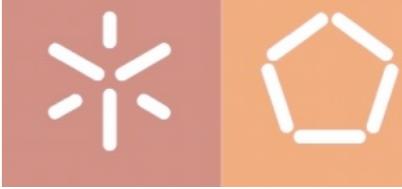


Segurança de Sistemas Informáticos

João Marco Silva
joaomarco@di.uminho.pt



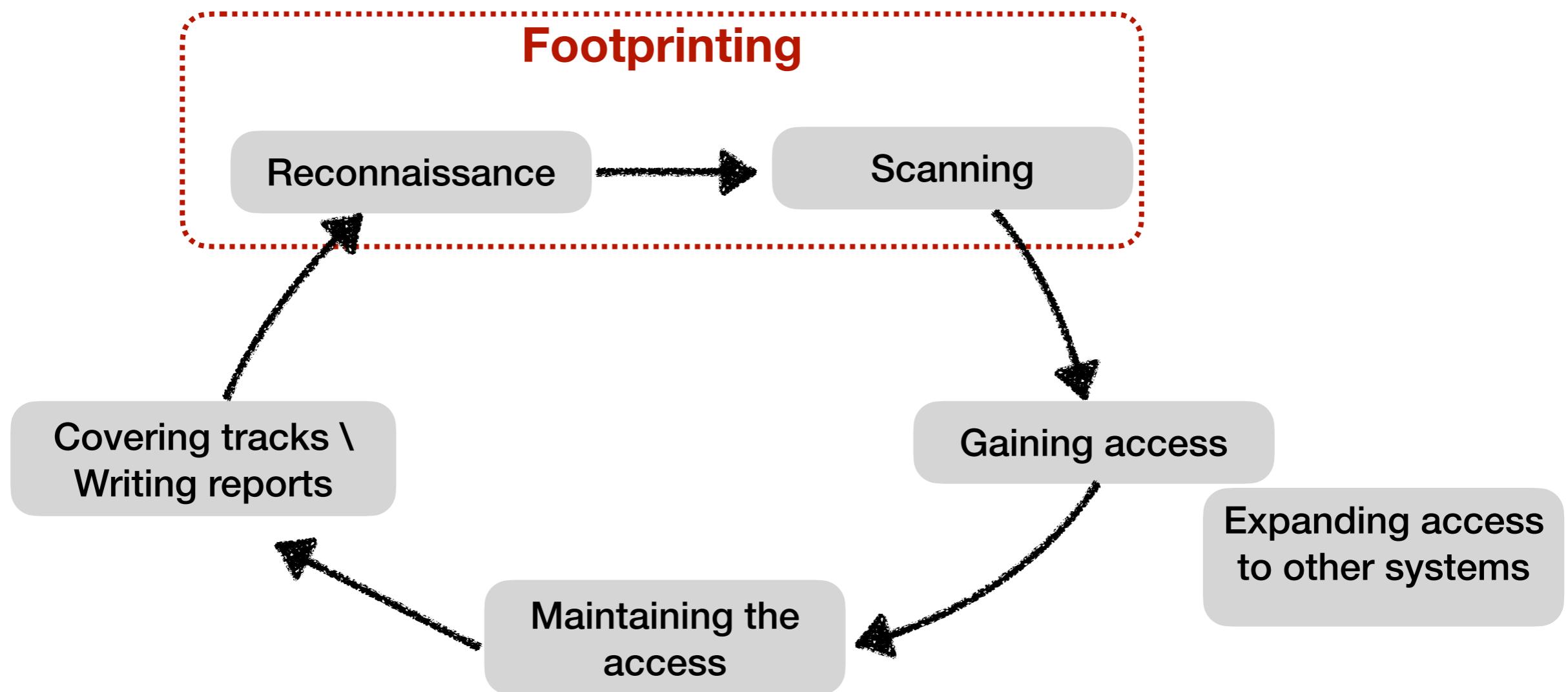
Penetration Testing - *Pentest*

- Authorised attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems
 - “Ethical hacking”



Penetration Testing

- Cyclical 5 stages process





Penetration Testing

- Footprinting
 - passive (reconnaissance) or active (scanning) information gathering about some target
 - enable an attacker to create a near complete profile of an organisation's security posture



Pentest - Reconnaissance

- Internal source
 - DNS information
 - private websites
 - dumpster diving
 - shoulder surfing
 - eavesdropping



Pentest - Reconnaissance

- External source
 - Services
 - Web site
 - social network
 - whois (<https://lookup.icann.org/>)
 - DNS
 - Archive sites archive.org (WayBackMachine)
 - URL analysis
 - Source code
 - Search engine
 - Job vacancy



Pentest - Reconnaissance

- Example - Website



- Typically exposed data
 - Board members
 - Technical teams
 - Addresses
 - Business partners

Google João Marco Silva

haslab.uminho.pt › joamarco › **João Marco Silva**
HASLab - **João Marco Silva**. I am a post-doc researcher at HASLab, INESC TEC, working on Security in Computer Communications. Previously, I rec.
You've visited this page 2 times. Last visit: 9/16/20

algoritmi.uminho.pt › Members › [Translate this page](#)
João Marco Cardoso da Silva - Centro ALGORITMI
João Marco Cardoso da Silva, Centro ALGORITMI Member (University of Minho). Other (Outro). Current Degree: MSc (Mestrado).

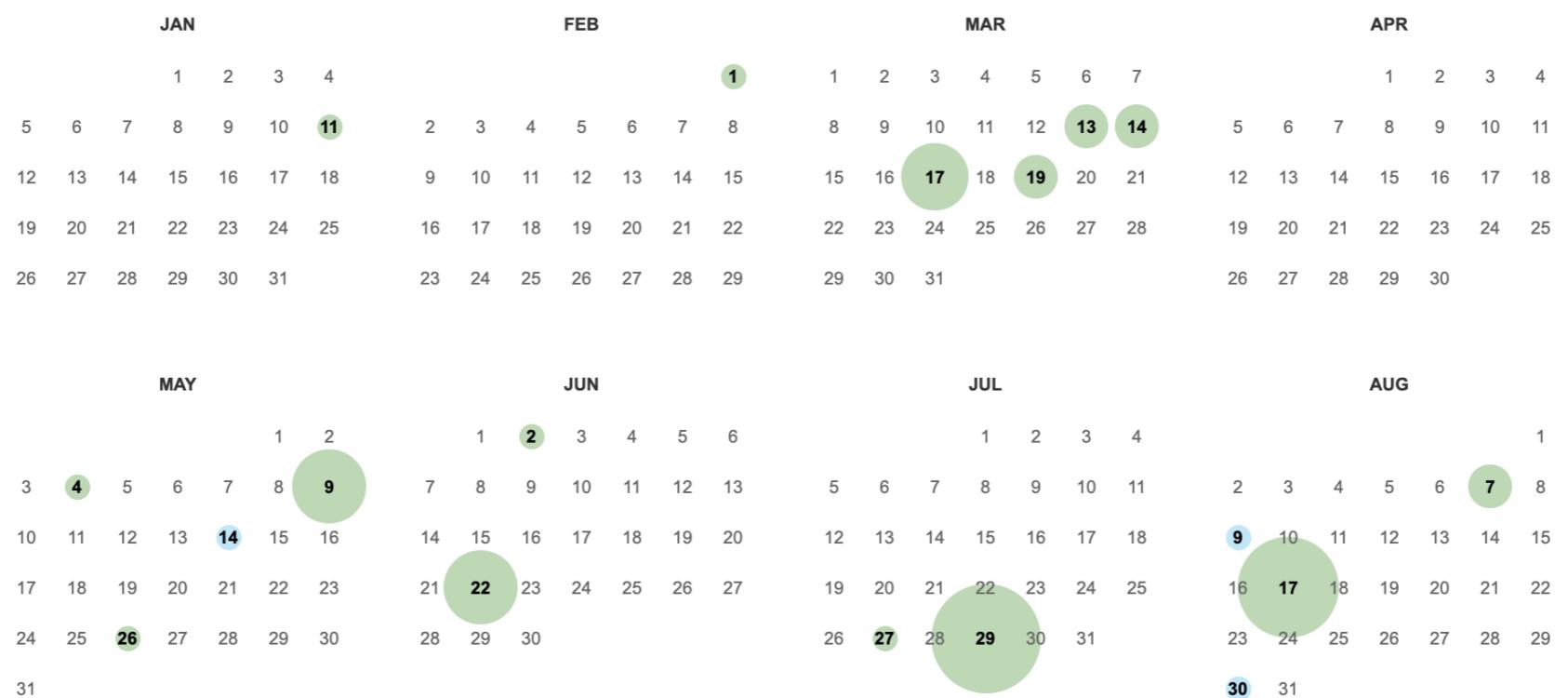
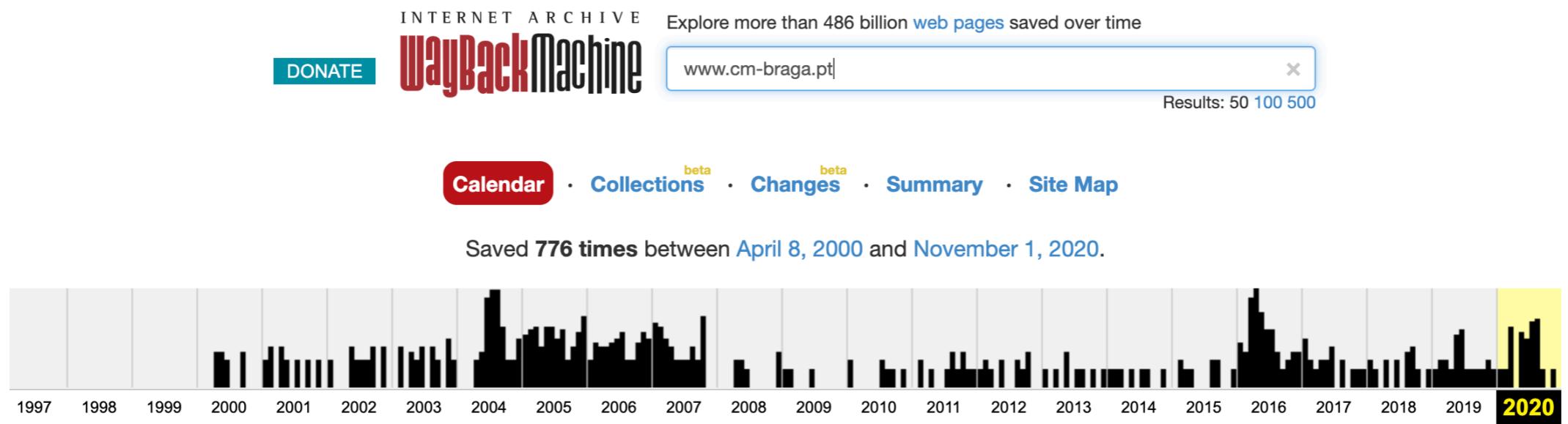
unu.edu › experts › joao-marco-silva › **João Marco Silva - United Nations University**
João Marco Silva is a Visiting Fellow at UNU-EGOV and an Assistant Researcher at INESC TEC – Institute for Systems and Computer Engineering, Technology ...

www.researchgate.net › profile › Joa... › [Translate this page](#)
João Marco SILVA | Research Assistant | PhD in Informatics ...
João Marco Cardoso Silva. Monitoring current communication networks and services is an increasingly complex task as a result of a growth in the number and ...



Pentest - Reconnaissance

- Example - archive.org





Pentest - Reconnaissance

- Example - Job vacancy

Windows Administrator (.Net/Java)

Apply Now Save

Job Company

Must Have:

- Minimum of 5 years of confirmed expertise and working experience in:
 - Windows Server 2008 / 2012r2 / 2016 administration in large infrastructures
 - Very good knowledge of server hardware layers, especially HP, and the surrounding environment (LAN, SAN, etc ...)
 - Ability to design and develop IT solutions (VB script, Windows Shell, PowerShell).
 - Ability to automate and script in order to keep all administration actions simple and standard
 - Microsoft Windows Active Directory administration (infra, GPO), DNS, DHCP, IIS, cluster, middleware (Dotnet, Java), WSUS.
 - Microsoft Windows Platforms (SCOM, SharePoint, IIS, .NET,...)
 - PowerShell scripting and other languages
 - Configuration and managing of remote servers
- Knowledge of Puppet would be a plus
- Knowledge in Symantec AV and TSM Backup · ServiceNow · IPC knowledge

Senior Vmware Administrator

Apply Now Save

Job Company Rating Salary Benefits

Required qualifications to be successful in this role

Must Have minimum of 3 years of confirmed expertise and working experience in:

- Virtualization expert for ESX and Vmware environment (versions: 6 / 6.5 / 6.7)
- Good knowledge of Vrealize (Vrops) tools
- Proven experience in IT production environment (incident, 24H/7 on duty, early morning organization) , with DRP architecture.
- A good experience on Vmware migration & upgrade.
- Hyperconvergent solution skills is appreciated : Nutanix, VSAN, VRA, ..
- Audit and security skills.
- Scripting skills and automation.
- Strong general knowledge in IT and Datacenter infrastructure architectures



Pentest - Reconnaissance

- Example - Whois DB

```
[jotamarco@macbookpro ~ % whois scanme.nmap.org
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:      whois.pir.org
domain:     ORG

organisation: Public Interest Registry (PIR)
address:    11911 Freedom Drive 10th Floor,
address:    Suite 1000
address:    Reston, VA 20190
address:    United States

contact:    administrative
name:       Director of Operations, Compliance and Customer Support
organisation: Public Interest Registry (PIR)
address:    11911 Freedom Drive 10th Floor,
address:    Suite 1000
address:    Reston, VA 20190
address:    United States
phone:      +1 703 889 5778
fax-no:     +1 703 889 5779
e-mail:     ops@pir.org

contact:    technical
name:       Senior Director, DNS Infrastructure Group
organisation: Afiliias
address:    Building 3, Suite 105
address:    300 Welsh Road
address:    Horsham, Pennsylvania 19044
address:    United States
phone:      +1 215.706.5700
fax-no:     +1 215.706.5701
e-mail:     tld-tech-poc@afiliias.info
```

whois.domaintools.com

DOMAINTOOLS PROFILE ▾ CONNECT ▾ MONITOR ▾ SUPPORT Whois Lookup Q

— Website

Website Title	Account Suspended
Server Type	Apache/2.4.46 (cPanel) OpenSSL/1.1.1h mod_bwlimited/1.4
Response Code	200
Terms	14 (Unique: 12, Linked: 0)
Images	0 (Alt tags missing: 0)
Links	0 (Internal: 0, Outbound: 0)

Whois Record (last updated on 2020-11-19)

domain:	[REDACTED]
owner:	[REDACTED]
owner-c:	JMS770
tech-c:	BRCTA23
nserver:	dns1.ma9.com.br
nsstat:	20201119 AA
nslastaa:	20201119
nserver:	dns2.ma9.com.br
nsstat:	20201119 AA
nslastaa:	20201119
created:	20041217 #1917879
changed:	20191218
expires:	20211217
status:	published
nic-hdl-br:	JMS770
person:	Joao Marco Cardoso da Silva
created:	20051028
changed:	20190319
nic-hdl-br:	BRCTA23
person:	[REDACTED]
created:	20150930
changed:	20190514



Pentest - Reconnaissance

- Example - DNS

Using OS resolver

```
jotamarco@macbookpro ~ % host www.uminho.pt
www.uminho.pt has address 193.137.9.114
jotamarco@macbookpro ~ % dig www.uminho.pt

; <>> DiG 9.10.6 <>> www.uminho.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4776
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.uminho.pt.          IN      A

;; ANSWER SECTION:
www.uminho.pt.      14062   IN      A      193.137.9.114

;; Query time: 65 msec
;; SERVER: 192.168.86.1#53(192.168.86.1)
;; WHEN: Thu Nov 19 11:58:19 WET 2020
;; MSG SIZE rcvd: 58
```

nslookup with local DNS server

```
[jotamarco@macbookpro ~ % nslookup www.totalsem.com
Server:      192.168.86.1
Address:     192.168.86.1#53

Non-authoritative answer:
Name:   www.totalsem.com
Address: 34.200.194.131

[jotamarco@macbookpro ~ % nslookup server1.totalsem.com
Server:      192.168.86.1
Address:     192.168.86.1#53

** server can't find server1.totalsem.com: NXDOMAIN
```

Check if an IP address is a functioning DNS

```
[jotamarco@macbookpro ~ % nslookup
[> server 177.70.15.142
Default server: 177.70.15.142
Address: 177.70.15.142#53
[> www.uminho.pt
Server:      177.70.15.142
Address:     177.70.15.142#53

** server can't find www.uminho.pt: REFUSED
[> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
[> www.uminho.pt
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   www.uminho.pt
Address: 193.137.9.114
```



Pentest - Scanning

We will use the information acquired during the reconnaissance stage to shape probes and communicate directly with targets with the intent of identifying potential threats and vulnerabilities

- To do so, it is required to know
 - specifics about the Operating System (OS)
 - what services are available on the server
 - application version information
 - ...



Pentest - Scanning

- Passive vs Active scanning
 - a tradeoff between detectability and depth of information
 - Use public vulnerability databases to determine if the target system might be vulnerable to attack
 - In this phase, there is no exploiting activities
 - it is an auditing process aiming to identify which risks might exist - not to prove their existence



Pentest - Scanning

- Activity examples
 - check for live systems
 - check for open ports
 - scan beyond the IDS/Firewalls
 - banner grabbing
 - scan for vulnerabilities



Pentest - Scanning

- Tools
 - Nmap Security Scanner
 - Source <https://nmap.org/>
 - documentation <https://nmap.org/book/man.html>
 - vulnerability scanner
 - OpenVAS - <http://www.openvas.org/>
 - Nessus - <https://www.tenable.com/downloads/nessus>
 - Other tools might be used
 - <https://sectools.org/tag/app-scanners/>
 - <https://sectools.org/tag/web-scanners/>



Pentest - Scanning

- Port Scanning
 - verifying the existence of the target system
 - obtaining a list of communication channels (ports) that accept connections
 - identify what applications are on the communication channels



Pentest - Scanning

- Port scanning with nmap
 - checking for live systems
 - ICMP - Internet Control Message Protocol (using ping)
 - ICMP might be disabled (use nmap with -sn flag)
 - -sn -> nmap ping scan (-sP in older versions)



Pentest - Scanning

- Port scanning with nmap
 - Most of the interesting applications from a PenTest perspective use TCP to communicate
 - Web servers
 - file transfer applications
 - databases
 - Tools use the TCP three-way handshake to identify open ports

nmap -sS target

```
jotamarco@macbookpro ~ % sudo nmap -sS 192.168.86.200
Password:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 17:33 WET
Nmap scan report for 192.168.86.200
Host is up (0.0044s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
873/tcp   open  rsync
3261/tcp  open  winshadow
5000/tcp  open  upnp
5001/tcp  open  commplex-link
50001/tcp open  unknown
50002/tcp open  iiimsf
```



Pentest - Scanning

- Different types of scan are supported aiming to avoid being identified by a firewall
 - ACK scan (-sA)
 - FIN scan (-sF)
 - Null scan (-sN)
 - Xmas Tree scan (-sX)



Pentest - Scanning

- System identification
 - most application exploits are written for specific OS, so finding out the running OS is essential to identify possible vulnerabilities on the target

```
# nmap -O target
```
 - Passive OS fingerprinting
 - capturing TCP packets and analysing TTL information in order to identify manually the OS
 - Application banner also might provide such information



Pentest - Scanning

- Services identification
 - Banner
 - connecting to an unknown service on a port and checking if that port provides information about the service itself
 - with nmap, use the `-sV` flag

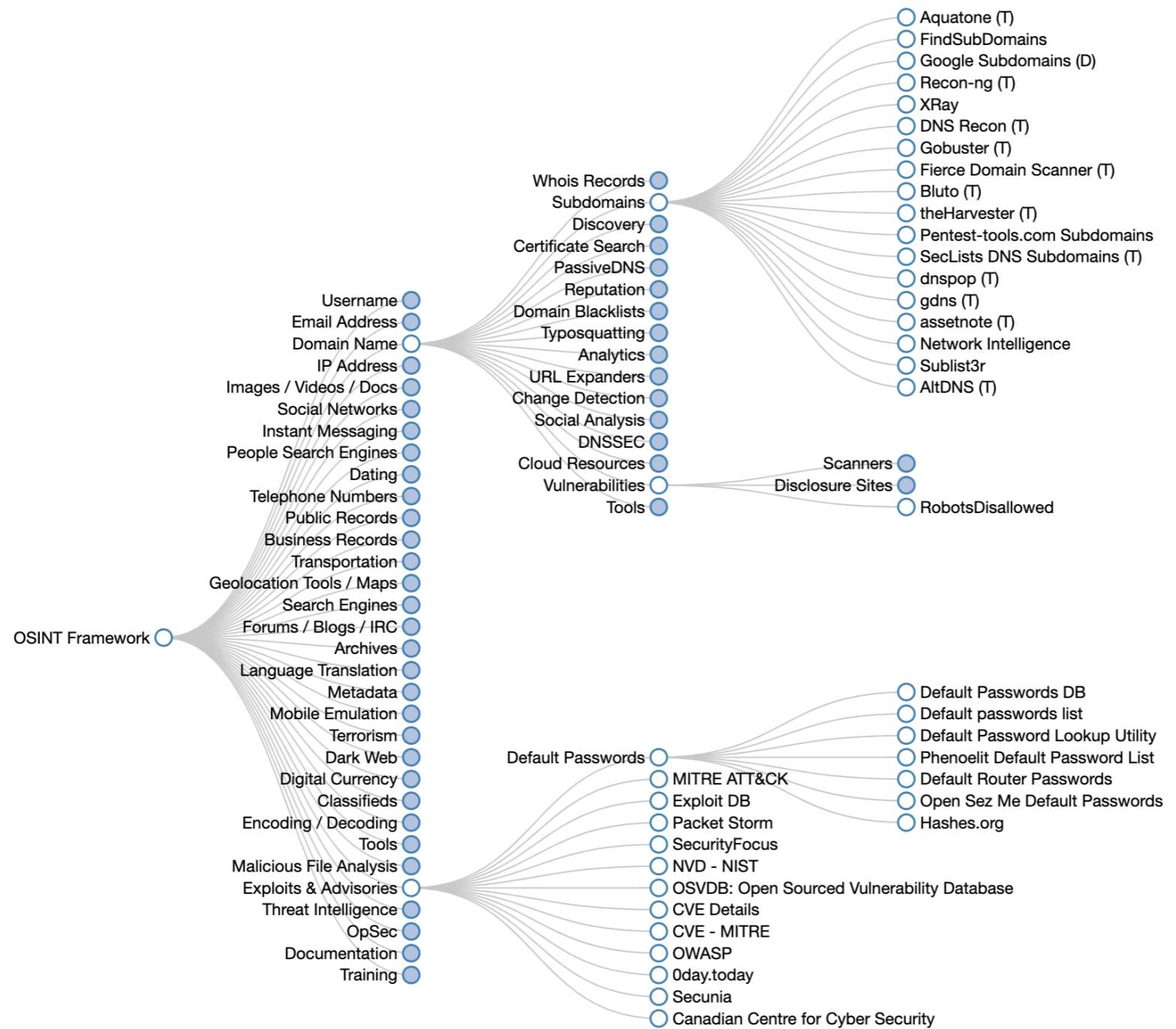
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 17:35 WET
Nmap scan report for 192.168.86.200
Host is up (0.0038s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
80/tcp    open  http         nginx
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: BACKUPS)
443/tcp   open  ssl/http    nginx
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: BACKUPS)
873/tcp   open  rsync
3261/tcp  open  iscsi        Synology DSM Snapshot Replication iSCSI LUN
5000/tcp  open  http         nginx
5001/tcp  open  ssl/http    nginx
50001/tcp open  upnp        Portable SDK for UPnP devices 1.6.21 (Linux 4.4.59+; UPnP 1.0)
50002/tcp open  http         lighttpd 1.4.43
```

- Packet analysis
 - analysing TCP/IP stack from captured packets and matching the data to known services



Pentest - Footprinting

- OSINT: Open-source intelligence framework





Pentest - Footprinting

- OSINT resources in cybersecurity

1	OSINT Framework	14	Creepy
2	CheckUserNames	15	Nmap
3	HavelbeenPwned	16	WebShag
4	BeenVerified	17	OpenVAS
5	Censys	18	Fierce
6	BuiltWith	19	Unicornscan
7	Google Dorks	20	Foca
8	Maltego	21	ZoomEye
9	Recon-Ng	22	Spyse
10	theHarvester	23	IVRE
11	Shodan	24	Metagoofil
12	Jigsaw	25	Exiftool
13	SpiderFoot		

 SecurityTrails