valamennyire rejti az ip-címet)(RND helyett lehet -D vagy beírt ip-k 1.1.1.1,2.2.2.2,ME 3…) (utána még hozzáadhatunk scan típusokat (RND:5 -sS))

-S „ip” -Pn - IP-cím meghamisítás (FONTOS: -Pn / A Ping-ellenőrzés elvetése!)(amúgy a pn-nel feltételezi a gépünk hogy minden Host online) (A -Pn kombóhoz esetenként kellhet hozzá az -e is) (Az -e a hálózati interfész megadására szolgál(pl: -e eth0)) (utána megadhatunk egy random portszámot a -g „portszám” -mal, ezzel különböző portokra fogja küldeni a csomagokat(ez akkor jó amikor a rendszergazda egy bizonyos portra állítja be a beérkező csomagokat))

-sF – ha a SYN scan nem működik megpróbálhatjuk a FIN scant. Csak egy FIN csomagot küld egyéb flagek nélkül.

-T - időzítési sablon (T0/T1 IDS megkerülésére, lassabbak)(van táblázat fentebb)