Network Mapping

- CEG 6430/4430 Cyber Network Security
- Junjie Zhang
- junjie.zhang@wright.edu
- Wright State University

Network Mapping

Network Mapping is to identify (potentially vulnerable) devices on the network or the Internet.

Interchangeable Terms: i) Scanning and ii) Target Identification

Sample Questions:

- Is this IP address used?
- If so, any active services?
- If so, any known vulnerable service?

Network Mapping

Tools:

- ARP Scanning: arp-scan, netwox 72, nmap
- TCP Port Scanning: netcat, netwox, nmap
- IoT Scanning: Shodan
- Web Server Scanning: Google

ARP Scanning

ARP Scanning is to discover active MAC addresses in the subnet and associate each MAC address with its manufacturer.

- You can use `arp-scan -l`.
- I ran this in a virtual network of WSL. It only discovered the virtual gateway.

```
[jzhang@DESKTOP-DSVPHPI system32]$sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:15:5d:e5:16:91, IPv4: 172.31.104.107
Starting arp-scan 1.9.7 with 4096 hosts (https://github.com/royhills/arp-scan)
172.31.96.1     00:15:5d:97:a7:d6       Microsoft Corporation
```

ARP Scanning

- Use Wireshark to capture packets.

TCP Port Scanning

TCP Port Scanning is to send a TCP SYN packet to a port on an IP address:

- If SYN-ACK is replied, this IP-port is active.
- Otherwise, this IP-port is inactive.

A port number indicates (but cannot guarantee) the service.

- Examples: 20, 21, 22, 80, 443, 8080

TCP Port Scanning

Using `netcat` to scan a range of ports on a single IP

```
[jzhang@DESKTOP-DSVPHPI system32]$netcat -zv 172.31.104.107 1-7
netcat: connect to 172.31.104.107 port 1 (tcp) failed: Connection refused
netcat: connect to 172.31.104.107 port 2 (tcp) failed: Connection refused
netcat: connect to 172.31.104.107 port 3 (tcp) failed: Connection refused
netcat: connect to 172.31.104.107 port 4 (tcp) failed: Connection refused
netcat: connect to 172.31.104.107 port 5 (tcp) failed: Connection refused
netcat: connect to 172.31.104.107 port 6 (tcp) failed: Connection refused
netcat: connect to 172.31.104.107 port 7 (tcp) failed: Connection refused
```

Similarly, you can use `nmap` to scan a range of ports for a range of IPs.

TCP Port Scanning

- Use Wireshark to capture packets.

What can you learn from captured packets?

- Failed attempts.
  - How do you define a **failed** attempt?
    - ARP?
    - TCP?
- It is noisy and therefore easy to be observed.
  - How can you make it more stealthy?

Scanning: More Tools and/or Resources

- the ZMap Project
- censys data set

IoT Scanning

Shodan is a search engine that lets users search for various types of servers (webcams, routers, servers, etc.) connected to the internet using a variety of filters.

Shodan Developers Book View All...

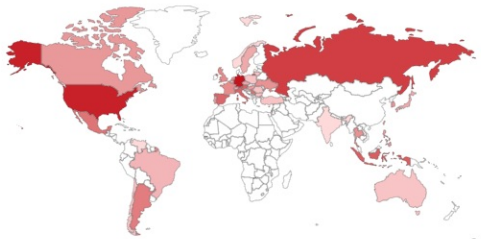
SHODAN webcam product:"webcam 7 httpd" Explore Downloads Reports Developer Pricing

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS

382

TOP COUNTRIES



Germany	68
United States	55
Russian Federation	34
Indonesia	20
Italy	18

TOP SERVICES

HTTP (8080)	234
HTTP	44
8081	35
AndroMouse	19
HTTP (81)	9

TOP ORGANIZATIONS

Deutsche Telekom AG	40
PT Telkom Indonesia	12
Telekom Austria	8
True Internet	6
Vodafone DSL	4

webcam 7
212.220.1.25
adsl-212-220-1-25.nojabrsk.ru
Rostelecom
Added on 2019-03-16 11:45:28 GMT
Russian Federation, Salekhard

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2186
Cache-control: no-cache, must revalidate
Date: Sat, 16 Mar 2019 11:45:08 GMT
Expires: Sat, 16 Mar 2019 11:45:08 GMT
Pragma: no-cache
Server: webcam 7
```

webcam 7
91.234.132.46
static-TB-132-46.kbcnet.rs
Privredno Drustvo Za Proizvodnju Promet I Usluge K
Added on 2019-03-16 11:19:42 GMT
Serbia, Beograd
Technologies:

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7925
Cache-control: no-cache, must revalidate
Date: Sat, 16 Mar 2019 11:19:41 GMT
Expires: Sat, 16 Mar 2019 11:19:41 GMT
Pragma: no-cache
Server: webcam 7
```

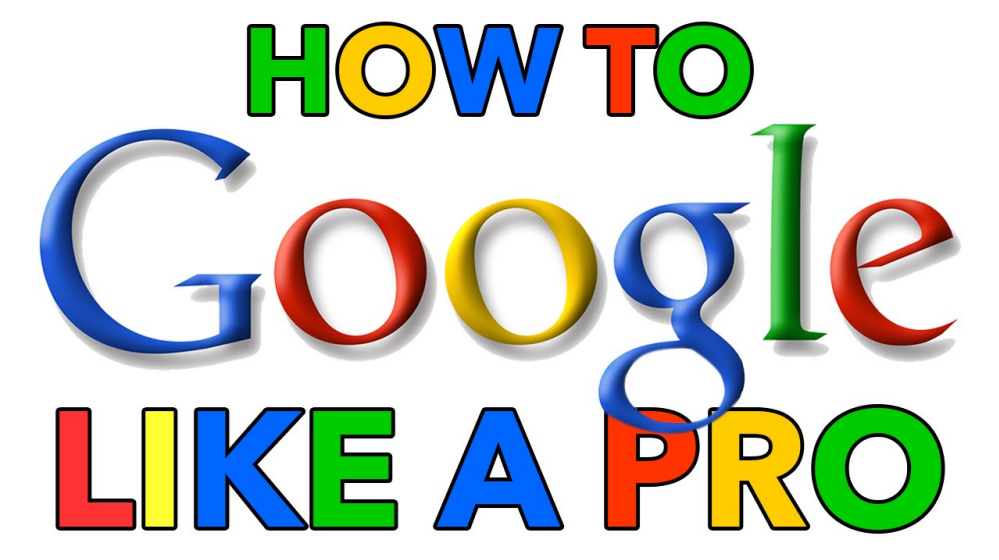
webcam 7
86.126.210.64
86-126-210-64.rdsnet.ro
RCS & RDS Business
Added on 2019-03-16 13:48:03 GMT
Romania, Cluj-napoca

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2186
Cache-control: no-cache, must revalidate
```


DS-2CD2420F-IW

Google

Do you know how to use Google?



Google

Do you really know how to use Google?

Please read this article before you answer this question.

WordPress Google Dorks: Find Vulnerabilities & Sensitive Data