External Network Penetration Testing

- External Network Penetration Testing
  - OSINT
  - Reconnaissance
    - Passive External Network Reconnaissance
      - Dorks
      - Pastebin
      - Certificate Transparency
      - Exposed credentials and leaks (Flare, DarkWeb Agent, dehashed, breach-parse)
      - DNS history
      - ASN Lookups
      - Web Archive
    - Active External Network Reconnaissance
      - Subdomain enumeration
      - HTTP/HTTPS Screenshots
      - Web App Pentest Checklists
      - Linkedin users search
      - Subdomain takeover
      - Bypassing CloudFlare
      - NMAP
      - Recon-NG
      - User account enumeration
      - Exposed documents - Metadata
      - Virtual Host
      - BGP Hijacking
      - Cloud enumeration
    - Exposed services - Protocols
      - HTTP/HTTPS
      - SMTP
      - DKIM / DMARC / SPF misconfiguration
      - SNMP
      - FTP
      - SSH
      - Databases (MySQL, MSSQL, Oracle, DB2, Postgre, MongoDB...)
      - Exposed storages
      - Scanning external target
  - Exploitation
    - RCE
    - Exposed source code or credentials
    - SAP
    - Lync
    - IIS specific checks
    - Web vulnerabilities
    - SSL/TLS implementation

        - Default Credentials in use
        - Open SMTP Relay
        - DNS Zone Transfer
        - VPN - IKE Aggressive Mode
    - Password spray
        - General tool
            - CheckPoint SSL VPN
            - O365
            - OWA
            - Azure
            - IP rotation
        - 2FA/MFA implementation issues
    - Resources
        - FOREGENIX : Know your attack surfaces
        - Offensive OSINT
        - OSINT Resources
        - Pentest Check-List
        - Haax cheatsheet

OSINT

- spiderfoot
  https://github.com/smicallef/spiderfoot
- Maltego
- Metabigor
  https://github.com/j3ssie/metabigor
- Very complete and Great OSINT Blog https://start.me/p/ZME8nR/osint

Reconnaissance

Passive External Network Reconnaissance

Dorks

Google dorks

```
site:company.com -site:www.company.com
site:*.company.com
```

Bing dorks

```
site:company.com -site:www.company.com
site:*.company.com
```

Pastebin

- https://github.com/carlospolop/Pastos

- https://github.com/leapsecurity/Pastepwnd
- https://github.com/CIRCL/AIL-framework
- https://github.com/cvandeplas/pystemon
- https://github.com/xme/pastemon
- https://github.com/woj-ciech/pepe

Certificate Transparency

- crt.sh
- https://developers.facebook.com/tools/ct/ https://transparencyreport.google.com/https/certificates
- https://certstream.calidog.io/
- ct-exposer

```
python3 ct-exposer.py -d teslamotors.com
```

Finding domain for a company using certificate transparency list (Domain Parser)

```
curl -s https://crt.sh/\?o\=Company\&output\=json > crt.txt
cat crt.txt | jq -r '.[].common_name' | DomainParser | sort -u
```

Exposed credentials and leaks (Flare, DarkWeb Agent, dehashed, breach-parse)

- Social networks (linkedIn, hunter.io, clearbit, phonebook.cz, Facebook, Company twitter/instagram)

DNS history

- Security-Trails
- https://intodns.com/company.com)

ASN Lookups

https://bgp.he.net/dns/company.com#_ipinfo
Shodan ASN filter feature

Google search

```
ipinfo asn Company Name
```

Amass Intel module

```
amass intel -org CompanyName
```

TLSX : TLS Grabber

```
echo "144.178.0.0/10" | tlsx -san
```

Web Archive

- Wayback machine
- https://archive.fo

- Google cache

Active External Network Reconnaissance

- masscan
- censys
- shodan (search engine filters + monitor feature)
- scans.io

Subdomain enumeration

- DNS brute force (aiodnsbrute, subLocal)
- DNS Recon (amass, sublist3r) https://0xffsec.com/handbook/information-gathering/subdomain-enumeration/#asn-enumeration

A (script)[https://github.com/appsecco/the-art-of-subdomain-enumeration/blob/master/san_subdomain_enum.py] to extract sub-domains from Subject Alternate Name(SAN) in X.509 certs

- Source: https://github.com/appsecco/the-art-of-subdomain-enumeration

```
python3 san_subdomain_enum.py company.com
```

- https://github.com/projectdiscovery/subfinder Subdomain discovery tool that discovers valid subdomains for websites by using passive online sources.

```
subfinder -d targetdomain.com -o output.txt
```

DNS Scan

```
python3 dnscan.py -d aecon.com -w subdomains.txt
```

aiodnsbrute

```
aiodnsbrute -t 20 company.com -o csv -f subdomains -w ./subdomains-top1million-110000.txt
```

HTTP/HTTPS Screenshots

- Aquatone
- Eyewitness
- WitnessMe
- GoWitness

Web App Pentest Checklists

- https://pentestbook.six2dez.com/others/web-checklist
- https://alike-lantern-72d.notion.site/Web-Application-Penetration-Testing-Checklist-4792d95add7d4ffd85dd50a5f50659c6
- https://github.com/swisskyrepo/PayloadsAllTheThings

Linkedin users search

- https://github.com/initstring/linkedin2username.git
- https://github.com/vysecurity/LinkedInt.git

Subdomain takeover

- https://www.hackerone.com/blog/Guide-Subdomain-Takeovers
- (https://github.com/haccer/subjack)

```
./subjack -w subdomains.txt -t 100 -timeout 30 -o results.txt -ssl
```

Bypassing CloudFlare

- https://github.com/greycatz/CloudUnflare
- https://www.ericzhang.me/resolve-cloudflare-ip-leakage/

NMAP

- NSE scripts : 14 categories
  - auth
  - broadcast
  - brute
  - default
  - discovery
  - dos (not recommanded)
  - exploit
  - external
  - fuzzer
  - intrusive
  - malware
  - safe
  - version
  - vuln

Scanning /24 IP range with UDP and TCP scan using SMB NSE script.

```
nmap -sU -sT -p U:137,139,T:22,21,80,443,139,445 --script=smb2-security-mode.nse 192.168.0.10/24
```

Recon-NG

- https://github.com/lanmaster53/recon-ng

User account enumeration

Against web app portal

Exposed documents - Metadata

- Foca
- PowerMeta
- Pymeta

Virtual Host

- https://wya.pl/2022/06/16/virtual-hosting-a-well-forgotten-enumeration-technique/

BGP Hijacking

- BGP Deep Dive
- https://www.youtube.com/watch?v=oESNgliRar0
- Breaking HTTPS with BGP Hijacking
- Pentest Mag - BGP Hijacking
- NIST SP-800-54 - BGP Security
- Defcon 16 - Stealing the Internet

Cloud enumeration

- MicroBurst
- cloud_enum.py

Exposed services - Protocols

HTTP/HTTPS

SMTP

DKIM / DMARC / SPF misconfiguration

- https://github.com/BishopFox/spoofcheck.git
- https://github.com/Mr-Un1k0d3r/SPFAbuse
- https://github.com/MattKeeley/Spoofy

```
python3 spoofy.py -d company.com -o stdout
```

SNMP

- snmpget
- onesixtyone

```
for i in $(cat onesixtyone/dict.txt); do echo -n "$i : "; snmpget -v 3 -u $i udp6:[IPv6] MIB_TO_F
```

FTP

SSH

Databases (MySQL, MSSQL, Oracle, DB2, Postgre, MongoDB...)

Exposed storages

- AWS S3 buckets
- Azure blob storage
- GCP storage

Scanning external target

- Nessus, Burp Enterprise, Qualys, nuclei, wpscan, joomscan.

- Nessus Perl Parser

Exploitation

RCE

RCE-as-a-feature (Jenkins, Serv-U, etc).

- https://github.com/p0dalirius/Awesome-RCE-techniques

Exposed source code or credentials

- .git folder
- Access key, token, secret on github, gitlab, mercurial, code repo solutions... Git / Repo secret parsers
- gitleaks (https://github.com/zricethezav/gitleaks)
- trufflehog (https://github.com/trufflesecurity/truffleHog)
- git-secrets (https://github.com/awslabs/git-secrets)
- shhgit (https://github.com/eth0izzle/shhgit)
- gitrob (https://github.com/michenriksen/gitrob)

SAP

- https://book.hacktricks.xyz/network-services-pentesting/pentesting-sap

Lync

- https://www.mdsec.co.uk/2017/04/penetration-testing-skype-for-business-exploiting-the-missing-lync/
- https://www.trustedsec.com/blog/attacking-self-hosted-skype-businessmicrosoft-lync-installations/
- https://github.com/mdsecresearch/LyncSniper
- https://github.com/nyxgeek/lyncsmash

IIS specific checks

ASPNET_CLIENT Folder enumeration

- http://itdrafts.blogspot.com/2013/02/aspnetclient-folder-enumeration-and.html
- IIS Fuzz wordlist
- IIS Wordlist HackTricks
- .Trace.axd file

IIS tilde character “~” Vulnerability/Feature

- Burp Suite Module IIS Tilde Enumeration
- IIS-ShortName-Scanner

```
java -jar iis_shortname_scanner.jar 2 20 https://iiswebserver.com
```

Web vulnerabilities

- serialization/deserialization

SSL/TLS implementation

- heartbleed
- Shellshock

Default Credentials in use

- https://diarium.usal.es/pmgallardo/2020/10/31/list-of-default-credentials-websites/
- https://cirt.net/passwords
- https://datarecovery.com/rd/default-passwords/

Open SMTP Relay

- https://www.blackhillsinfosec.com/how-to-test-for-open-mail-relays/

DNS Zone Transfer

- https://github.com/mschwager/fierce.git

```
fierce -dns domain.fr
```

- https://github.com/cybernova/DNSaxfr

```
dig @your-ip -t axfr <TARGETDOMAIN.COM>
```

```
nmap --script dns-zone-transfer.nse --script-args "dns-zone-transfer.domain=<TARGETDOMAIN.COM>" -
```

VPN - IKE Aggressive Mode

Password spray

(o365, Azure, Citrix, RDP, VPN, OWA, etc)

General tool

- https://github.com/knavesec/CredMaster

The following plugins are currently supported:

- OWA - Outlook Web Access
- EWS - Exchange Web Services
- O365 - Office365
- O365Enum - Office365 User Enum (No Authentication Request)
- MSOL - Microsoft Online
- Okta - Okta Authentication Portal
- FortinetVPN - Fortinet VPN Client
- HTTPBrute - Generic HTTP Brute Methods (Basic/Digest/NTLM)

- ADFS - Active Directory Federation Services
- AzureSSO - Azure AD Seamless SSO Endpoint
- GmailEnum - Gmail User Enumeration (No Authentication Request)

CheckPoint SSL VPN

- https://github.com/lutzenfried/checkpointSpray

O365

- https://github.com/SecurityRiskAdvisors/msspray
- https://github.com/blacklanternsecurity/TREVORspray

```
./trevorspray.py -e emails.txt --passwords "Winter2021!"  --delay 15 --no-current-ip --ssh ubunt
```

OWA

Metasploit module : `scanner/http/owa_login`

Azure

- https://github.com/dafthack/MSOLSpray
- https://github.com/blacklanternsecurity/TREVORspray

IP rotation

Sometimes during password spraying or brute force attack attacker will need to rotate IP and geolocation to avoid being blocked.

- Burp Extension: IPRotate
- RhinoSecurity Blog : https://rhinosecuritylabs.com/aws/bypassing-ip-based-blocking-aws/
- AWS Keys Setup : https://www.youtube.com/watch?v=_YQLao6p9GM
- Proxycannon https://www.blackhillsinfosec.com/using-burp-proxycannon/
- BHIS blog (https://www.blackhillsinfosec.com/how-to-rotate-your-source-ip-address/)
- Amazon Lambda
- Fireprox

2FA/MFA implementation issues

- MFASweep: Detect MFA for various Microsoft Servers
- Credsniper

Re-using valid credentials on alternate services

- Mailsniper
- https://infosecwriteups.com/all-about-multi-factor-authentication-security-bypass-f1a95f9b6362
- https://medium.com/proferosec-osm/multi-factor-authentication-in-the-wild-bypass-methods-689f53f0b62b

Resources

FOREGENIX : Know your attack surfaces

- https://www.foregenix.com/blog/know-your-attack-surfaces

Offensive OSINT

- https://www.offensiveosint.io/offensive-osint-introduction/

OSINT Resources

- https://cheatsheet.haax.fr/resources/osint/
- https://cheatsheet.haax.fr/open-source-intelligence-osint/

Pentest Check-List

- https://github.com/ibr0wse/RedTeam-PenTest-Cheatsheet-Checklist

Haax cheatsheet

- https://cheatsheet.haax.fr/open-source-intelligence-osint/technical-recon/subdomain_discovery/