Cyber Reconnaisance

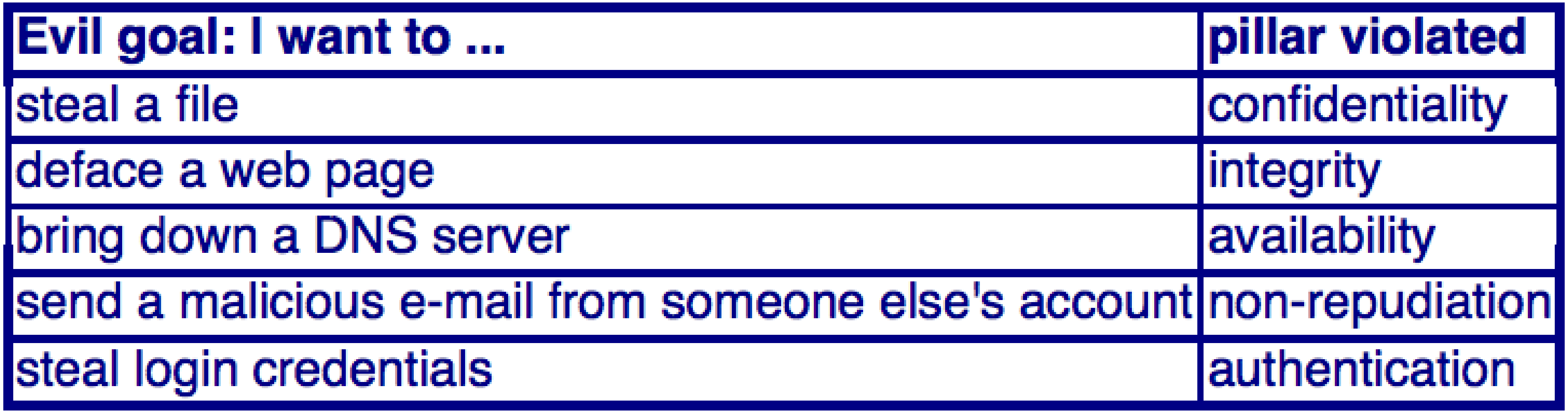
Review - Locard’s Exchange Principle

- Simply states:
  - In the commission of a crime, the perpetrator:
    - Leaves something at the crime scene
    - Takes away something from the crime scene
  - Evidence!

Review - Metadata

- That information in the file properties is metadata or data about data. It described the word document!
- Programs like Word embed this metadata in files.

Violating a Pillar of Cyber Security



Evil goal: I want to ...	**pillar violated**
steal a file	confidentiality
deface a web page	integrity
bring down a DNS server	availability
send a malicious e-mail from someone else's account	non-repudiation
steal login credentials	authentication

Security Tools for Defense

- Firewalls
- Encryption (symmetric and asymmetric)
- Hashing & Salting
- Password Authentication
- Digital Certificates

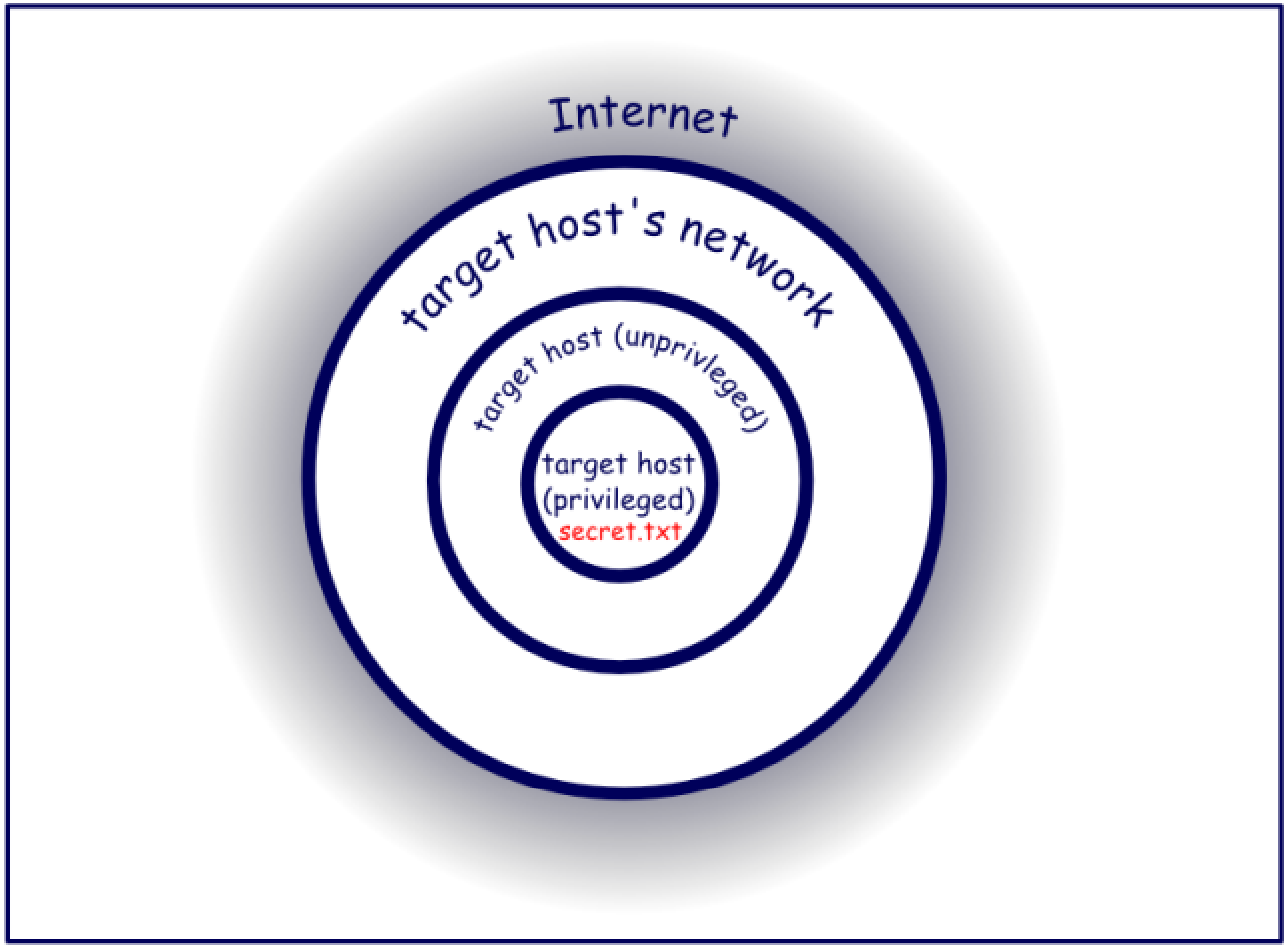
- These are all trying to protect the Pillars.

View from the attacker’s perspective

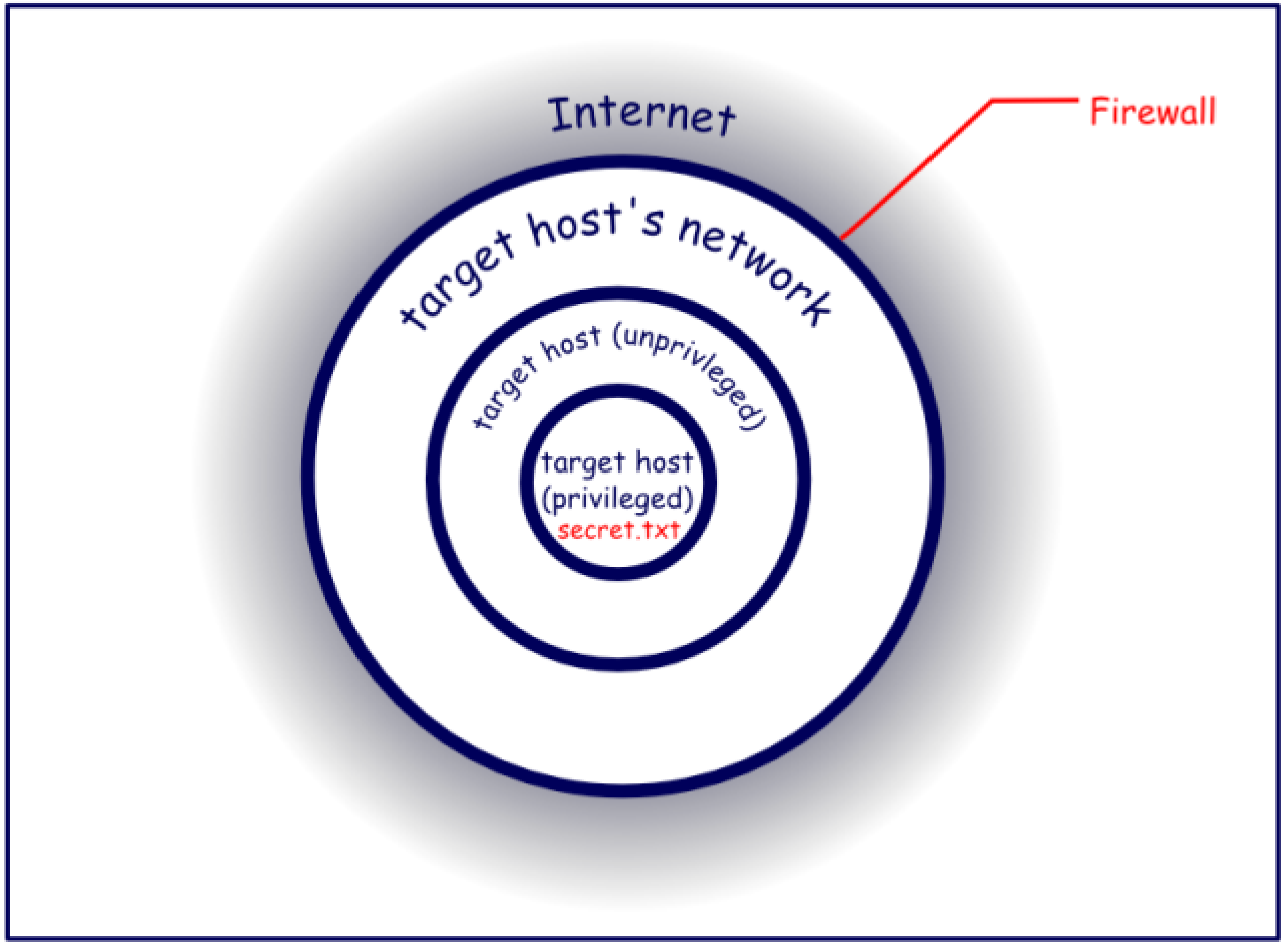
- If you want to attack a system, you need to violate a pillar.
- In order to violate a pillar, you need to defeat the tools that are being used to protect the pillar.

- If you are the attacker, and you look at a network, what do you see?

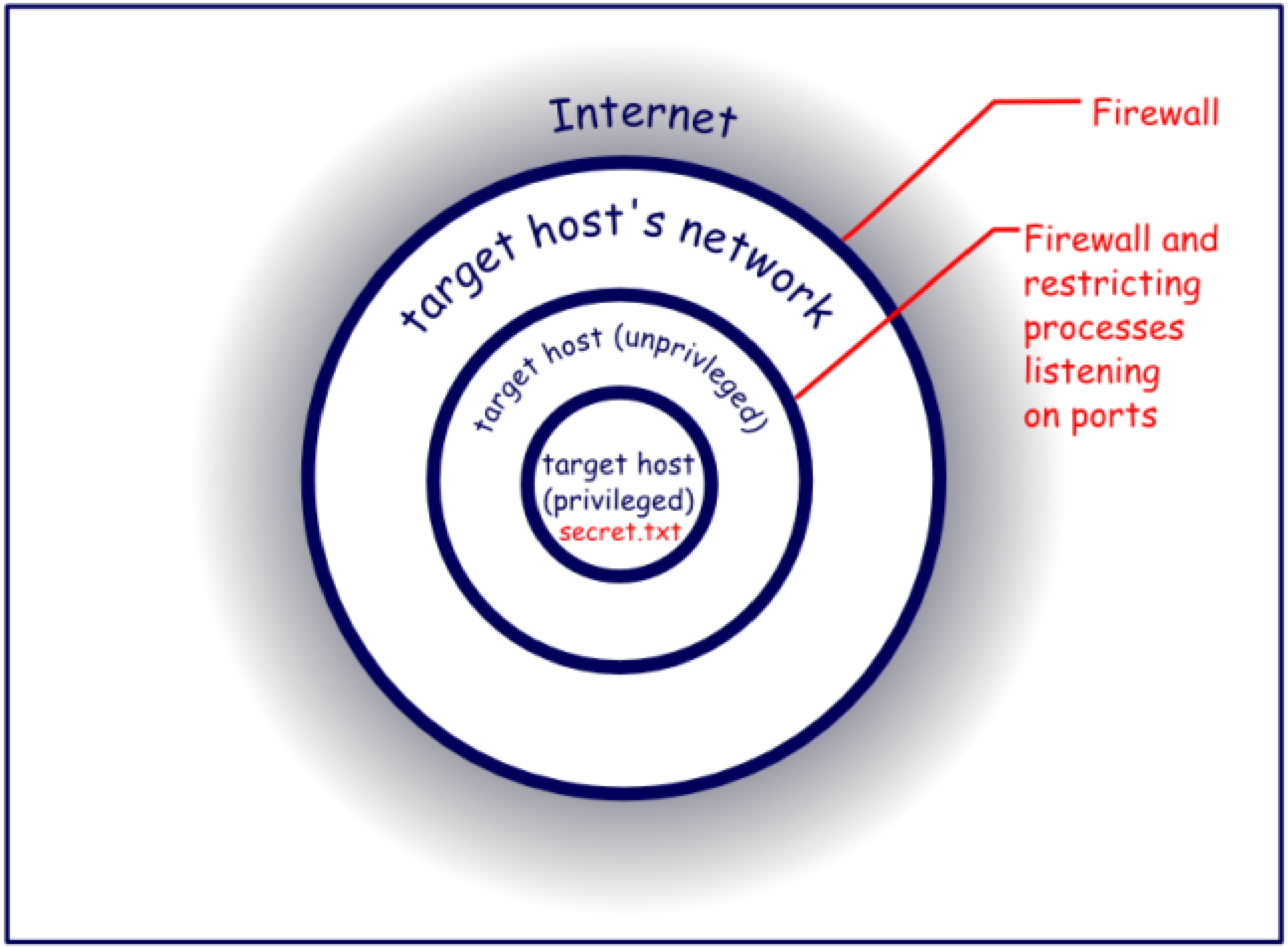
View from the attacker's perspective



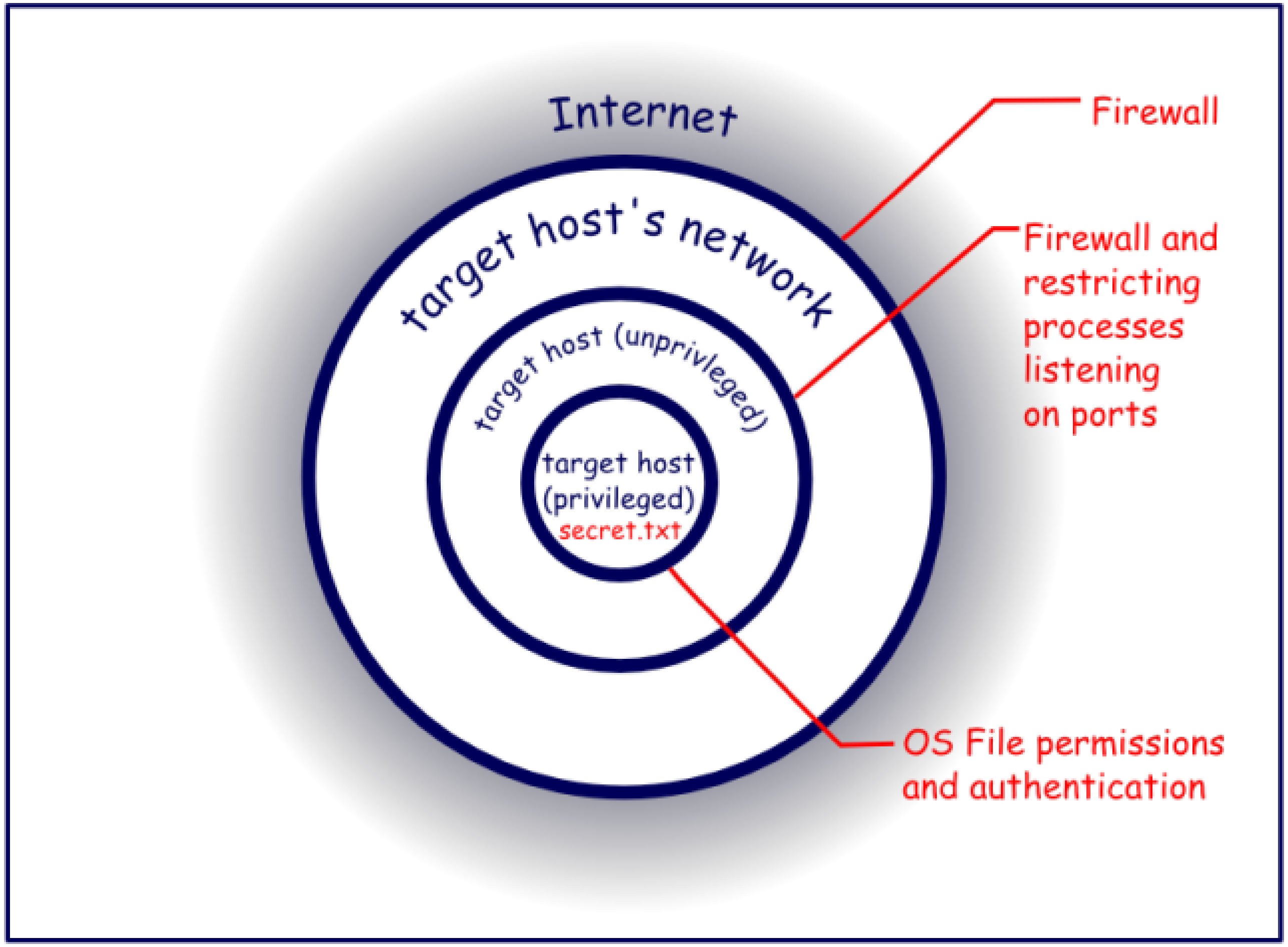
View from the attacker's perspective



View from the attacker's perspective



View from the attacker's perspective

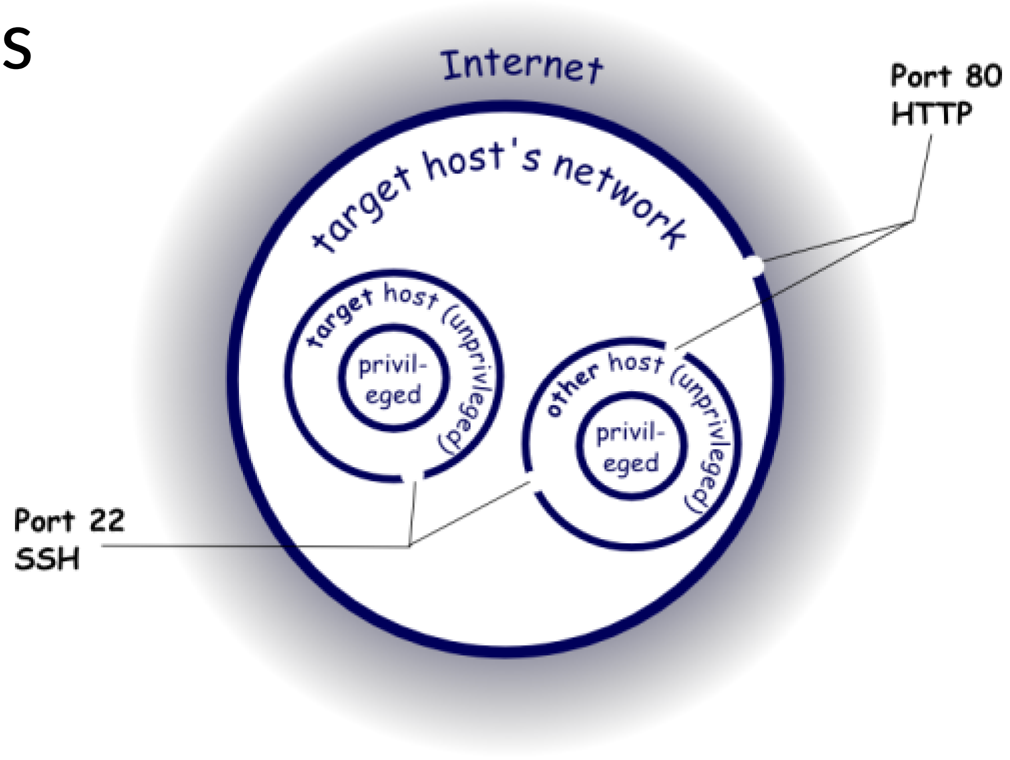


View from the attacker's perspective

- If you are the attacker, and you look at a network what do you see?
- There are multiple barriers in your way
  - Network Barrier (Outermost)
  - Host Barrier (Middle)
  - Privilege Barrier (Inside)

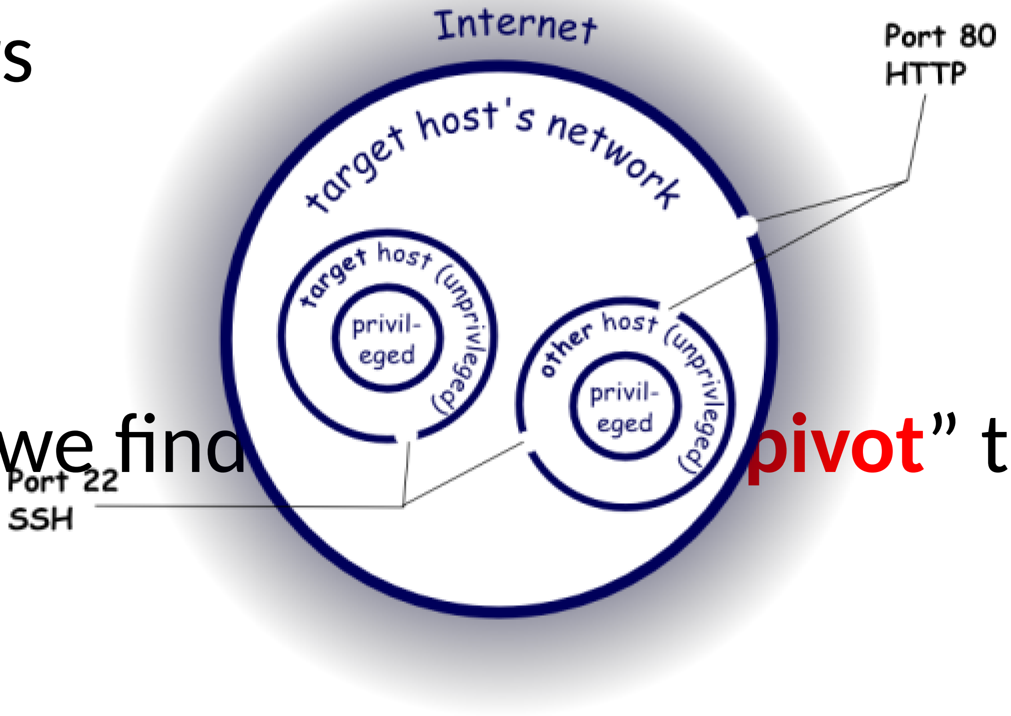
View from the attacker's perspective

- As an attacker we are looking for gaps in the barriers



View from the attacker's perspective

- As an attacker we are looking for gaps in the barriers



- When we find [illegible] **pivot**” to the target!

Three Basic Phases

- **Reconnaissance** – searching for the information to actually get in.
  - Firewall information, services, etc.
- **Infiltration** – Gain the access needed to achieve the goal
- **Exfiltrate & Maintain Access**
  - Obtain the goal
  - Hide the evidence
  - Maintain access

Reconnaissance

- What type of information would useful?

Reconnaissance

- What type of information would useful?
  - Network information
    - IPs , subnet mask, network topology, domain names
  - Host information
    - user names, groups, architecture, OS, services
  - Security policies
    - Password complexity requirements and change frequency
    - Expired / Disabled account retention
    - Physical security (locks, badges, etc.)
    - Firewalls
    - Intrusion Detection Systems
  - Human Information
    - Home Address, telephone, hangouts, hobbies, …

How do they get the info?

- Where would you find all of this information?

How do they get the info?

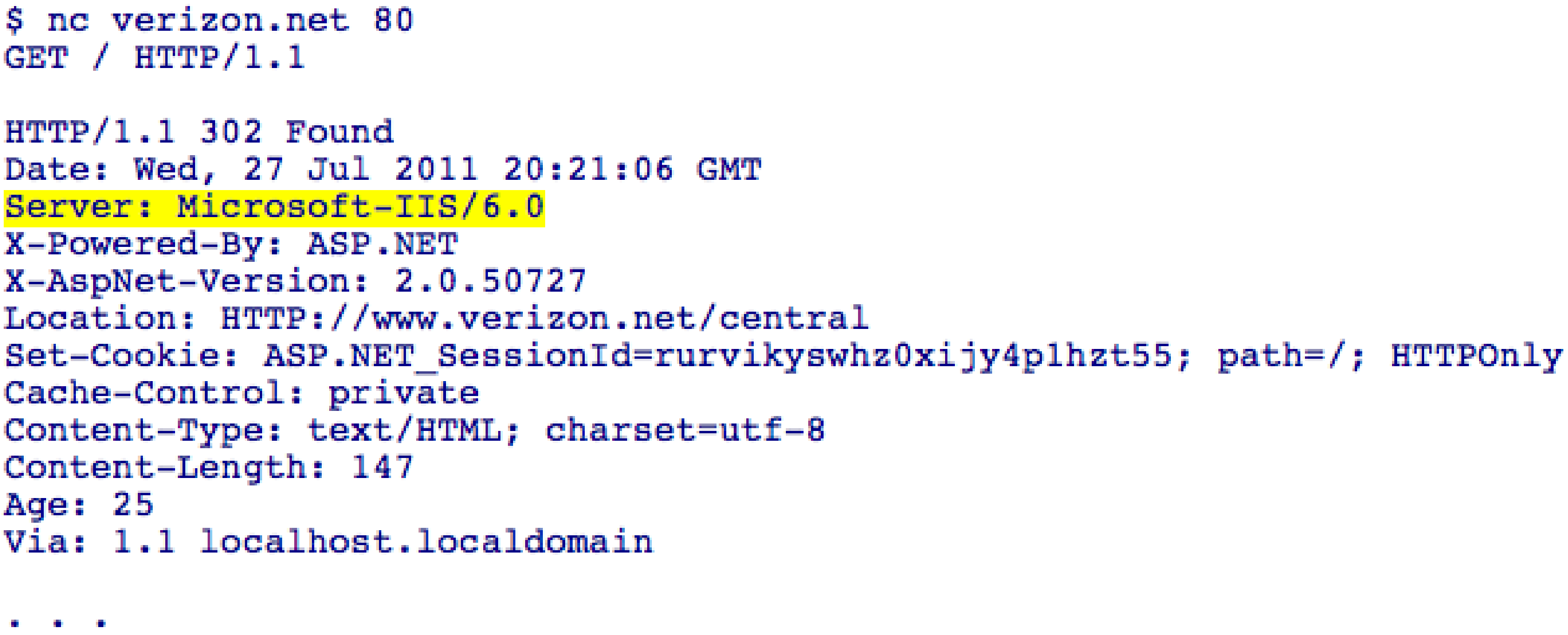
- Where would you find all of this information?
  - – Passive Reconnaissance
    - Banner Grabbing
      - Open Ports and Services
      - Inspecting with modern web browser
    - Google
    - Public Network Information
  - – Active Reconnaissance (scanning)
    - Common tools

How do they get the info?

- Passive Recon
  - Gathering information, often indirectly, in a manner unlikely to alert the subject of the surveillance.
  - Minimize interaction with the target network which may raise flags in the computer logs

Passive Recon

- Banner Grabbing: Open Ports and Services



```
$ nc verizon.net 80
GET / HTTP/1.1

HTTP/1.1 302 Found
Date: Wed, 27 Jul 2011 20:21:06 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Location: HTTP://www.verizon.net/central
Set-Cookie: ASP.NET_SessionId=rurvikyswhz0xijy4plhzt55; path=/; HTTPOnly
Cache-Control: private
Content-Type: text/HTML; charset=utf-8
Content-Length: 147
Age: 25
Via: 1.1 localhost.localdomain

. . .
```

Passive Recon

- Banner Grabbing: Web Browser

1) Open Google Chrome.
2) Open a new tab and go to a web page, on the web, of your choosing.
3) Open the Web Developer Console (Ctrl-Shift-J [Windows]).
4) Navigate to the Network pane.
5) Reload the web page (Ctrl-r).
6) In the tree view select one of the source documents in the Name column.
7) Select the Header tab.
8) Explore the information returned by the web server:
    - Remote Address: IP address of the web server.
    - Date: Date the server thinks it is, includes time zone location.
    - Server: Information about the web server program, and likely operating system of the web server.

Passive Recon

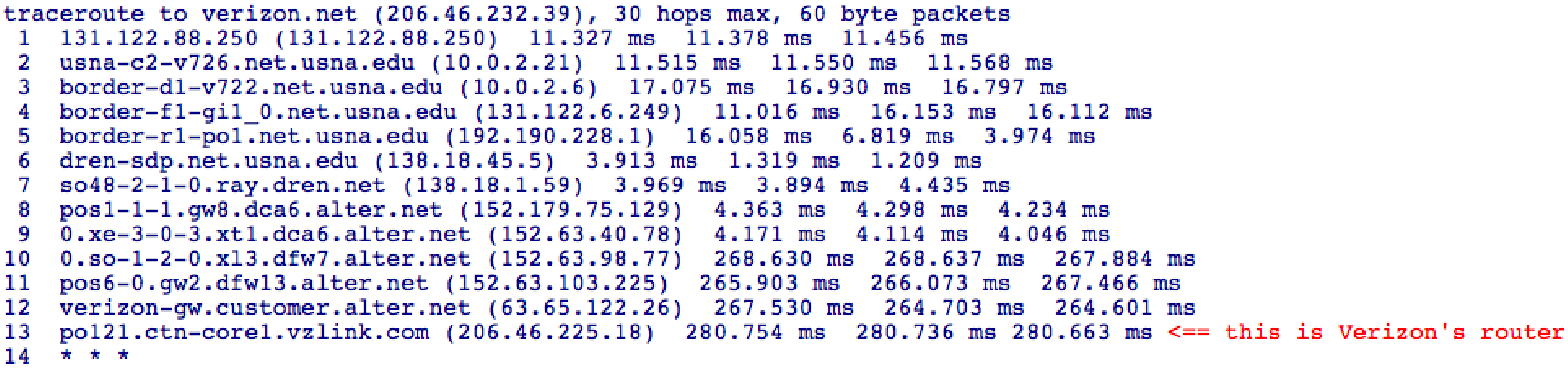
- Google
  - Free info
  - What can you learn about targeted users?
  -
- Public Network Information
  - All IP addresses and Domain Names are registered.

How do they get the info?

- Active Recon
  - Gathering information while interacting with the target directly
  - In a manner than can usually be discovered
  - Try all the doors and windows (IPs and ports)
  - Commonly called “scanning”

Active Recon

- Common Tools:
  - Ping
  - Traceroute
  - NMAP – The Network Mapper (will use in lab)



```
traceroute to verizon.net (206.46.232.39), 30 hops max, 60 byte packets
 1  131.122.88.250 (131.122.88.250)  11.327 ms  11.378 ms  11.456 ms
 2  usna-c2-v726.net.usna.edu (10.0.2.21)  11.515 ms  11.550 ms  11.568 ms
 3  border-d1-v722.net.usna.edu (10.0.2.6)  17.075 ms  16.930 ms  16.797 ms
 4  border-f1-gi1_0.net.usna.edu (131.122.6.249)  11.016 ms  16.153 ms  16.112 ms
 5  border-r1-po1.net.usna.edu (192.190.228.1)  16.058 ms  6.819 ms  3.974 ms
 6  dren-sdp.net.usna.edu (138.18.45.5)  3.913 ms  1.319 ms  1.209 ms
 7  so48-2-1-0.ray.dren.net (138.18.1.59)  3.969 ms  3.894 ms  4.435 ms
 8  pos1-1-1.gw8.dca6.alter.net (152.179.75.129)  4.363 ms  4.298 ms  4.234 ms
 9  0.xe-3-0-3.xt1.dca6.alter.net (152.63.40.78)  4.171 ms  4.114 ms  4.046 ms
10  0.so-1-2-0.xl3.dfw7.alter.net (152.63.98.77)  268.630 ms  268.637 ms  267.884 ms
11  pos6-0.gw2.dfw13.alter.net (152.63.103.225)  265.903 ms  266.073 ms  267.466 ms
12  verizon-gw.customer.alter.net (63.65.122.26)  267.530 ms  264.703 ms  264.601 ms
13  po121.ctn-core1.vzlink.com (206.46.225.18)  280.754 ms  280.736 ms 280.663 ms <== this is Verizon's router
14  * * *
```

Questions?