Kaitlin Hoffmann

Office Hours:

SH 243 Monday 1:15 - 3:15 PM. Tuesday 2:45 - 4:45 PM.

Email: hoffmank4@newpaltz.edu

RECONNAISSANCE

CYBERSECURITY

OBJECTIVES

- Reconnaissance
- Passive Recon
- Active Recon
- Passive Recon Tools
- Active Recon Tools

WHAT IS RECONNAISSANCE

- **Reconnaissance** is the information-gathering stage of ethical hacking, where you collect data about the target system.
- This data can include anything from network infrastructure to employee contact details. The goal of reconnaissance is to identify as many potential attack vectors as possible.
- Used in Ethical Hacking! Vital in penetration testing.
- https://www.comptia.org/blog/best-certifications-for-ethical-hackers
- https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh-v12/

DATA COLLECTED

Data collected from reconnaissance may include:

- **Security policies**: Knowing an organization's security policies can help you find weaknesses in their system.
- **Network infrastructure**: A hacker needs to know what type of network the target is using (e.g., LAN, WAN, MAN), as well as the IP address range and subnet mask.
- **Employee contact details**: Email addresses, phone numbers, and social media accounts can be used to launch social engineering attacks.
- **Host information**: Information about specific hosts, such as operating system type and version, can be used to find vulnerabilities.

PASSIVE RECONNAISSANCE

- In **passive reconnaissance**, you rely on publicly available knowledge. It is the knowledge that you can access from publicly available resources **without directly engaging** with the target.
- Think of it like you are looking at target territory from afar without stepping foot on that territory.
- Passive reconnaissance activities include many activities, for instance:
  - Looking up DNS records of a domain from a public DNS server.
  - Checking job ads related to the target website.
  - Reading news articles about the target company.

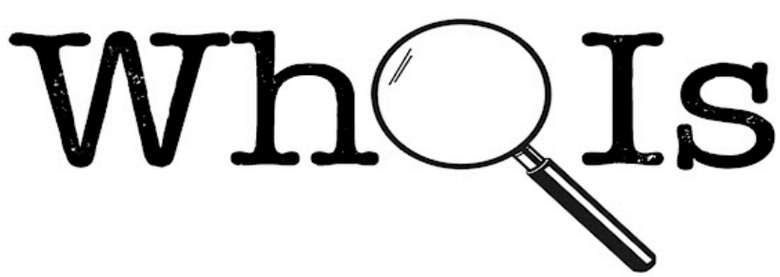
ACTIVE RECONNAISSANCE

- Active reconnaissance, on the other hand, cannot be achieved so discreetly. It requires **direct engagement** with the target.
- Think of it like you check the locks on the doors and windows, among other potential entry points.
- Examples of active reconnaissance activities include:
  - Connecting to one of the company servers such as HTTP, FTP, and SMTP.
  - Calling the company in an attempt to get information (social engineering).
  - Entering company premises pretending to be a repairman.

IMPORTANT: Due to the invasive nature of active reconnaissance, one can quickly get into legal trouble unless one obtains proper legal authorization.

PASSIVE RECONNAISSANCE TOOLS — WHOIS

- **WHOIS** is a public database that houses the information collected when someone registers a domain name or updates their DNS settings. A WHOIS server listens on TCP port 43 for incoming requests.
- ICANN, the International Corporation for Assigned Names and Numbers, regulates the WHOIS database: https://lookup.icann.org/en
- whois is a command-line utility used in Linux systems to retrieve information about domain names, IP addresses, and network devices.



WHOIS

- **Syntax:** `whois` *domainName*

- Can use this information to find new attack surfaces.

```
kaitlin@hydra:~$ whois newpaltz.edu
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

----------------------------------------------------------

Domain Name: NEWPALTZ.EDU

Registrant:
        State University of New York at New Paltz
```

WHOIS

- How can an attacker use this information to their advantage?

- We have the admin's name; can use social engineering on students, faculty, staff, etc.

- We know the DNS server is Azure; can look up potential vulnerabilities to exploit. Can use to execute attack.

```
Domain Name: NEWPALTZ.EDU

Registrant:
        State University of New York at New Paltz
        Information Technology Services - HAB 50
        1 Hawk Drive
        New Paltz, NY 12561
        USA

Administrative Contact:
        John Reina
        SUNY New Paltz
        IT Services - HAB 50
        1 Hawk Drive
        New Paltz, NY 12561
        USA
        +1.8452573685
        reinaj@newpaltz.edu

Technical Contact:
        Network Operations Center
        SUNY New Paltz
        IT Services - HAB 50
        1 Hawk Drive
        New Paltz, NY 12561
        USA
        +1.8452573130
        noc@newpaltz.edu

Name Servers:
        NS3-09.AZURE-DNS.ORG
        NS4-09.AZURE-DNS.INFO
        NS2-09.AZURE-DNS.NET
        NS1-09.AZURE-DNS.COM

Domain record activated:    30-Apr-1990
Domain record last updated: 14-Jun-2023
Domain expires:             31-Jul-2025
```

PASSIVE RECONNAISSANCE TOOLS — NSLOOKUP

- **nslookup** is a command-line tool to discover the IP address or DNS record of a specific domain name. It also allows for reverse DNS lookup, letting you find the domain attached to an IP address.
- NsLookup.io is a web based DNS lookup application.
- In the command line, the simplest command to find the IP address of a domain name is: `nslookup` *`domainName`*

```
kaitlin@hydra:~$ nslookup newpaltz.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   newpaltz.edu
Address: 137.140.1.48
```

NSLOOKUP

- You can add extra parameters with nslookup:

```
nslookup OPTIONS DOMAIN_NAME SERVER
```

- **OPTIONS** contains the query type as shown in the table in the next slide. Example, you can use A for IPv4 addresses and AAAA for IPv6 addresses.
- **DOMAIN_NAME** is the domain name you are looking up.
- **SERVER** is the DNS server that you want to query. You can choose any local or public DNS server to query. Example:
  - Cloudflare – 1.1.1.1 and 1.0.0.1
  - Google – 8.8.8.8 and 8.8.4.4

NSLOOKUP — OPTIONS

Query type	Result
A	IPv4 Addresses
AAAA	IPv6 Addresses
CNAME	Canonical Name
MX	Mail Servers
SOA	Start of Authority
TXT	TXT Records

```
user@TryHackMe$ nslookup -type=A tryhackme.com 1.1.1.1
```

NSLOOKUP — MORE EXAMPLES

- As shown below, tryhackme has three IP addresses.
- Each of these IP addresses can be further checked for insecurities, assuming they lie within the scope of the penetration test.

```
[kaitlin@hydra:~$ nslookup -type=a tryhackme.com 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
Name:   tryhackme.com
Address: 104.22.54.228
Name:   tryhackme.com
Address: 172.67.27.10
Name:   tryhackme.com
Address: 104.22.55.228
```

NSLOOKUP — MORE EXAMPLES

- Below we can see newpaltz uses outlook for their mail server. (We obviously know this, but an attacker may not)
- Outlook would be difficult to attack successfully, but if a smaller company creates their **own** mail server, it may not be adequately secured or patched.

```
kaitlin@hydra:~$ nslookup -type=mx newpaltz.edu 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
newpaltz.edu    mail exchanger = 10 newpaltz-edu.mail.protection.outlook.com.
```

PASSIVE RECONNAISSANCE TOOLS — DIG

- For more advanced DNS queries and additional functionality, you can use **dig (domain information groper)**.
- Simplest command to use: `dig` *`domainName`*

```
kaitlin@hydra:~$ dig newpaltz.edu

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> newpaltz.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25211
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;newpaltz.edu.                  IN      A

;; ANSWER SECTION:
```

PASSIVE RECONNAISSANCE TOOLS — DIG

- Like with nslookup, you can add extra parameters to specify what DNS server you want to query as well as the type:

```
dig SERVER DOMAIN_NAME TYPE
```

```
[kaitlin@hydra:~$ dig 1.1.1.1 newpaltz.edu MX

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> 1.1.1.1 newpaltz.edu MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 59990
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;1.1.1.1.                       IN      A

;; AUTHORITY SECTION:
.                       37834   IN      SOA     a.root-servers.net. nstld
```

PASSIVE RECONNAISSANCE TOOLS — DNSDUMPSTER

- DNS lookup tools, such as nslookup and dig, cannot find subdomains on their own.
- **Example:** if tryhackme.com has the subdomains *wiki.tryhackme.com* and *webmail.tryhackme.com*, you want to learn more about these two as they can hold a trove of information about your target.
- There is a possibility that one of these subdomains has been set up and is not updated regularly which usually leads to vulnerable services. But how can we know that such subdomains exist? **DNSDumpster** is one option.

DNSDUMPSTER

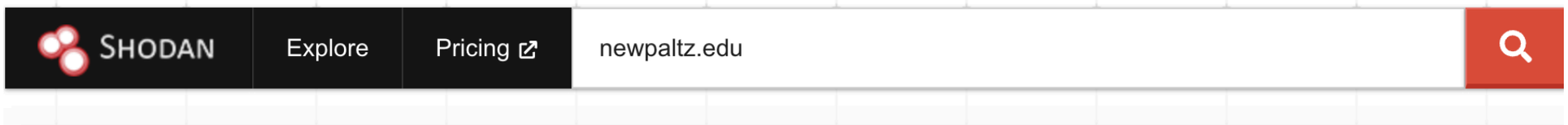
- DNSDumpster is a FREE domain research tool that can discover hosts related to a domain.
- Let's look up New Paltz's website with DNSDumpster...

PASSIVE RECONNAISSANCE TOOLS — SHODAN.IO

- Shodan is a search engine that lets users search for various types of servers connected to the internet using a variety of filters.
- Shodan.io collects information related to any device it can find connected online. Some information you may find:
  - IP address
  - hosting company
  - geographic location
  - server type and version

PASSIVE RECONNAISSANCE TOOLS — SHODAN.IO

- Check out New Paltz's website again!



TOTAL RESULTS

7

TOP PORTS

443	5
80	2

TOP ORGANIZATIONS

SUNY College at New Paltz	6
Microsoft Corporation	1

TOP PRODUCTS

Apache httpd	5
BigIP	2

View Report View on Map

Access Granted: Want to get more out of your existing Shodan account? Check

State University of New York at New Paltz

137.140.1.49
testwebapps.newpaltz.edu
my.newpaltz.edu
testmy.newpaltz.edu
www3.newpaltz.edu
webapps.newpaltz.edu
SUNY College at New Paltz
United States, New Paltz

SSL Certificate

Issued By:
|- Common Name:
Sectigo RSA Domain Validation Secure Server CA
|- Organization:
Sectigo Limited

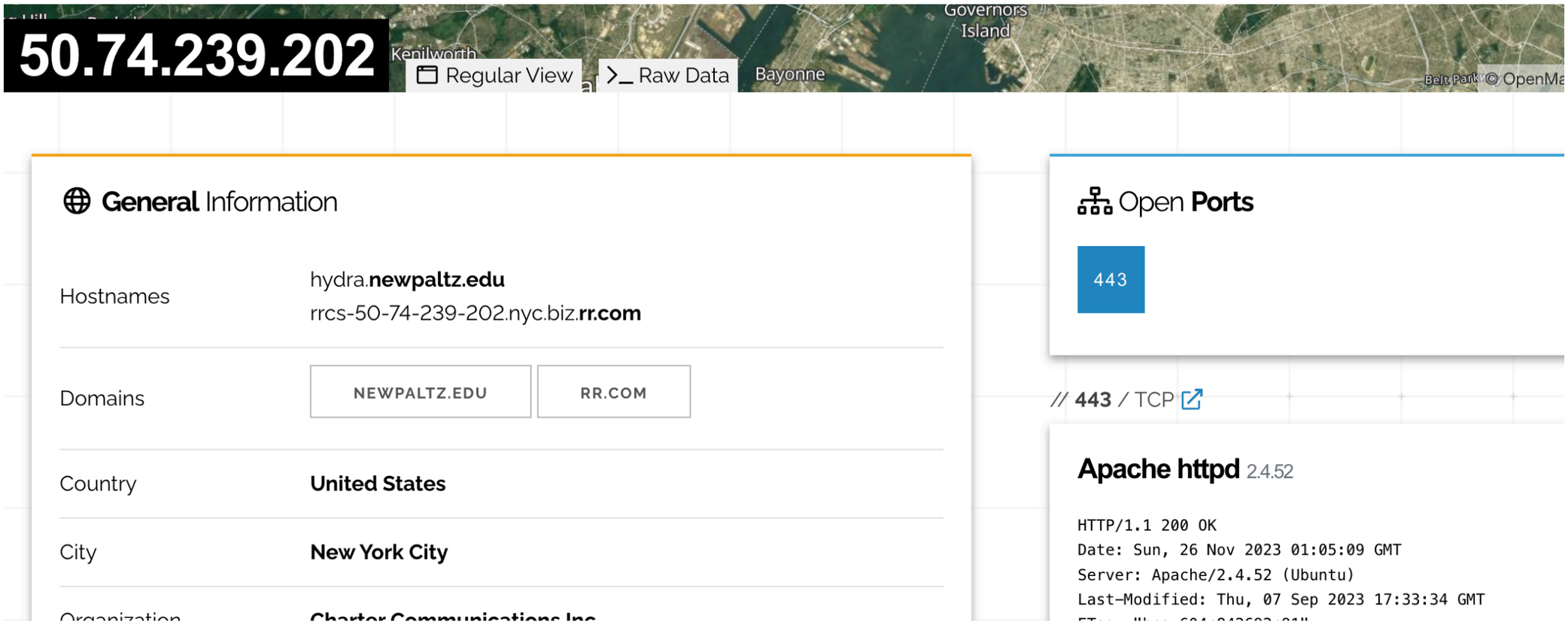
Issued To:
|- Common Name:
my.newpaltz.edu

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Sun, 26 Nov 2023 11:07:40 G
Server: Apache
Strict-Transport-Security: max-ag
Last-Modified: Mon, 20 Feb 2023 1
ETag: "159-5f522b2822de3"
Accept-Ranges: bytes
Content-Length: 345
X-FRAME-OPTIONS: SAMEORIGIN
Content-Security-P...
```

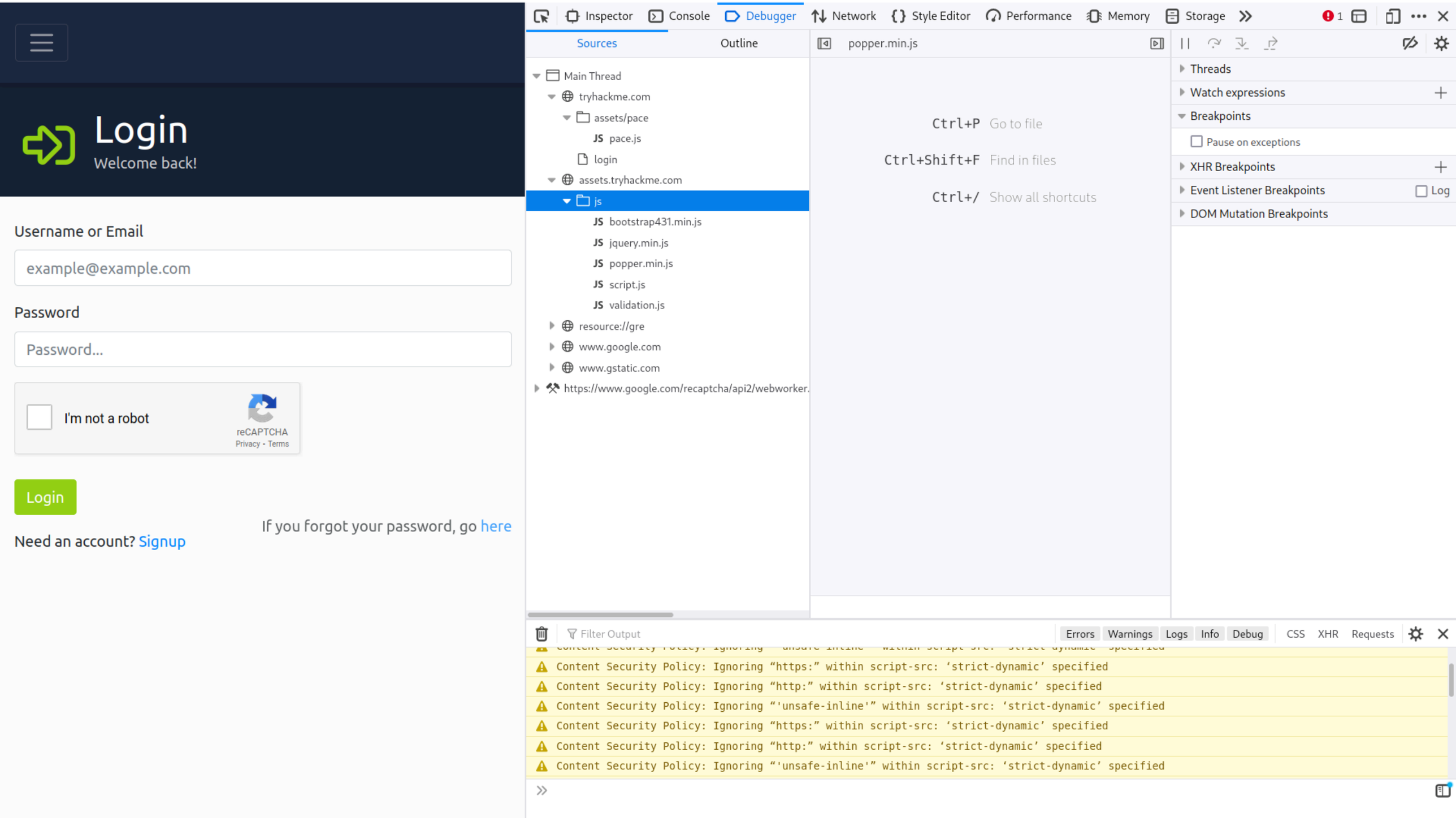
PASSIVE RECONNAISSANCE TOOLS — SHODAN.IO

- One reason why you may want to find the IP addresses is so you are able to find information using Shodan.
- For example, hydra.newpaltz.edu does not return any results in Shodan; *however*, hydra's IP address does!



ACTIVE RECON TOOLS – WEB BROWSER

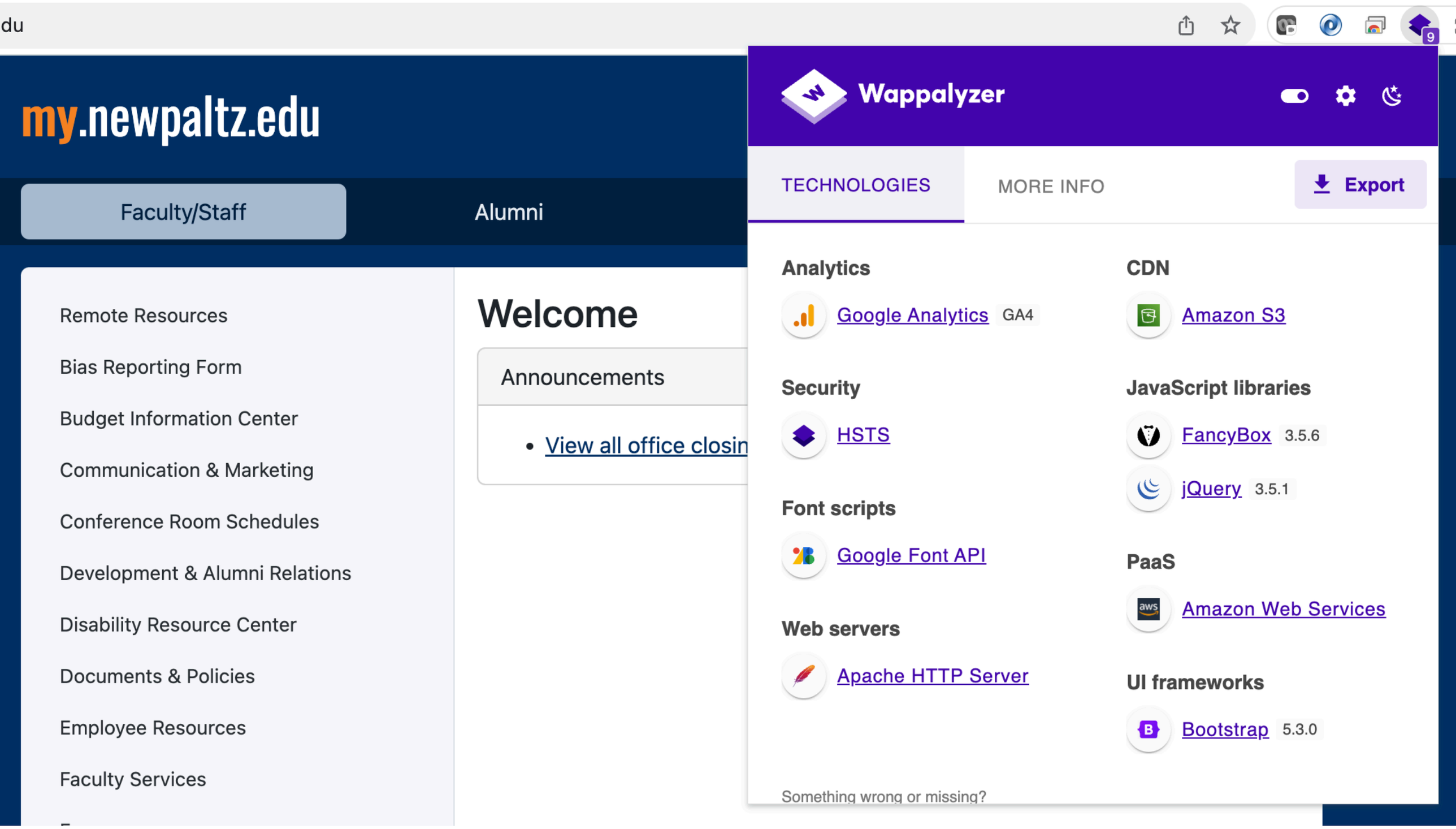
- While browsing a web page, you can press `Ctrl+Shift+I` on a PC or `Option+Command+I` (⌥ + ⌘ + I) on a Mac to open the Developer Tools on Firefox.
- Developer Tools lets you inspect many things that your browser has received and exchanged with the remote server.
- You can view and modify JavaScript files, inspect the cookies set on your system and discover the folder structure of the site content. Example…


Login
Welcome back!
Username or Email
example@example.com
Password
Password...
I'm not a robot
reCAPTCHA
Privacy - Terms
Login
Need an account? Signup
If you forgot your password, go here
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Sources
Outline
popper.min.js
Main Thread
tryhackme.com
assets/pace
pace.js
login
assets.tryhackme.com
js
bootstrap431.min.js
jquery.min.js
popper.min.js
script.js
validation.js
resource://gre
www.google.com
www.gstatic.com
https://www.google.com/recaptcha/api2/webworker.
Ctrl+P Go to file
Ctrl+Shift+F Find in files
Ctrl+/ Show all shortcuts
Threads
Watch expressions
Breakpoints
Pause on exceptions
XHR Breakpoints
Event Listener Breakpoints
Log
DOM Mutation Breakpoints
Filter Output
Errors
Warnings
Logs
Info
Debug
CSS
XHR
Requests
Content Security Policy: Ignoring “https:” within script-src: ‘strict-dynamic’ specified
Content Security Policy: Ignoring “http:” within script-src: ‘strict-dynamic’ specified
Content Security Policy: Ignoring “'unsafe-inline'” within script-src: ‘strict-dynamic’ specified
Content Security Policy: Ignoring “https:” within script-src: ‘strict-dynamic’ specified
Content Security Policy: Ignoring “http:” within script-src: ‘strict-dynamic’ specified
Content Security Policy: Ignoring “'unsafe-inline'” within script-src: ‘strict-dynamic’ specified

ACTIVE RECON TOOLS – WEB BROWSER

- Add-ons for Firefox and Chrome can help in penetration testing. Examples:
  - **FoxyProxy** lets you quickly change the proxy server you are using to access the target website. (A proxy server acts as a gateway between you and the internet.)
  - **User-Agent Switcher and Manager** gives you the ability to pretend to be accessing the webpage from a different operating system or different web browser.
  - **Wappalyzer** provides insights about the technologies used on the visited websites.

WAPPALYZER


du
my.newpaltz.edu
Faculty/Staff
Alumni
Remote Resources
Bias Reporting Form
Budget Information Center
Communication & Marketing
Conference Room Schedules
Development & Alumni Relations
Disability Resource Center
Documents & Policies
Employee Resources
Faculty Services
Welcome
Announcements
View all office closin
Wappalyzer
TECHNOLOGIES
MORE INFO
Export
Analytics
Google Analytics GA4
Security
HSTS
Font scripts
Google Font API
Web servers
Apache HTTP Server
CDN
Amazon S3
JavaScript libraries
FancyBox 3.5.6
jQuery 3.5.1
PaaS
Amazon Web Services
UI frameworks
Bootstrap 5.3.0
Something wrong or missing?

ACTIVE RECON TOOLS – PING

- **ping** is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.
- In simple terms, the ping command sends a packet to a remote system, and the remote system replies. This lets you know if the remote system is online.
- Simplest Command: `ping MACHINE_IP` or `ping HOSTNAME`

```
[kaitlinhoffmann ~ $ ping hydra.newpaltz.edu
PING hydra.newpaltz.edu (50.74.239.202): 56 data bytes
64 bytes from 50.74.239.202: icmp_seq=0 ttl=59 time=5.529 ms
64 bytes from 50.74.239.202: icmp_seq=1 ttl=59 time=13.585 ms
64 bytes from 50.74.239.202: icmp_seq=2 ttl=59 time=16.548 ms
64 bytes from 50.74.239.202: icmp_seq=3 ttl=59 time=15.756 ms
64 bytes from 50.74.239.202: icmp_seq=4 ttl=59 time=15.451 ms
64 bytes from 50.74.239.202: icmp_seq=5 ttl=59 time=16.864 ms
```

PING

- If you don't specify the count on a Linux system, you will need to hit CTRL+C to force it to stop.
- Instead, you can enter the amount of packets that will send. Example, to send only 10 packets: `ping -c 10 MACHINE_IP`

```
kaitlinhoffmann ~ $ ping -c 5 hydra.newpaltz.edu
PING hydra.newpaltz.edu (50.74.239.202): 56 data bytes
64 bytes from 50.74.239.202: icmp_seq=0 ttl=59 time=15.192 ms
64 bytes from 50.74.239.202: icmp_seq=1 ttl=59 time=14.983 ms
64 bytes from 50.74.239.202: icmp_seq=2 ttl=59 time=14.937 ms
64 bytes from 50.74.239.202: icmp_seq=3 ttl=59 time=17.880 ms
64 bytes from 50.74.239.202: icmp_seq=4 ttl=59 time=15.770 ms

--- hydra.newpaltz.edu ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 14.937/15.752/17.880/1.104 ms
```

PING

- Generally speaking, when we don't get a ping reply back, there are a few explanations that would explain why we didn't get a ping reply, for example:
  - The destination computer is not responsive; possibly still booting up or turned off, or the OS has crashed.
  - It is unplugged from the network, or there is a faulty network device across the path.
  - A firewall is configured to block such packets. The firewall might be a piece of software running on the system itself or a separate network appliance. Note that MS Windows firewall blocks ping by default.
  - Your system is unplugged from the network.

ACTIVE RECON TOOLS – TRACEROUTE

- The **traceroute** command ***traces*** the route taken by the packets from your system to another host.
- The purpose is to find the IP addresses of the routers or hops that a packet traverses as it goes from your system to a target host.
- This command also reveals the number of routers between the two systems.
- Command for Linux and Mac: `traceroute MACHINE_IP`.
- Command for Windows: `tracert MACHINE_IP`.

ACTIVE RECON TOOLS – TRACEROUTE

- In the traceroute output below, we have 10 numbered lines; each line represents one router/hop.

```
kaitlin@hydra:~$ traceroute tryhackme.com
traceroute to tryhackme.com (104.22.54.228), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  0.350 ms  0.308 ms  0.290 ms
 2  rrcs-50-74-239-201.nyc.biz.rr.com (50.74.239.201)  0.971 ms  0.954 ms  0.936 ms
 3  lag-101.mcr02nycmnywi.netops.charter.com (24.29.148.39)  3.913 ms  3.897 ms  3.879 ms
 4  lag-9.nyclnyrg01r.netops.charter.com (24.29.148.33)  5.929 ms  5.912 ms  5.894 ms
 5  lag-29.nwrknjmd67w-bcr00.netops.charter.com (107.14.19.24)  3.991 ms lag-19.nwrknjmd67w-bcr00
.charter.com (66.109.6.78)  3.991 ms lag-29.nwrknjmd67w-bcr00.netops.charter.com (107.14.19.24)  4
s
 6  lag-20.nycmny837aw-bcr00.netops.charter.com (66.109.5.138)  4.426 ms  4.550 ms lag-12.nycmny83
r00.netops.charter.com (66.109.6.27)  6.064 ms
 7  lag-1.pr2.nyc20.netops.charter.com (66.109.9.5)  5.407 ms lag-0.pr2.nyc20.netops.charter.com (
.5.119)  5.273 ms  5.396 ms
 8  * 162.158.61.22 (162.158.61.22)  5.076 ms *
 9  199.27.132.46 (199.27.132.46)  6.133 ms 172.70.112.4 (172.70.112.4)  6.387 ms 162.158.152.5 (1
.152.5)  4.566 ms
10  104.22.54.228 (104.22.54.228)  5.290 ms  5.273 ms  5.302 ms
kaitlin@hydra:~$ $
```

ACTIVE RECON TOOLS – TRACEROUTE

- If I am in Hydra, how many hops would I get if I entered **`traceroute hydra.newpaltz.edu`**?

```
kaitlin@hydra:~$ traceroute hydra.newpaltz.edu
traceroute to hydra.newpaltz.edu (50.74.239.202), 30 hops max, 60 byte packets
 1  rrcs-50-74-239-202.nyc.biz.rr.com (50.74.239.202)  0.334 ms  0.288 ms  0.307 ms
kaitlin@hydra:~$
```

One!

ACTIVE RECON TOOLS – TELNET

- Before there was SSH, there was TELNET (Teletype Network). However, TELNET sends all data as cleartext making it a security vulnerability (hence SSH was created).
- However, TELNET is useful for connecting to a service that runs TCP and access its banner (initial response after connecting to a service).
- Command Syntax: `telnet MACHINE_IP PORT`,

ACTIVE RECON TOOLS – TELNET

```
kaitlin@hydra:~$ telnet 50.74.239.202 80
Trying 50.74.239.202...
Connected to 50.74.239.202.
Escape character is '^]'.
GET / HTTP/1.1
host: telnet

HTTP/1.1 200 OK
Date: Thu, 30 Nov 2023 02:36:41 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Thu, 07 Sep 2023 17:33:34 GMT
ETag: "bca-604c842692c91"
Accept-Ranges: bytes
Content-Length: 3018
Vary: Accept-Encoding
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
```

- Example connecting to hydra web server. **80** is the port for HTTP.
- Need to ask for a page. GET / HTTP/1.1 will give us the home page. GET /*page*.html HTTP/1.1 will give us the specified page.
- Must enter a host, such as telnet.
- Hit enter twice.
- This tells us the server info! (Apache Server with Ubuntu OS).

ACTIVE RECON TOOLS – NETCAT

- Netcat is similar to Telnet, but Netcat supports **both** TCP and UDP protocols.
- It can:
  1. Function as a client that connects to a listening port
  2. Act as a server that listens on a port of your choice.
- Client Command Syntax: `nc MACHINE_IP PORT`

ACTIVE RECON TOOLS – NETCAT

- Below is an example from tryhackme. The output is similar giving us the server information (nginx/1.6.2):

```
pentester@TryHackMe$ nc MACHINE_IP 80
GET / HTTP/1.1
host: netcat

HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 17 Aug 2021 11:39:49 GMT
Content-Type: text/html
Content-Length: 867
Last-Modified: Tue, 17 Aug 2021 11:12:16 GMT
Connection: keep-alive
ETag: "611b9990-363"
Accept-Ranges: bytes
...
```

ACTIVE RECON TOOLS – NETCAT

- Command to have Netcat act as a server: `nc -lvnp PORT_NUMBER`
- On the *server* system, the port entered is the port you want to listen on. The options above mean the following:

option	meaning
-l	Listen mode
-p	Specify the Port number
-n	Numeric only; no resolution of hostnames via DNS
-v	Verbose output (optional, yet useful to discover any bugs)
-vv	Very Verbose (optional)
-k	Keep listening after client disconnects

ACTIVE RECON TOOLS – NETCAT

Server

```
kaitlin@hydra:~$ nc -vnlp 1234
Listening on 0.0.0.0 1234
Connection received on 127.0.0.1 57906
hi
```

Client

```
kaitlin@hydra:~$ nc 0.0.0.0 1234
hi
```

ASSIGNMENT 3 – LABS

- https://tryhackme.com/room/passiverecon
- https://tryhackme.com/r/room/activerecon
- Set up your virtual machine.