Black Hat Academy: *Cybersecurity From the Attacker's Perspective*

School Administrators of Montana

Ross Lemke
Privacy Technical Assistance Center (PTAC)

United States Department of Education
Student Privacy Policy Office
Privacy Technical Assistance Center

Disclaimer

This content was produced by the U.S. Department of Education’s Student Privacy Policy Office (SPPO) through its Privacy Technical Assistance Center (PTAC) for the purposes of this presentation. This presentation is provided for informational purposes only. Nothing in this presentation constitutes official policy or guidance from the U.S. Department of Education.

Official policy and guidance can be found on our website at https://studentprivacy.ed.gov/.

Who are we?

- PTAC is a technical assistance center under the Student Privacy Policy Office (SPPO)
- Provide guidance on FERPA, student privacy & data security
- Resources on our website: https://studentprivacy.ed.gov/
  - Trainings and Webinars
  - Documents
  - FAQs
- We are <u>not</u> the FERPA Police

Privacy Technical Assistance Center (PTAC)

Who We Are:

- One-stop resource to learn about data privacy, confidentiality, and security practices related to student data
- Operate Student Privacy Help Desk
- Develop privacy and security training materials
- Issue privacy and security best practice recommendations
- Conduct technical assistance site visits
- Host privacy-focused regional meetings and lessons learned forums

PTAC Resources

Visit our Website https://studentprivacy.ed.gov/ for great resources like

- *Online Training Modules*
  - FERPA 101
  - FERPA 201
- *Guidance Videos*
  - Email and Student Privacy
  - Communicating with Parents about Data Use and Security
- *Resource Documents*
  - Data Security & Data Breach Checklists
  - Incident Response Exercise Training Kits
- *Recorded Webinars*

Subscribe to our Newsletter!

The U.S. Department of Education is releasing new material all the time.

To stay abreast of these developments, please join our Student Privacy Newsletter: https://studentprivacy.ed.gov/subscribe-student-privacy-newsletter

Who Wants to Hack a School?

The Experts Agree… Schools are a Favorite Target of Cyber-Criminals, Hackers, and Ransomware Gangs!

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

The Cybersecurity & Infrastructure Security Agency (CISA) is the Federal Government agency responsible for protecting the national infrastructure from cyber threats. They have put out several reports and notices to schools about the increased cyber-threat!

Report: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats (2023)

K-12 Education Leaders’ Guide to Ransomware: Prevention, Response, and Recovery (2021)

Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data (2020)

The Problem

- Uncontrolled Internet facing applications & services
- Misconfiguration
- Bad Passwords & Permissions
- Legacy Software / Hardware

What is this session all about?

We talk about hackers, cyber-attackers, and ransomware gangs a lot…

but when things go wrong, we don’t really understand how this happened to us!

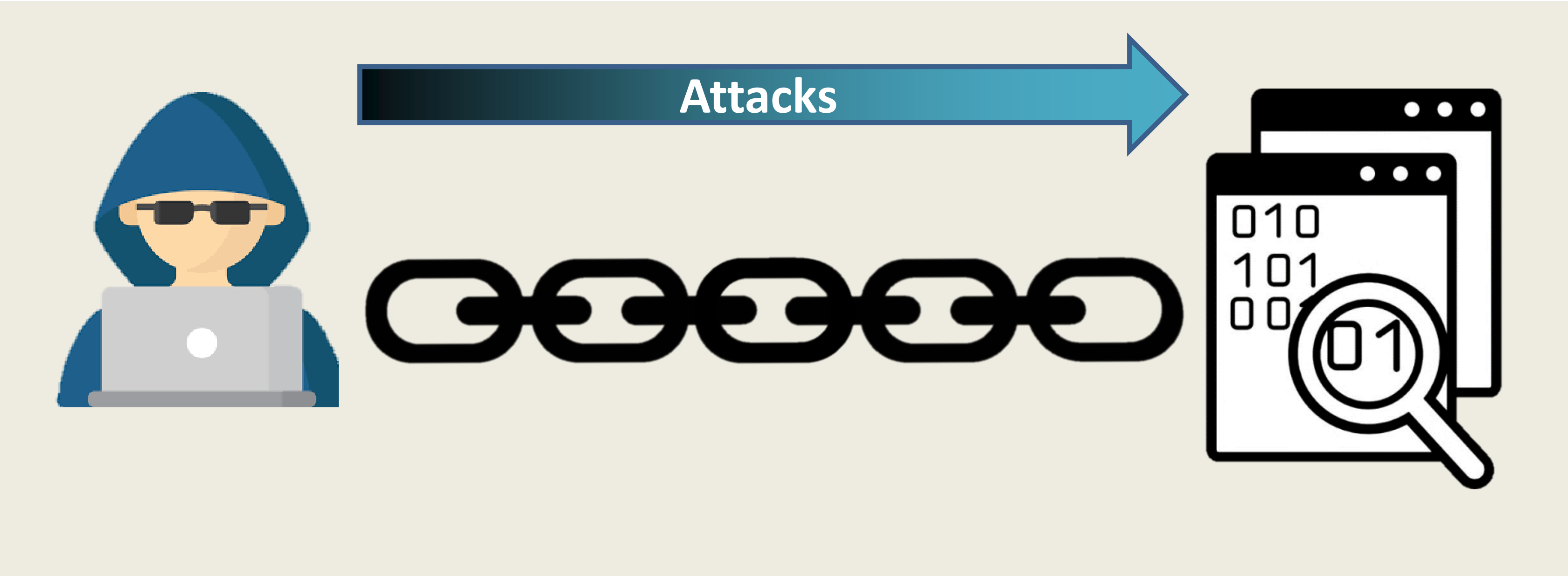
The Classical Phases of Cyber Intrusion

1. Reconnaissance *(passive & active)*
2. Exploitation
3. Establishing Persistence
4. Actions on Objective
5. Covering Tracks

This is sometimes referred to as the "Kill Chain"

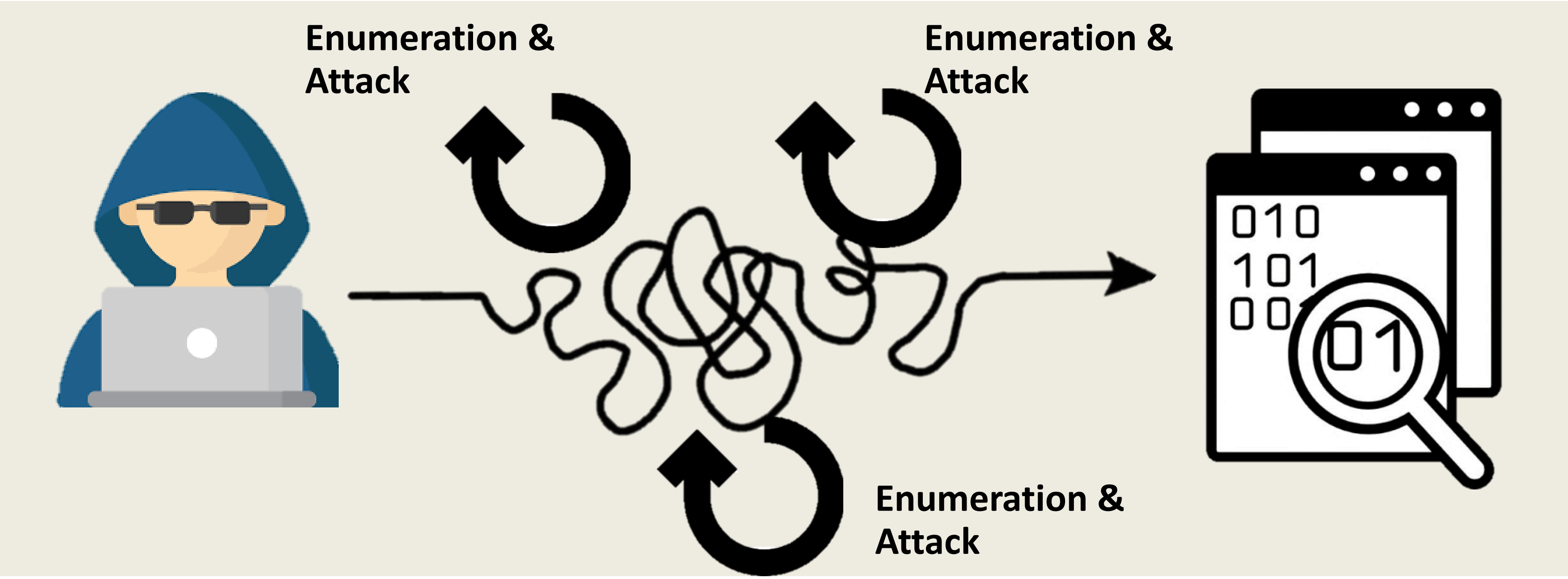
Attacks are not A -> B

Here's Where We Get it WRONG!



Attackers Iterate

Here's Where We Get it WRONG!



Enumeration & Attack

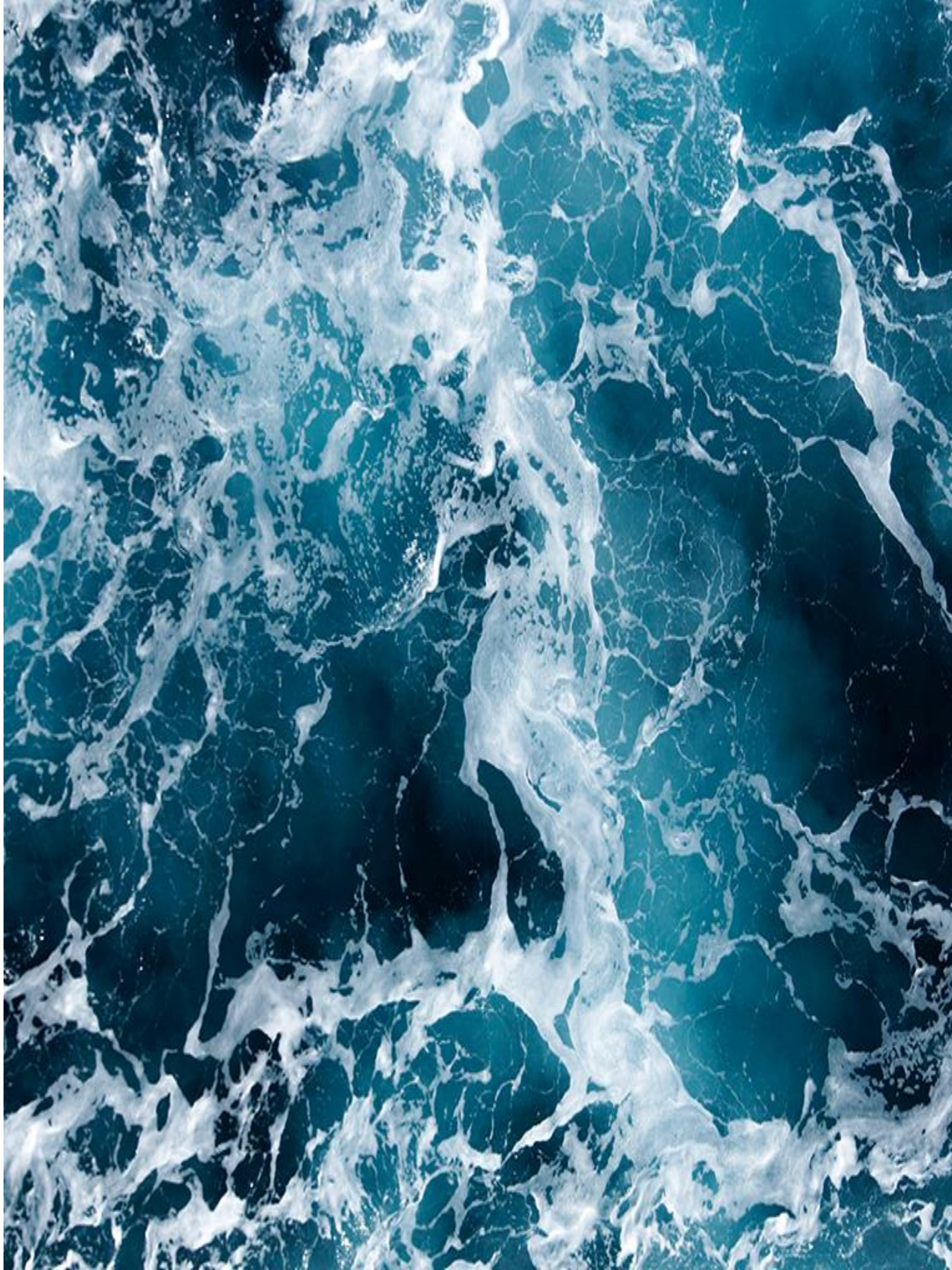
Enumeration & Attack

Enumeration & Attack

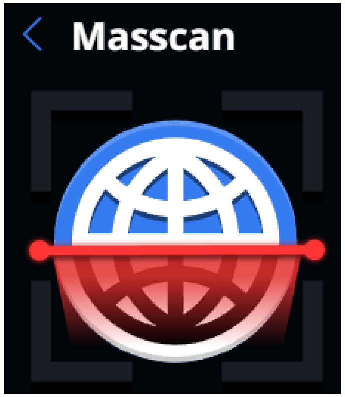
Hackers are Like Water

Looking for the Path of Least Resistance

- *Legacy Software*
- *Misconfiguration*
- *Human Error*
- *Social Engineering*
- *Reliable Exploits*



So How Do They Even Find this Stuff?

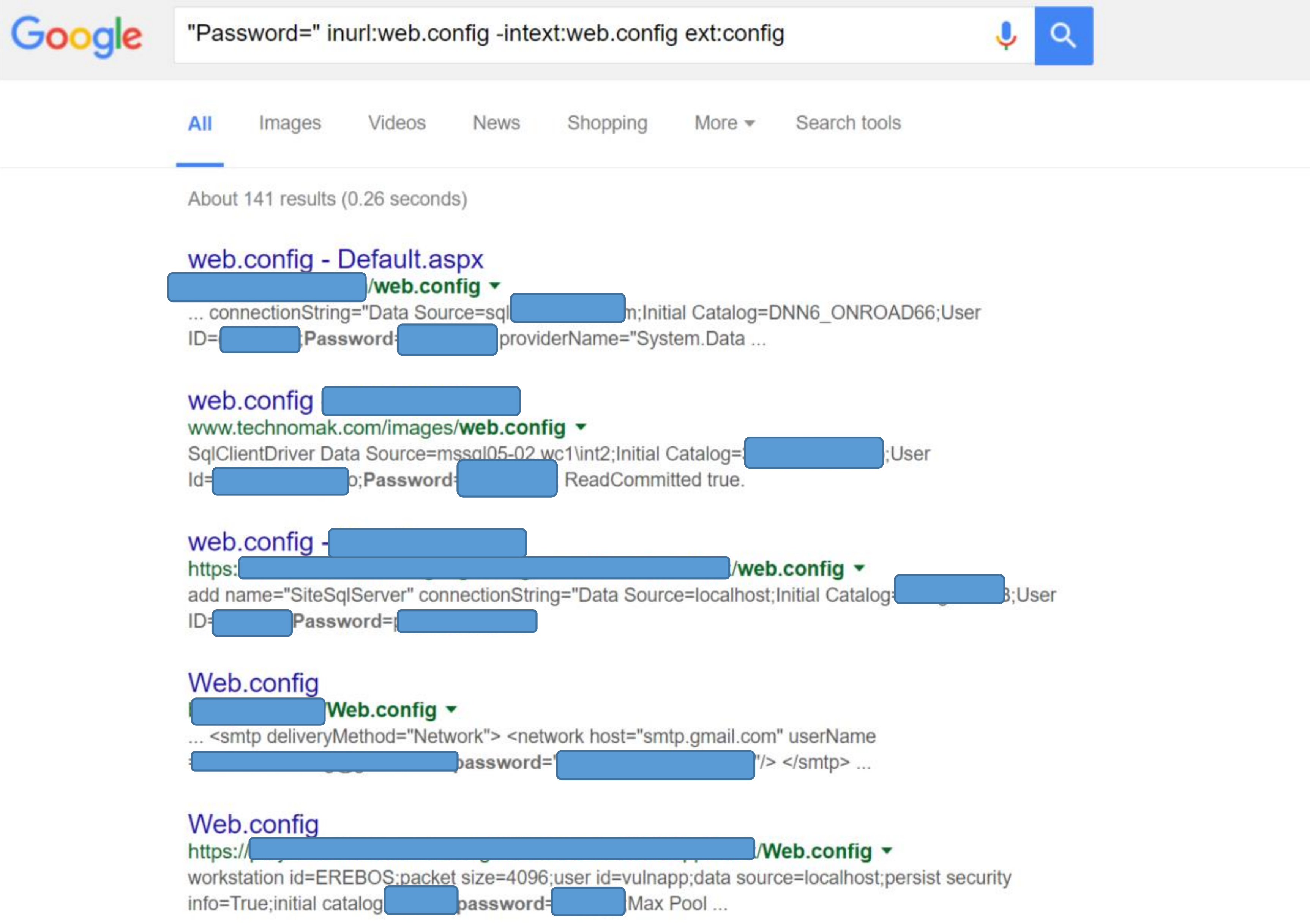


Let’s Talk Tools

#1 Search Engines for Fun & Profit

Google

a hacker’s best friend



"Password=" inurl:web.config -intext:web.config ext:config

About 141 results (0.26 seconds)

web.config - Default.aspx
[redacted]/web.config
... connectionString="Data Source=sql[redacted]m;Initial Catalog=DNN6_ONROAD66;User ID=[redacted];Password[redacted]providerName="System.Data ...

web.config [redacted]
www.technomak.com/images/web.config
SqlClientDriver Data Source=mssql05-02.wc1\int2;Initial Catalog=[redacted];User Id=[redacted]p;Password[redacted] ReadCommitted true.

web.config -[redacted]
https:[redacted]/web.config
add name="SiteSqlServer" connectionString="Data Source=localhost;Initial Catalog[redacted];User ID[redacted]Password=[redacted]

Web.config
[redacted]Web.config
... <smtp deliveryMethod="Network"> <network host="smtp.gmail.com" userName [redacted]assword="[redacted]"/> </smtp> ...

Web.config
https://[redacted]/Web.config
workstation id=EREBOS;packet size=4096;user id=vulnapp;data source=localhost;persist security info=True;initial catalog[redacted]password[redacted]Max Pool ...

Google Hack-Fu

Advanced Operators

- *Modify searches to limit the scope or content of returned information*
- *Some examples include:*

  “allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, related:, site:”

GHDB – Google Hacking Database

- A website that contains a library of pre-configured Google searches (Google Dorks)
- https://www.exploit-db.com/google-hacking-database
- Allows you to quickly build highly targeted searches to find "interesting" information
- Categories include things like "Files containing Passwords" and "Sensitive Directories" and "Vulnerable Servers"

Website Analysis - Passive

- View Source
- Identify links for folder structure, sensitive readable folders
- Looking for hardcoded variables, poorly secured code, comments
- Downloading and evaluating JS and CSS
- Looking for robots.txt

Website Analysis - Active (ie. Get authorization first)

- CMS & plugins Identification
  - Tools like Droopscan, CMSmap, WPScan, Joomscan, etc.
- Web scanners like Nikto
- Brute-force analysis (Dirbuster, etc.)
- Evaluating application request/response, fiddling with parameters (Burpsuite, etc.)

Ports, Protocols & Services

Identify all the exposed ports and associated services that are public facing

- Shodan.io and similar services index publicly facing ports and services
- Port scanning using NMAP, Unicorn, or even manually using Netcat or your favorite scripting language
- Look for vulnerabilities using a vulnerability scanner like Nessus, Nexpose, or OpenVas

Ports, Protocols & Services

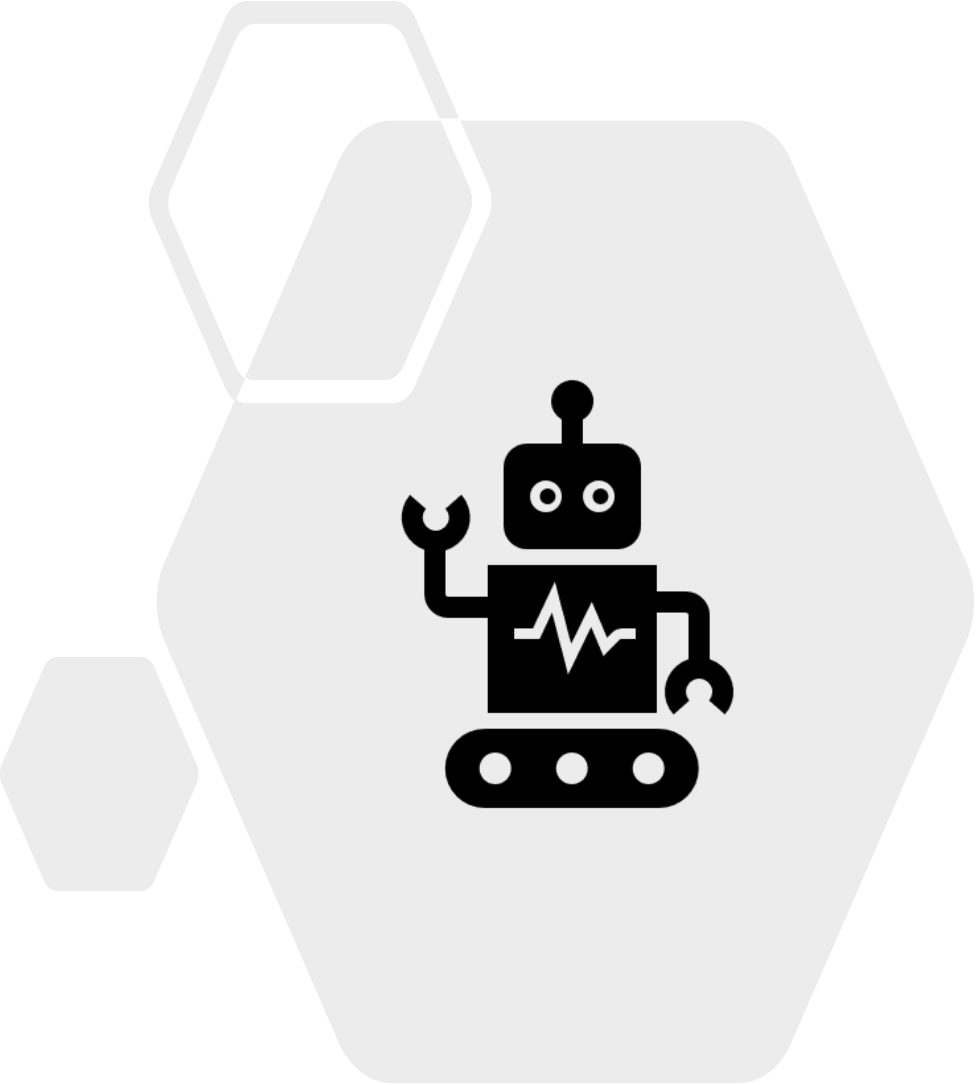
It’s like “Google” but for things…

Ports, Protocols & Services

- Shodan indexes every port on every device it can find
- It catalogues information like software services, versions
- Even indexes screen shots for services like RDP, VNC, and from IP Cameras
- Shodan also uses operators like Google: “hostname:, port:, country:, has_screenshot:”

Robots.txt

- Easy, unlikely to be noticed, also unlikely to knock anything over
- Might reveal “interesting” folders
- Intended to control crawlers & bots indexing



Port Scanning via NMAP

- Port scanner that identifies open ports and software running on them
- Lots of included scripts and features
- **Do not do this without coordination!**

Hopefully, My Sacrifice is Accepted

Time to Put on the Black Hat!

Let’s Hack a School District!

Virtual Lab

We have prepared a virtual “School District”, complete with several servers and workstations.

Your goal is to apply what we have learned today to gain access to these systems and retrieve any sensitive information you can.

This is a simulation and only a simulation. All the data present is created randomly and programmatically, including the pictures. No actual PII exists here and any resemblance to any persons is purely coincidental.

Background

Nowheresville is a sleepy community in a western state. Their school district has a nice web page with a parent portal, and they use their information systems to process lots of student data and keep the community informed on what is happening in the district.

We are going to take on the role of hackers looking to victimize the School and make off with student information and launch a ransomware attack.

Rules of the Road

- Be Kind! We are all here to learn
- Attack ONLY the devices and IP space specified as “in scope”
- Do not intentionally degrade the performance of the lab environment
- Do not attack or otherwise interfere with other attendees using the lab (*no king of the hill*)
- If you intentionally break these rules, you will be removed from the lab!

Lab Information

- **Lab WiFi**
  - SSID: PTAC_lab (PTAC_lab5g)
  - PW: PTAC2024!

- **Lab IP Space** ***(only these IPs are in scope)***
  - *10.0.0.50 – 10.0.0.60*

Be Good! I'll be watching…

CONTACT INFORMATION

United States Department of Education,
Student Privacy Policy Office (SPPO)

☎ (855) 249-3072
(202) 260-3887

✉ privacyTA@ed.gov

🖥 https://studentprivacy.ed.gov

📠 (855) 249-3073