Recon

Possible methods of discovery

- Revealed by target organization personnel
- Discovered by Google search
- Discovered by DNS Zone Transfer
- Discovered by DNS reverse lookups
- Discovered during network sweep: ICMP type, TCP port(s), UDP port(s)
- Discovered during wireless assessment or physical assessment
- Discovered by compromise of one host, allowing scans to find other hosts
- Numerous other methods

Tools

Recon-NG

Network

```
traceroute -n -p 443 8.8.8.8
```

```
nmap -Pn -sS 10.10.0.1 -p1-1024 --pack et- trace
```

`ping6 -I eth0 ff02::1` (multikast address all IPv6 nodes)

`ping6 -I eth0 ff02::2` (multikast address all IPv6 routers)

```
nmap -Pn -sV fe80:: 20c 0%eth0 --pack et- trace
```

```
nmap -n --scri pt= sshv1 --scri pt- trace 10.10.1 0.60
 -p22
```

Scapy

Metadata

Formats

pdf, doc, dot, docx, xls, xlt, xlsx, ppt, pot, pptx, jpg, jpeg, html/htm (comments, hidden forms)

Tools

ExifTool, FOCA, Strings

Get Data

```
wget -nd -r -R htm,ht ml, php ,as p,a spx,cgi -P /tmp/files [tgt_dom
ain]
wget -nd -r -A pdf,do c,d ocx ,xl s,xlsx -P /tmp/files [tgt_d omain]
```

Interesting Links

http://vulnerabilityassessment.co.uk/Penet-ration%20Test.html

https://makensi.es/stf/

www.whois.net

www.geektools.com

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com