

---

# **Lesson 5: Threat Modeling and OSINT**

---

---

# Attack surface



Evaluation



Measurement

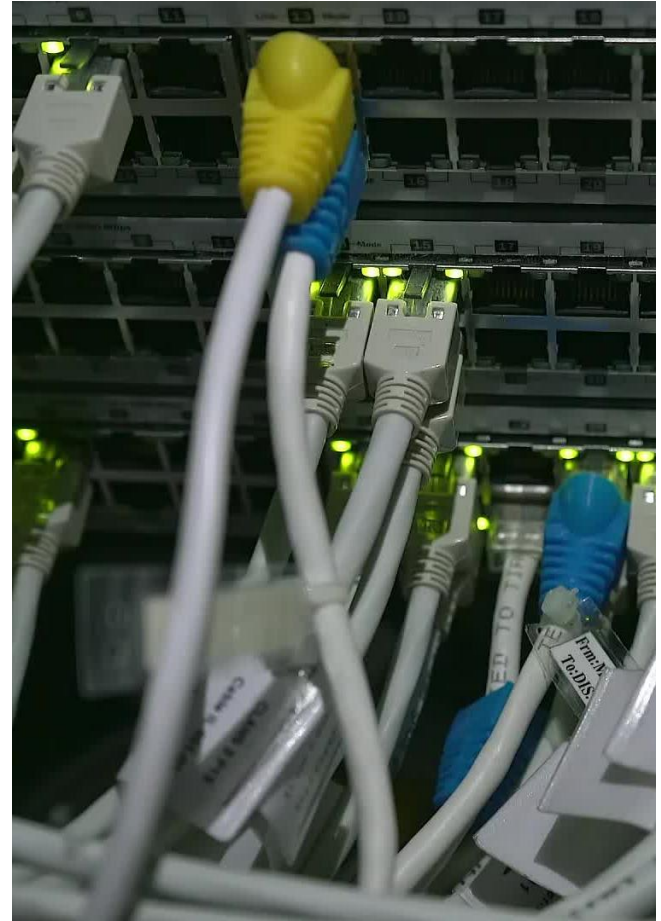


Minimization

---

# Attack surface

- Open Sockets
- Services
- Services running as SYSTEM
- Accounts
- Null sessions
- Guest account
- Weak access controls



---

# Threat modeling

---

## External Threats

---

## Internal Threats

---

# What is a Threat Model

- An overview of threat components
  - The system's attack surface
  - Threats who can attack the system
  - Assets threats may compromise
  - Estimate probability of attack
  - Impact of successful attack

# How to Threat Model

---

Identify

Assets

Threats

Vulnerabilities

---

Enumerate

Attack vectors

Actors

Risks

---

Evaluate

Probability

Impact

---

---

# Asset identification

CRITICAL DATA

INTERFACES

DATA FLOW

---

---

# Identifying Assets



## What is it that you want to protect?

Private data (e.g., customer list)

Proprietary data (e.g., intellectual property)

Potentially injurious data (e.g., credit card numbers, decryption keys)



## These also count as "assets"

Integrity of back-end databases

Integrity of the Web pages (no defacement)

Integrity of other machines on the network

Availability of the application

---

# Documenting Architecture

---

Define what the app does and how it's used

Users view pages with catalog items

Users perform searches for catalog items

Users add items to shopping carts

Users check out

---

Diagram the application

Show subsystems

Show data flow

List assets

---

---

# Decomposing the Application



## Refine the architecture diagram

Show authentication mechanisms

Show authorization mechanisms

Show technologies

Diagram trust boundaries

Identify entry points



## Begin to think like an attacker

Where are my vulnerabilities?

What am I going to do about them?

---

# STRIDE

## STRIDE

The acronym STRIDE is used to denote the following types of threats:

### **Threat**

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privilege

### **Security Property**

Authentication

Integrity

Nonrepudiation

Confidentiality

Availability

Authorization

---

# STRIDE-per-Element

Element	S	T	R	I	D	E
External Entity	√		√			
Process	√	√	√	√	√	√
Data Store		√	√*	√	√	
Data Flow		√		√	√	

---

# Dread

Damage Potential

Reproducibility

Exploitability

Affected Users

Discoverability

---

---

# VAST

**Vast**

**Visual**

**Agile**

**Simple**

**Threat Modeling**

- 
- VAST is about threat modeling through the software development lifecycle, particularly in Agile programming. VAST works with two concurrent types of models. The application threat model and the operational threat model. Threats are reviewed from both perspectives. Process flow diagrams are used to examine application threats. Data flow diagrams are used to examine operational threats. VAST integrates well with DevOps lifecycles.

# PASTA

Define Objectives	Identify Business Objectives Identify Security & Compliance Requirements Perform Business Impact Analysis
Define Technical Scope	Determine the boundaries of the technical environment Capture infrastructure dependencies
Application Decomposition	Identify Use Cases Define entry points and trust levels Identify Threat Actors Perform Data Flow Diagramming Determine Trust Boundaries
Threat Analysis	Examine Probabilistic attack scenarios Perform Regression analysis on security events Perform threat intelligence correlation
Vulnerability & Weakness Analysis	Review existing vulnerability reports Analyze design flaws and abuse cases Review scorings such as CVSS and CVE
Attack Modeling	Perform attack surface analysis Perform attack tree development Match vulnerabilities and exploits to attack trees
Risk & Impact Analysis	Qualify and Quantify Business Impact Analysis Identify countermeasures Perform residual risk analysis Identify risk mitigation strategies

- Process for Attack Simulation and Threat Analysis. This is a seven-step methodology for evaluating risk. As the name suggests, it is about simulating attacks in order to analyze the threats. PASTA is risk-centric and it was developed in 2012. The seven stages of PASTA are shown in the following table.

---

# Trike

- Trike was created as a security audit framework that uses threat modeling as a technique. It looks at threat modeling from a risk-management and defensive perspective.
- Key Concepts of Trike:
  - Requirements Model: This model defines the security characteristics of an IT system and determines acceptable risk levels for each asset. It's like a high-level blueprint of the system's security posture.
  - Implementation Model: This model uses Data Flow Diagrams (DFDs) to illustrate how data flows within the system and the actions users can perform. DFDs help visualize the system's structure and identify potential vulnerabilities.
  - Risk-Based: Trike prioritizes threats and security controls based on the risk they pose to the system. This allows for a more efficient allocation of security resources.
  - Communication and Coordination: The Trike framework facilitates communication and coordination between different security teams and stakeholders by providing a conceptual framework for understanding the system's security



---

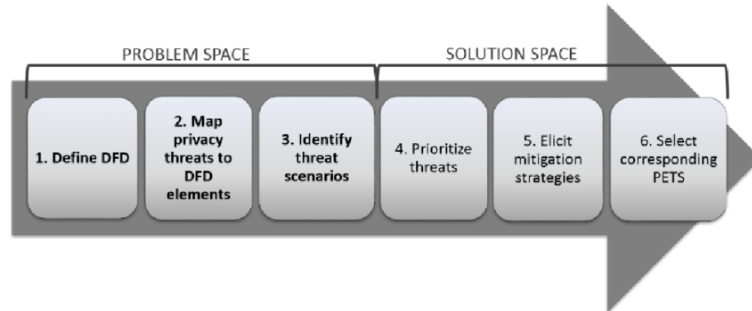
# Trike



- 
- **Trike Process:**
  - **Establish the System:** Define the scope of the system being modeled.
  - **Create a Requirements Model:** Identify actors, assets, expected actions, and rules within the system.
  - **Create a Data Flow Diagram (DFD):** Depict how data flows through the system, including trust boundaries.
  - **Analyze the Implementation Model:** Identify potential threats, assign risk values, and define security controls.
  - **Develop a Risk Model:** Based on the threat model, develop a risk model that outlines acceptable levels of risk for each asset.
  - **Implement Safeguards:** Put in place measures to mitigate identified threats.

# LINDDUN

- LINDDUN (linkability, identifiability, nonrepudiation, detectability, disclosure of information, unawareness, noncompliance)
- Focuses on privacy concerns and can be used for data security. Consisting of six steps, LINDDUN provides a systematic approach to privacy assessment.
- LINDDUN starts with a DFD of the system that defines the system's data flows, data stores, processes, and external entities. By systematically iterating over all model elements and analyzing them from the point of view of threat categories, LINDDUN users identify a threat's applicability to the system and build threat trees.
- <https://linddun.org/>



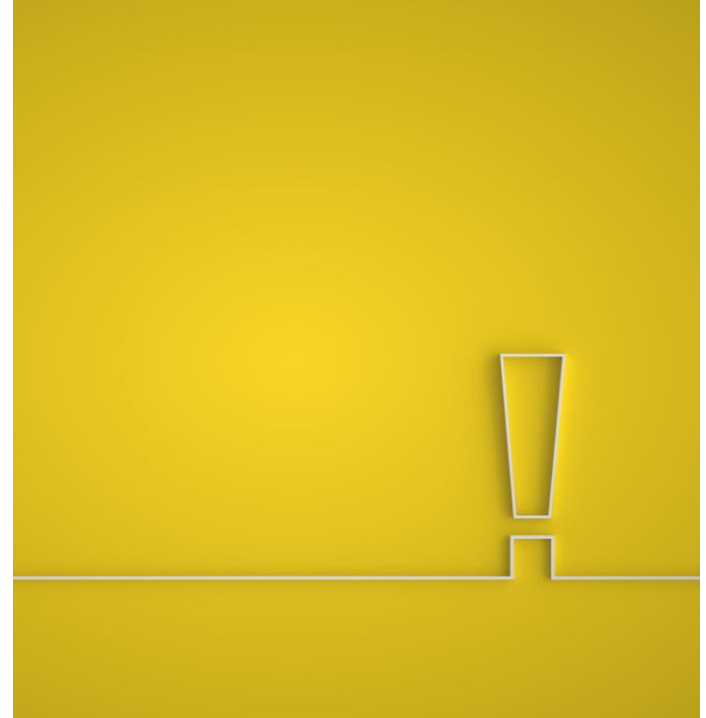
# The Threat Modeling Process



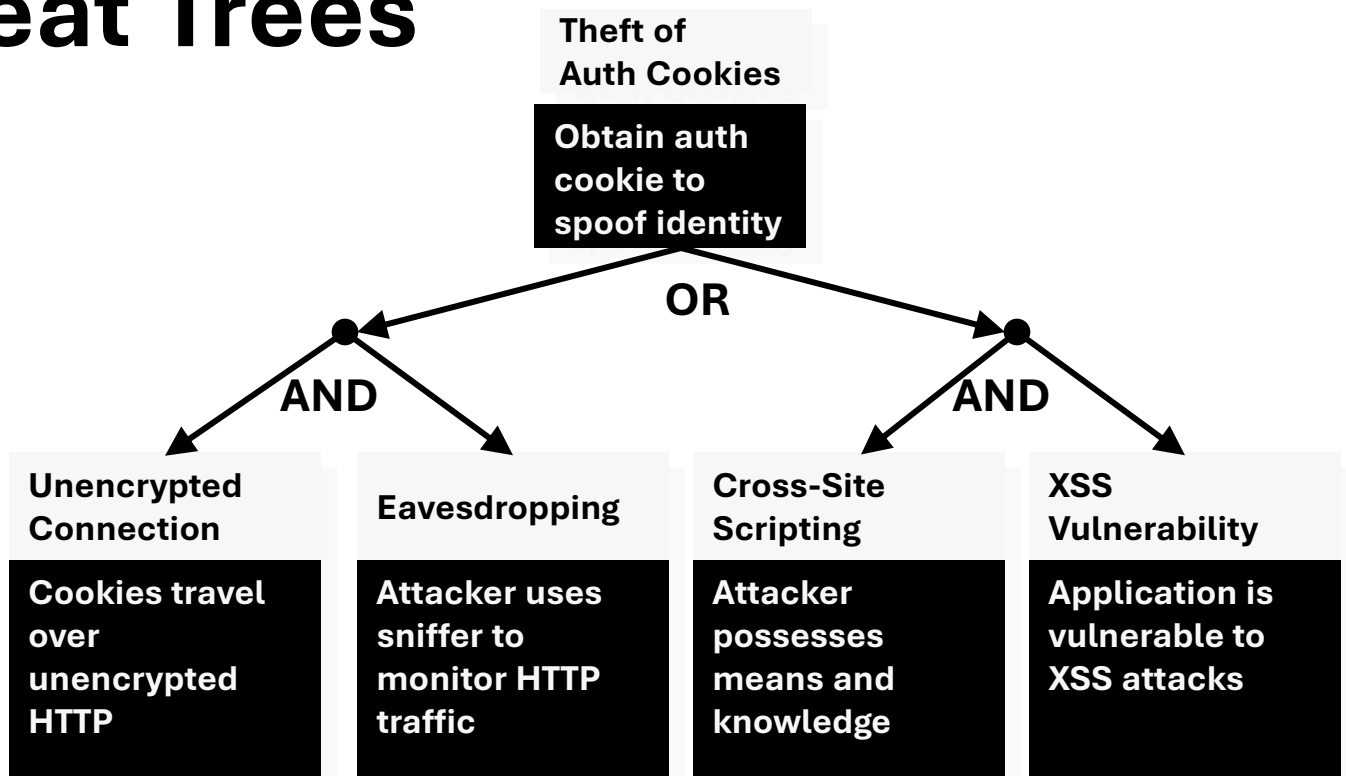
---

# Identifying Threats

- Method #1: Threat lists
  - Start with laundry list of possible threats
  - Identify the threats that apply to your app
- Method #2: STRIDE
  - Categorized list of threat types
  - Identify threats by type/category
- Optionally draw threat trees
  - Root nodes represent attacker's goals
  - Trees help identify threat conditions



# Threat Trees



---

# Sources for Data



- 
- <https://nvd.nist.gov>
  - <https://www.us-cert.gov/ncas/alerts>
  - <https://www.threatcrowd.org>
  - <https://isc.sans.edu>

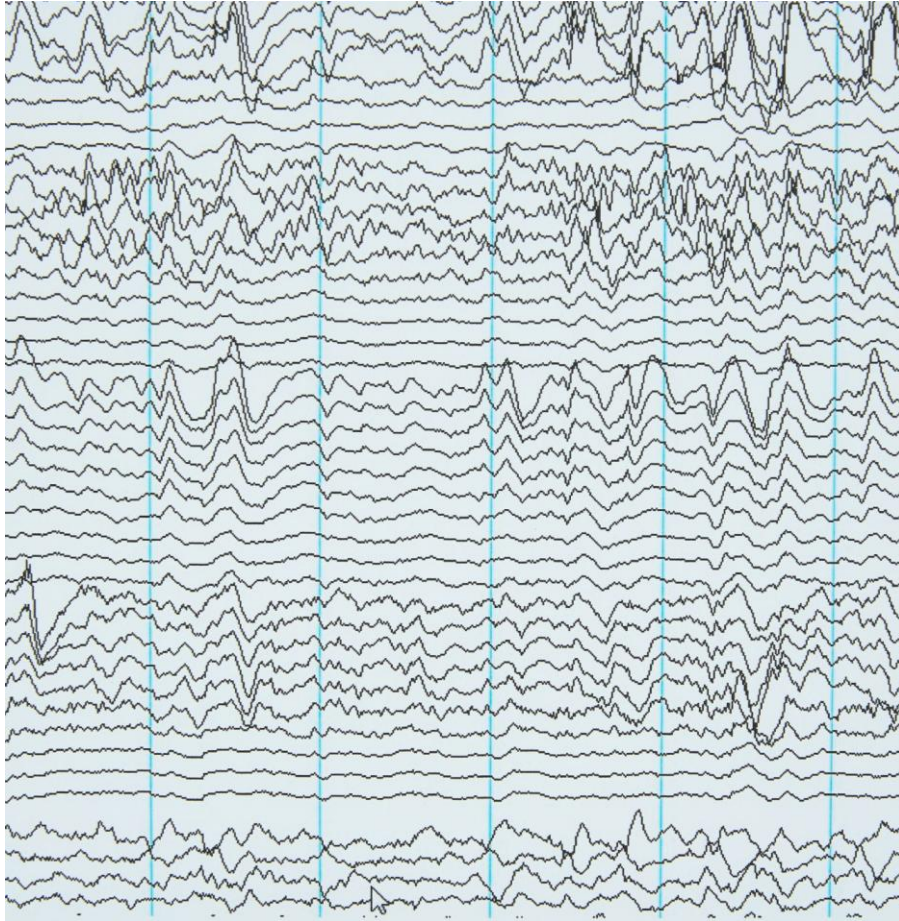


---

# CVE

“MITRE considers CVE as the industry standard to systematically register all discovered software vulnerabilities”

- Cyber Threat Intelligence (Advances in Information Security) . Springer International Publishing.



## Common Vulnerabilities and Exposures (CVE)

- Repositories of this type of data, such as CVE Details and the National Vulnerability Database (NVD), are used to help consumers find this data in order to help them weigh their options. The numbers and types of these vulnerabilities represent a fair indication of the level of vulnerability exhibited by a given product. It's important to consider that these types of repositories are not definitive. They could not possibly contain a listing for every vulnerability, but rather only known and fully documented vulnerabilities. Because of this, a high number of vulnerabilities could also be an indication, or a by-product, of the popularity of a given product.
- Several open-source tools exist that can be used for vulnerability analysis of the different systems and applications. Following are examples of links that list examples of such vulnerability analysis tools:

---

# CVSS

“A well-known standard for quantifying severity is the Common Vulnerability Scoring System (CVSS). As a framework designed to standardize the severity ratings for vulnerabilities, its model ensures accurate quantitative measurement so that users can better understand the impact of these weaknesses. With the CVSS scoring standard, members of industries, academia, and governments can communicate clearly across their communities.”

-Maymi, Fernando; Chapman, Brent; Parker, Jeff T.. CompTIA CySA+ Cybersecurity Analyst Certification Bundle (Exam CS0-001) . McGraw-Hill Education.

---

# CVS

- The common vulnerability scoring system (CVSS) is widely used to classify vulnerabilities. This is an open industry standard that allows for the scoring of vulnerabilities based on severity. The full specification can be found here <https://www.first.org/cvss/specification-document>.
- There are three groups of metrics: base, temporal, and environmental. The base group describes the basic characteristics of the vulnerability that are not determined by time (temporal) or environment. The metrics in this group are Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality Impact, Integrity Impact, and Availability Impact.
- The Attack Vector Metric can be: Network (N), Adjacent (A), Local (L), Physical (P). Attack Complexity can be: None (N), Low (L), and High (H). User Interaction can be: None (N) or Required (R). The Scope metric captures whether a vulnerability in one vulnerable component impacts resources in components beyond its security scope. Its values can be: Unchanged (U) or Changed (C). The Impact Metrics (Confidentiality, Availability, or Integrity) are all rated: High (H), Low (L), or None (N).

---

# CVS

- The Temporal Metric Group has three metrics: Exploit Code Maturity, Remediation Level, and Report Confidence. The Environmental Metric Group has four metrics: Modified Base Metrics, Confidentiality Requirement, Integrity Requirement, and Availability Requirement.
- Exploit Code Maturity measures the likelihood of the vulnerability being attacked and is typically based on the current state of exploit techniques, exploit code availability, or active, “in-the-wild” exploitation. The possible ratings are: Not Defined (X), High (H), Functional (F), Proof of Concept (P), and Unproven (U). The Remediation Level Metric can be: Not Defined (X), Unavailable (U), Workaround (W), Temporary Fix (T) or Official Fix (O). The Report Confidence metric indicates how confident we are in the details of the vulnerability. Its values can be: Not Defined (X), Confirmed (C), Reasonable (R), and Unknown (U).
- The values for the various metrics are summarized in the following table:

# CVS Table

Metric Group	Metric Name (and Abbreviated Form)	Possible Values	Mandatory?
	Attack Vector (AV)	[N,A,L,P]	Yes
	Attack Complexity (AC)	[L,H]	Yes
	Privileges Required (PR)	[N,L,H]	Yes
	User Interaction (UI)	[N,R]	Yes
	Scope (S)	[U,C]	Yes
	Confidentiality (C)	[H,L,N]	Yes
	Integrity (I)	[H,L,N]	Yes
	Availability (A)	[H,L,N]	Yes
	Exploit Code Maturity (E)	[X,H,F,P,U]	No
	Remediation Level (RL)	[X,U,W,T,O]	No
	Report Confidence (RC)	[X,C,R,U]	No
Environmental	Confidentiality Requirement (CR)	[X,H,M,L]	No
	Integrity Requirement (IR)	[X,H,M,L]	No
	Availability Requirement (AR)	[X,H,M,L]	No
	Modified Attack Vector (MAV)	[X,N,A,L,P]	No
	Modified Attack Complexity (MAC)	[X,L,H]	No
	Modified Privileges Required (MPR)	[X,N,L,H]	No
	Modified User Interaction (MUI)	[X,N,R]	No
	Modified Scope (MS)	[X,U,C]	No
	Modified Confidentiality (MC)	[X,N,L,H]	No
	Modified Integrity (MI)	[X,N,L,H]	No
	Modified Availability (MA)	[X,N,L,H]	No

---

# CVS

- CVSS scoring is often represented as a string such as CVSS:3.1/S:U/AV:N/AC:L/PR:H/UI:N/C:L/I:L/A:N/E:F/RL:X
- As can be seen CVSS scoring is a bit more involved than some of the other methods, such as CVE. However, it is also more informative. This method provides a quantifiable approach to categorizing vulnerabilities so they can be appropriately addressed. It is strongly recommended that you become well acquainted with CVSS.

---

# Cyber Kill Chain

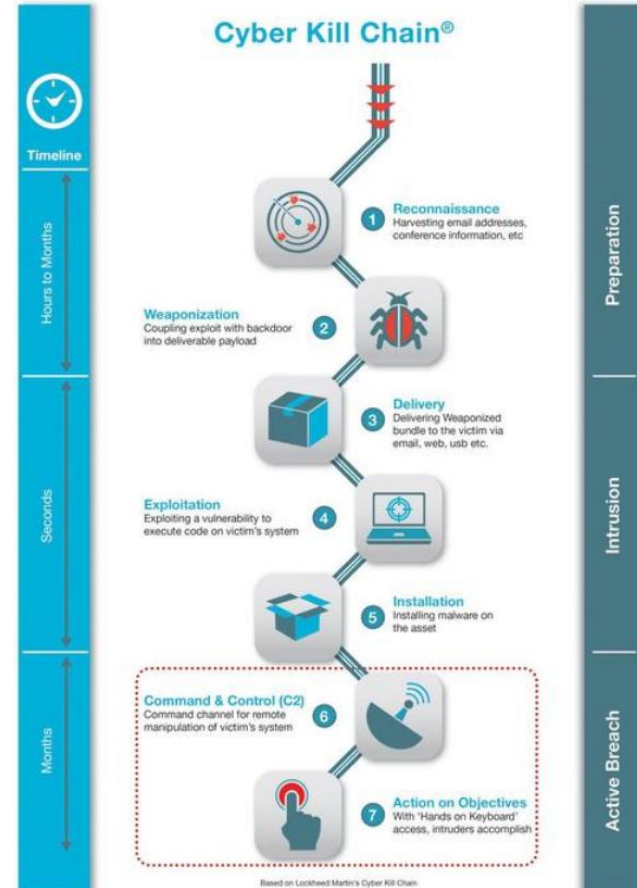
- The term was created by Lockheed Martin
- **Step 1: Reconnaissance.** The attacker gathers information on the target before the actual attack starts. He can do it by looking for publicly available information on the Internet.
- **Step 2: Weaponization.** The attacker uses an exploit and creates a malicious payload to send to the victim. This step happens at the attacker side, without contact with the victim.
- **Step 3: Delivery.** The attacker sends the malicious payload to the victim by email or other means, which represents one of many intrusion methods the attacker can use.
- **Step 4: Exploitation.** The actual execution of the exploit, which is, again, relevant only when the attacker uses an exploit.

---

# Cyber Kill Chain

- **Step 5: Installation.** Installing malware on the infected computer is relevant only if the attacker used malware as part of the attack, and even when there is malware involved, the installation is a point in time within a much more elaborate attack process that takes months to operate.
- **Step 6: Command and control.** The attacker creates a command and control channel in order to continue to operate his internal assets remotely. This step is relatively generic and relevant throughout the attack, not only when malware is installed.
- **Step 7: Action on objectives.** The attacker performs the steps to achieve his actual goals inside the victim's network. This is the elaborate active attack process that takes months, and thousands of small steps, in order to achieve.

# Cyber Kill Chain



---

# 15 top IoC

- 
- Unusual outbound network traffic
  - Anomalies in Privileged User Account Activity
  - Geographical Irregularities
  - Other Log-in Red Flags
  - Swells in Database Read Volume
  - HTML Response Sizes
  - Large Numbers of Requests for the Same File
  - Mismatched Port-Application Traffic
  - Suspicious Registry or System File Changes
  - DNS Request Anomalies
  - Unexpected Patching
  - Mobile Device Profile Changes
  - Data in the Wrong Places
  - Web traffic with non -human behavior
  - Signs of DDoS.
- 
- -<http://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647?>

---

# DoD OSINT

Derived exclusively from publicly or commercially available information to address specific intelligence priorities, requirements or gaps, OSINT is vital to the agency's mission – providing unique value and enabling all other intelligence collection disciplines. In today's world, information is everywhere, all the time. By focusing our efforts on open source information of intelligence value, DIA is able to maintain global awareness of breaking events that affect US interests at home and abroad. And, we have the right safeguards in place to protect the privacy and civil liberties of all persons while adhering to all relevant laws and implementing guidelines.

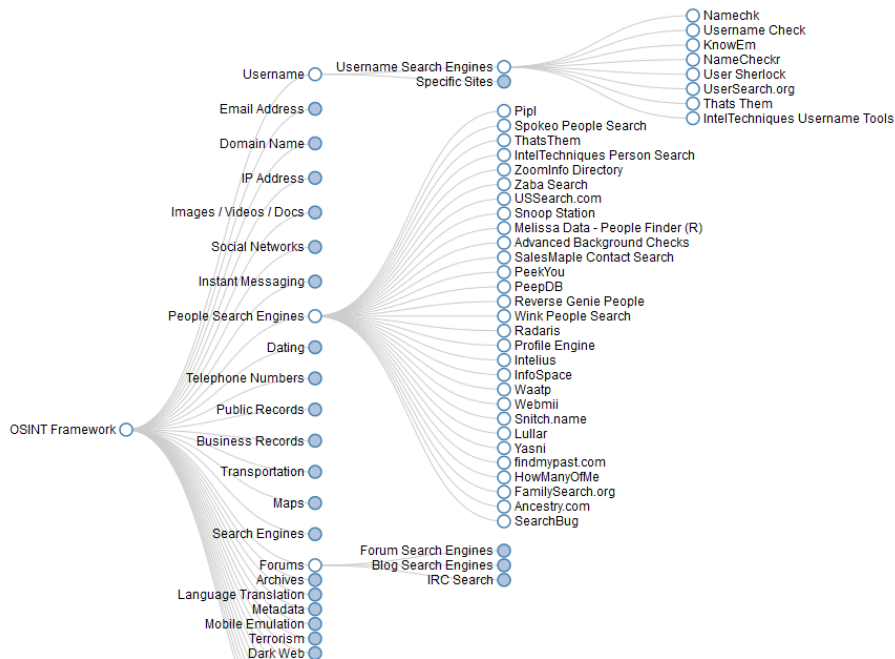
- <https://www.dia.mil/About/Open-Source-Intelligence/>

# Search Tools

<http://osintframework.com/>

## OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally  
(G) - Google Dork, for more information: [Google Hacking](#)  
(R) - Requires registration  
(U) - Indicates a URL that contains the search term and the URL itself must be edited manually







# Google Dorks

<https://www.exploit-db.com/google-hacking-database>

easttom site:facebook.com

Images Shopping News Videos Maps Books Flights Finance




About 3,600 results (0.32 seconds)

-  [facebook.com](https://www.facebook.com/sunsetchurchofchrist)  
https://m.facebook.com/sunsetchurchofchrist/posts
- John Easttom was baptized into... - Sunset Church of Christ**  
John **Easttom** was baptized into Christ tonight. A wonderful example of God's providence and the power of the gospel of Jesus Christ.
-  [facebook.com](https://www.facebook.com/joseph.easttom)  
https://www.facebook.com/joseph.easttom
- Joseph Easttom**  
Joseph **Easttom** is on Facebook. Join Facebook to connect with Joseph **Easttom** and others you may know. Facebook gives people the power to share and makes...
-  [facebook.com](https://www.facebook.com/.../Videos)  
https://www.facebook.com/.../Videos
- Thanks to Easttom family and their three Harmony students for ...**  
More from Harmony Science Academy Lubbock - 2023 8th Grade Graduation Ceremony - 2023 STAAR PEP RALLY.
-  [facebook.com](https://m.facebook.com/people/Derik-Easttom)  
https://m.facebook.com/people/Derik-Easttom
- Derik Easttom**  
Hometown. About Derik. I never in a million years, would have thought I'd be taking anti-depressants and different Psych meds to try to feel somewhat normal or ...

easttom site:linkedin.com

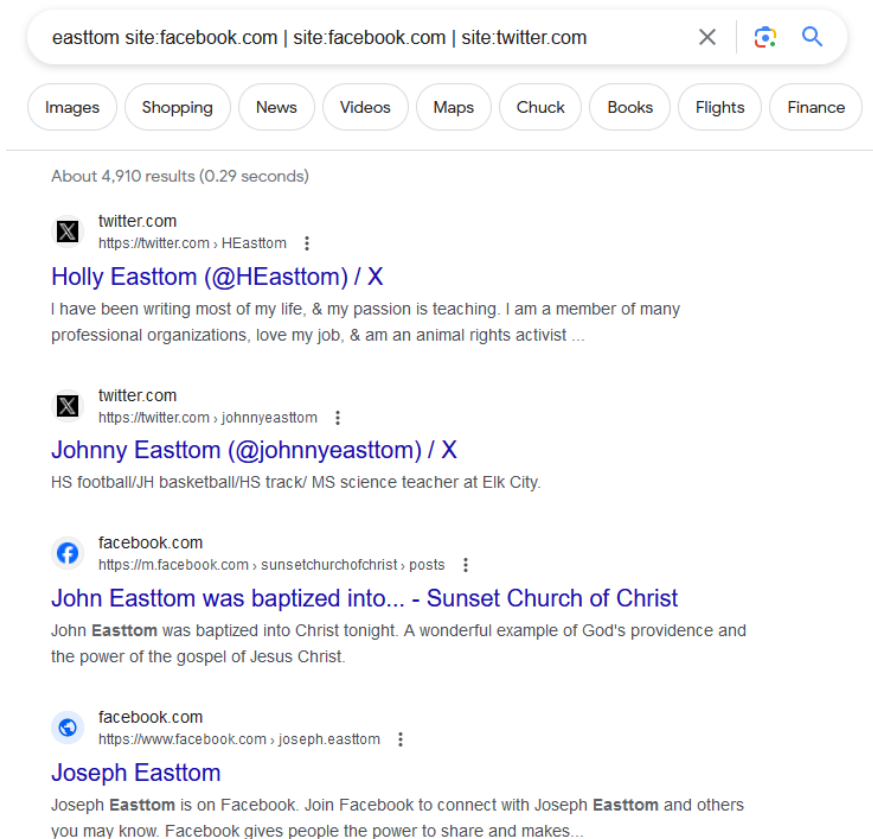
Images Shopping News Videos Maps Chuck Books Flights Finance

About 3,980 results (0.31 seconds)

-  [linkedin.com](https://www.linkedin.com/charlieeasttom)  
https://www.linkedin.com/charlieeasttom
- Charlie Easttom - Owner/Operator**  
Santa Monica, California, United States · Owner/Operator · Easttom's Enterprises  
I have deep industry knowledge, expertise in solid, liquid, and hazardous waste removal, treatment, and recycling. Additionally, I started my own business in ...
-  [linkedin.com](https://www.linkedin.com/pub/dir/Easttom)  
https://www.linkedin.com/pub/dir/Easttom
- 10+ "Easttom" profiles**  
View the profiles of professionals named "**Easttom**" on LinkedIn. There are 10+ professionals named "**Easttom**", who use LinkedIn to exchange information, ...
-  [linkedin.com](https://www.linkedin.com/holly-easttom-45752b83)  
https://www.linkedin.com/holly-easttom-45752b83
- Holly Easttom - Student publications advisor, assistant ...**  
I've taught many multi-faceted classes (anywhere from life guarding to English, advanced composition and news, to media culture and film criticism). My first ...

# Google Dorks


<https://www.exploit-db.com/google-hacking-database>



easttom site:facebook.com | site:facebook.com | site:twitter.com


Images Shopping News Videos Maps Chuck Books Flights Finance

About 4,910 results (0.29 seconds)

 **twitter.com**  
https://twitter.com › HEasttom


[Holly Easttom \(@HEasttom\) / X](#)

I have been writing most of my life, & my passion is teaching. I am a member of many professional organizations, love my job, & am an animal rights activist ...

 **twitter.com**  
https://twitter.com › johnnyeasttom


[Johnny Easttom \(@johnnyeasttom\) / X](#)

HS football/JH basketball/HS track/ MS science teacher at Elk City.

 **facebook.com**  
https://m.facebook.com › sunsetchurchofchrist › posts

[John Easttom was baptized into... - Sunset Church of Christ](#)

John **Easttom** was baptized into Christ tonight. A wonderful example of God's providence and the power of the gospel of Jesus Christ.

 **facebook.com**  
https://www.facebook.com › joseph.easttom

[Joseph Easttom](#)

Joseph **Easttom** is on Facebook. Join Facebook to connect with Joseph **Easttom** and others you may know. Facebook gives people the power to share and makes...

# Google Dorks

[https://www.exploit-  
db.com/google-  
hacking-database](https://www.exploit-db.com/google-hacking-database)

"vanderbilt is awesome" site:facebook.com | site:facebook.com | site:twitter X  

Images

Videos

Shopping

News

Maps

Books

Flights

Finance

About 268 results (0.28 seconds)



facebook.com

<https://www.facebook.com/VanderbiltHealth>, posts

## A sweet story about the bonds we make... - Vanderbilt Health

**Vanderbilt is awesome!!** Full of caring people.❤️. 3 yrs. 1. Susie Leming-Lee. Way to share the love Dermatology and make a positive difference in Mr. Hamm's



facebook.com

<https://m.facebook.com>, posts

## Hi! I'm Kelly Hewitt, and I am a... - Vanderbilt Health

Welcome!! 2 yrs. 1. Nella Nash. Welcome to TENNESSEE. 2 yrs. 1. Melissa Thiele. **Vanderbilt is awesome.** 2 yrs. 1. Connie Martin. Congratulations ...



facebook.com



<https://www.facebook.com/childrenshospital>, posts

## It's... - Monroe Carell Jr. Children's Hospital at Vanderbilt

**Vanderbilt is awesome!** Addison liked all the nurses, but she loved Ms Kelley! They are just wonderful with the kids. We will see y'all on ...

# Google Dorks

[https://www.exploit-  
db.com/google-  
hacking-database](https://www.exploit-db.com/google-hacking-database)


related:chuckeasttom.com ×  

Images Videos News Shopping Maps Books Flights Finance

About 610,000 results (0.44 seconds)



Chuck Easttom

<https://www.chuckeasttom.com> 

## Dr. Chuck Easttom's Website

Website of **Chuck Easttom**, Ph.D., D.Sc. This website provides information about Dr. **Chuck Easttom**. You can find his books , work in litigation support, and a ...

Missing: related-

You've visited this page 3 times. Last visit: 11/7/2023



Chuck Easttom


<https://www.chuckeasttom.com> > easttomcv 

## CV

Website of **Chuck Easttom**, Ph.D ... Coursework included technology **related** courses such as digital video editing, multimedia presentations, and computer graphics.



University of Dallas

<https://udallas.edu> > cob > about > faculty > easttom\_c... 

Google Dorks

## Chuck Easttom, Ph.D., CISSP






Dr. **Chuck Easttom** is the author of 28 books, including several on computer security, forensics, and cryptography. His books are used at over 60 universities. He ...

# Specialty Search Engines

*<https://buckets.grayhatwarfare.com>*

Showing 1 - 20 out of 97 results

Premium users using this query see 6 more results. [More info here.](#)

#	Bucket	Filename
1	 <a href="#">writersadminfiles.fra1.digitaloceanspaces.com</a> ✖	employer/uploads/Chuck Easttom - Digit...sponse (2022).pdf64ed5235cf2f227238.pdf
2	 <a href="#">ptabdata.blob.core.windows.net</a> ✖	files/2017/IPR2017-00221/v32_EX2001 (221) Easttom Declaration.pdf
3	 <a href="#">ptabdata.blob.core.windows.net</a> ✖	files/2017/IPR2017-00221/v35_EX2001 (221) Easttom Declaration.pdf
4	 <a href="#">ptabdata.blob.core.windows.net</a> ✖	files/2017/IPR2017-00221/v37_Ex. 1030 - Easttom Deposition Transcript.pdf
5	 <a href="#">ptabdata.blob.core.windows.net</a> ✖	files/2017/IPR2017-00222/v29_EX2001 (222) Easttom Declaration.pdf

---

# Specialty Search Engines

<https://intelx.io/>

## Person Lookup by Full Name

Chuck	Easttom	Search
-------	---------	--------

Spokeo     ThatsThem     FamilyTreeNow     ZabaSearch     radaris     melissa     FastPeopleSearch     TruePeopleSearch  
 truthfinder     spytox     PeopleLooker     Dehashed     CheckPeople     Whitepages     Grayhat     peekyou  
 YellowPages

[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.

---



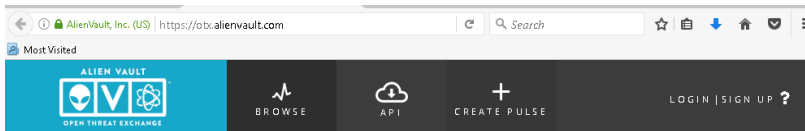
---

# Threat Intelligence

---

OTX – Open Threat Exchange: AlienVault  
Open Threat Exchange (OTX) provides open access to a global community of threat researchers and security professionals

<https://otx.alienvault.com/>



---

# Threat Intelligence

We've found 18M + results

Pulses ( 282K )

Users ( 260K )

Groups ( 769 )

Indicators ( 18M )

Malware Families ( 27K )

Industries ( 1K )

Show: All ▾ Sort: Recently Modified ▾



## SSH Brute-Force Honeypot Live

CREATED 2 YEARS AGO | MODIFIED 23 SECONDS AGO by [pr0v1eh](#) | Public | TLP: White

IPv4: 164326

every host is banned for 3 hours and receives an abuse report from me every 96 hours if it continues

[Bruteforce](#), [Brute-Force](#), [SSH](#), [Honeypot](#)



## ETIC Cybersecurity 2023-11-23 Port Scan

CREATED 23 HOURS AGO | MODIFIED 31 SECONDS AGO by [EticCybersecurity](#) | Public | TLP: White

IPv4: 41554

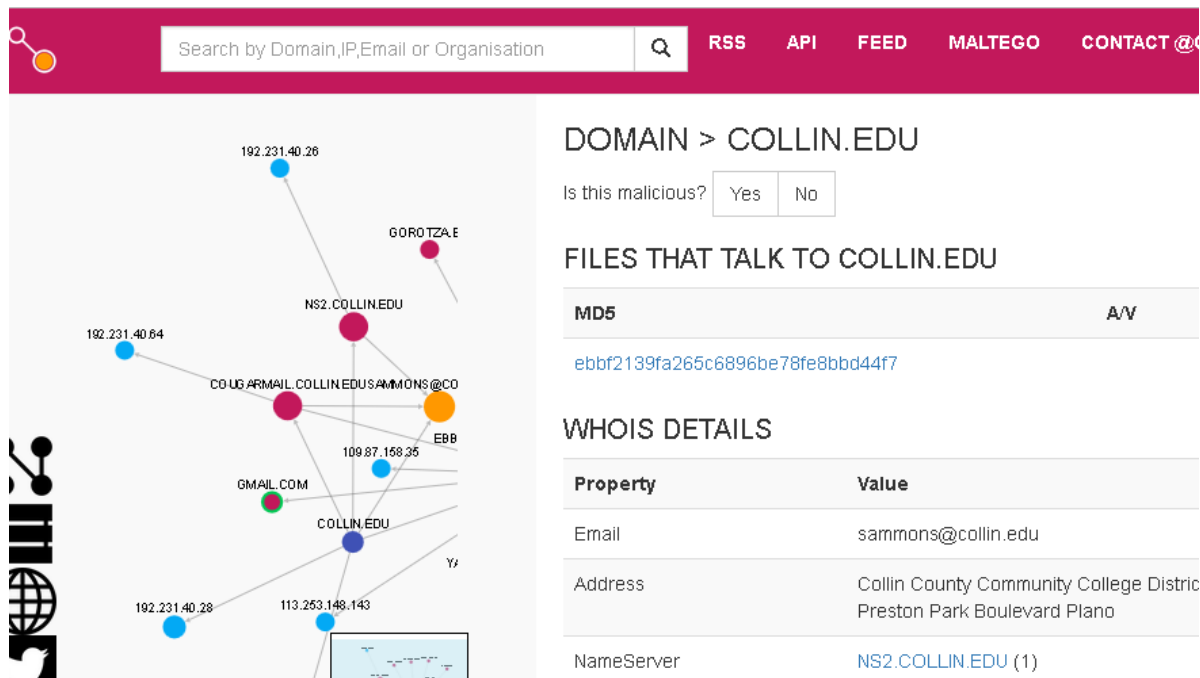
Threat Intelligence

---

OTX – Open Threat Exchange: AlienVault  
Open Threat Exchange (OTX)

<https://otx.alienvault.com/browse/global>

# Threatcrowd -continued



The screenshot displays the Threatcrowd interface for the domain COLLIN.EDU. On the left, a network diagram shows connections between various IP addresses and domain-related entities. On the right, the domain's WHOIS details are listed.

**Search by Domain,IP,Email or Organisation** [Search Icon] **RSS** **API** **FEED** **MALTEGO** **CONTACT @**

**DOMAIN > COLLIN.EDU**

Is this malicious?

**FILES THAT TALK TO COLLIN.EDU**

MD5	A/V
<a href="#">ebbf2139fa265c6896be78fe8bbd44f7</a>	

**WHOIS DETAILS**

Property	Value
Email	sammons@collin.edu
Address	Collin County Community College District Preston Park Boulevard Plano
NameServer	<a href="#">NS2.COLLIN.EDU</a> (1)

**Network Diagram Labels:** 192.231.40.26, GOROTZAE, NS2.COLLIN.EDU, 192.231.40.64, COUGARMAIL.COLLIN.EDUSAMMONS@CO, 109.87.168.35, EBB, GMAIL.COM, COLLIN.EDU, 192.231.40.28, 113.253.148.143, Yz

---

# Threat Intelligence

---

<https://isc.sans.edu/>



Last Daily Podcast (Fri, Nov 17th): [Faster tcpdump](#); [Zimbra Exploit Details](#); [FortiSIEM Vuln: AI-Exploits](#); [CrushFTP and FortiSIEM Patches](#); [@sans\\_edu](#) Research; [Scott Poley](#); [Storing Less](#)

## Diaries

[View All](#)

Published: 2023-11-22 by Guy Bruneau

### **[CVE-2023-1389: A New Means to Expand Botnets](#)**

[This is a Guest Diary by Jonah Latimer, an ISC intern as part of the SANS.edu [BACS](#) program]

#### **Introduction**

I am currently pursuing a Bachelor degree from SANS Technology Institute, and part of the requirements for graduation is to complete a 20 week internship with the SANS Internet Storm Center. During this internship I created a honeypot using an Amazon EC2 instance, and overserved and reported on seven different attacks that were leveraged against it. The following blog post is going to dive into one of the vulnerabilities that I came across.

#### **Summary**

---

# Threat Intelligence

---

<https://openphish.com/>

Timely. Accurate. Relevant Phishing Intelligence.

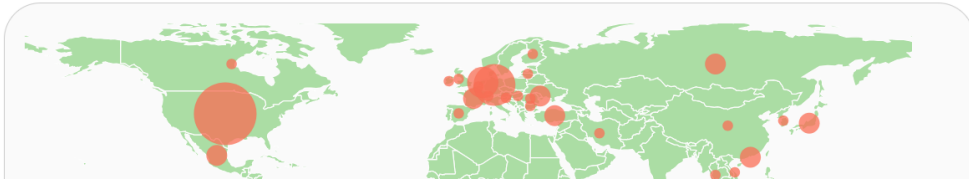
**8,645,670**  
URLs Processed

7-Day Phishing Trends

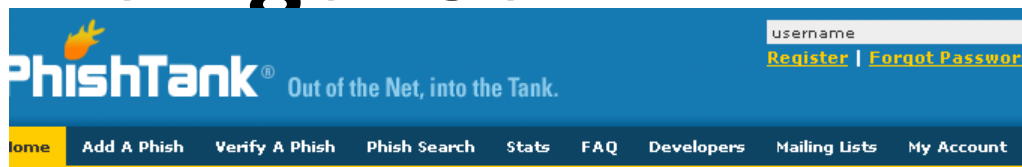
**10,585**  
New Phishing URLs

**226**  
Brands Targeted

24-Hour Phishing Activity



# Threat Intelligence



## Join the fight against phishing

[Submit](#) suspected phishes. [Track](#) the status of your submissions.  
[Verify](#) other users' submissions. [Develop](#) software with our free API.

Found a phishing site? Get started now – see if it's in the Tank:

## Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

D	URL	Submitted by
<a href="#">.652099</a>	<a href="http://webservice-verification-csrh.com/webapps/d3...">http://webservice-verification-csrh.com/webapps/d3...</a>	<a href="#">PhishReporter</a>
<a href="#">.652098</a>	<a href="http://webservice-verification-csrh.com/">http://webservice-verification-csrh.com/</a>	<a href="#">PhishReporter</a>
<a href="#">.652097</a>	<a href="http://www.raceandrally.com/library/contas/acessib...">http://www.raceandrally.com/library/contas/acessib...</a>	<a href="#">irual</a>
<a href="#">.652096</a>	<a href="http://www.barjercito.online/">http://www.barjercito.online/</a>	<a href="#">GlobalCybersec</a>

<https://phishtank.org/>

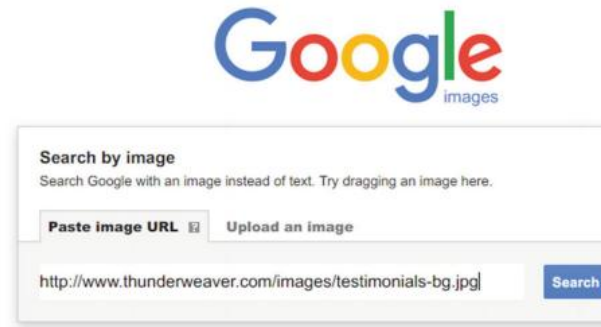
# Image Search

- Google Image Search  
<https://images.google.com>
- Picsearch [www.picsearch.com](http://www.picsearch.com)
- SmugMug <https://www.smugmug.com>
- Imgur <https://imgur.com>
- Lakako ( <https://www.lakako.com> ): This searches Instagram, Twitter, and Google + for photos and people.
- Flickr map ( <https://www.flickr.com/map> ): View uploaded images on a map according to the uploader country of origin.

---

# Image Search

- idGettr ([https:// www.webpagefx.com/tools/ idgettr](https://www.webpagefx.com/tools/idgettr) ): Find the Flickr ID number (also works for groups).
- Google reverse search (<https://www.google.com/imghp?hl=en>): Google has a dedicated search engine for image reverse searches; you can either paste the image URL in the search box or upload it to Google

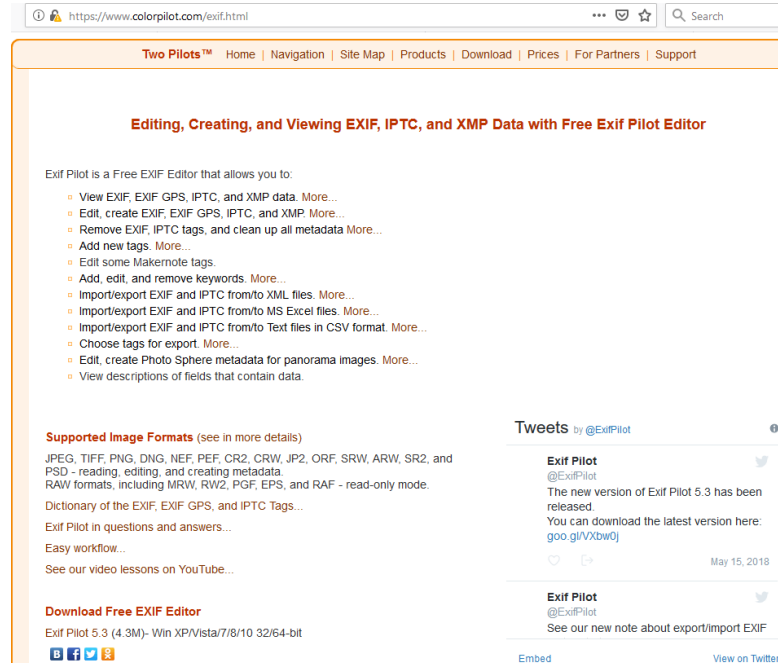


# Image Search

- TinyEye ( [www.tineye.com](http://www.tineye.com) ): You can search by image or URL; more than 24 billion images have already been indexed.
- Reverse Image Search ( [www.reverse-image-search.com](http://www.reverse-image-search.com) ): Conduct a reverse image search with Google, Bing, and Yandex.
- Image Identification Project ( <https://www.imageidentify.com> ): This uses visual search technology to recognize uploaded images.

# Image data

Exif Pilot ( [www.colorpilot.com/exif.html](http://www.colorpilot.com/exif.html) ) is a free EXIF editor that allows you to view, edit, and remove EXIF, EXIF GPS, IPTC, and XMP data



The screenshot shows the website for Exif Pilot. At the top, there is a navigation bar with the following links: Home | Navigation | Site Map | Products | Download | Prices | For Partners | Support. Below the navigation bar is a main heading: **Editing, Creating, and Viewing EXIF, IPTC, and XMP Data with Free Exif Pilot Editor**.

The main content area starts with the text: "Exif Pilot is a Free EXIF Editor that allows you to:" followed by a list of features:

- View EXIF, EXIF GPS, IPTC, and XMP data. More...
- Edit, create EXIF, EXIF GPS, IPTC, and XMP. More...
- Remove EXIF, IPTC tags, and clean up all metadata More...
- Add new tags. More...
- Edit some Makernote tags.
- Add, edit, and remove keywords. More...
- Import/export EXIF and IPTC from/to XML files. More...
- Import/export EXIF and IPTC from/to MS Excel files. More...
- Import/export EXIF and IPTC from/to Text files in CSV format. More...
- Choose tags for export. More...
- Edit, create Photo Sphere metadata for panorama images. More...
- View descriptions of fields that contain data.

Below the list is a section titled **Supported Image Formats** (see in more details) which lists: JPEG, TIFF, PNG, DNG, NEF, PEF, CR2, CRW, JP2, ORF, SRW, ARW, SR2, and PSD - reading, editing, and creating metadata. It also mentions RAW formats including MRW, RW2, PGF, EPS, and RAF - read-only mode. Other links include "Dictionary of the EXIF, EXIF GPS, and IPTC Tags...", "Exif Pilot in questions and answers...", "Easy workflow...", and "See our video lessons on YouTube..."

At the bottom left, there is a section for **Download Free EXIF Editor** with the text: "Exif Pilot 5.3 (4.3M)- Win XP/Vista/7/8/10 32/64-bit" and social media icons for Facebook, Twitter, and YouTube.

On the right side of the page, there is a "Tweets by @ExifPilot" section. The first tweet is from Exif Pilot (@ExifPilot) dated May 15, 2018, stating: "The new version of Exif Pilot 5.3 has been released. You can download the latest version here: [goo.gl/vXbw0j](http://goo.gl/vXbw0j)". The second tweet is also from Exif Pilot (@ExifPilot) and says: "See our new note about export/import EXIF".

# Image Tools

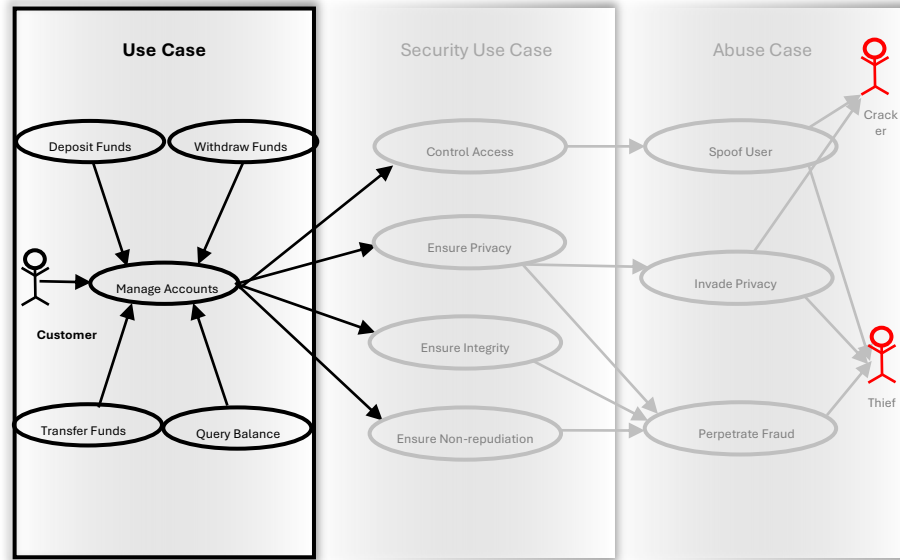
- Forensically ( <https://29a.ch/photo-forensics/#forensic-magnifier> ): This site offers free tools for image forensics analysis; it includes clone detection, error-level analysis, metadata extraction, and more.
- Ghire ( [www.getghiro.org](http://www.getghiro.org) ): This is an open source tool that can analyze images in bulk and extract metadata information, use GPS metadata to search for nearby images, and perform ELA to detect whether an image has been manipulated. You can download this program as a virtual appliance that is ready to use (it comes installed within Linux Ubuntu).

---

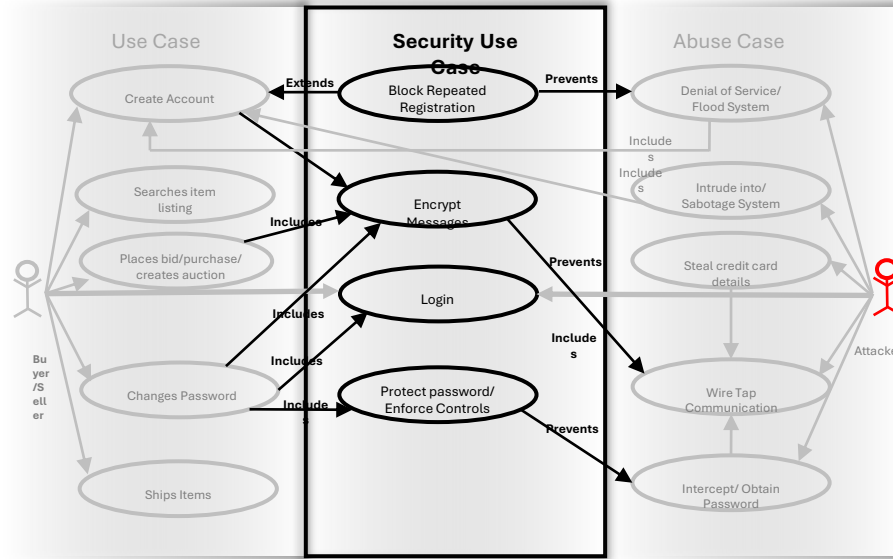
# Video Search

- YouTube ( [https:// www.youtube.com](https://www.youtube.com) )
- Google videos ( <https://www.google.com/videohp> )
- StartPage video search ( <https://www.startpage.com/eng/video.html> )
- Veoh ( [www.veoh.com](http://www.veoh.com) )
- Vimeo ( <https://vimeo.com> )
- 360daily ( [www.360daily.com](http://www.360daily.com) )

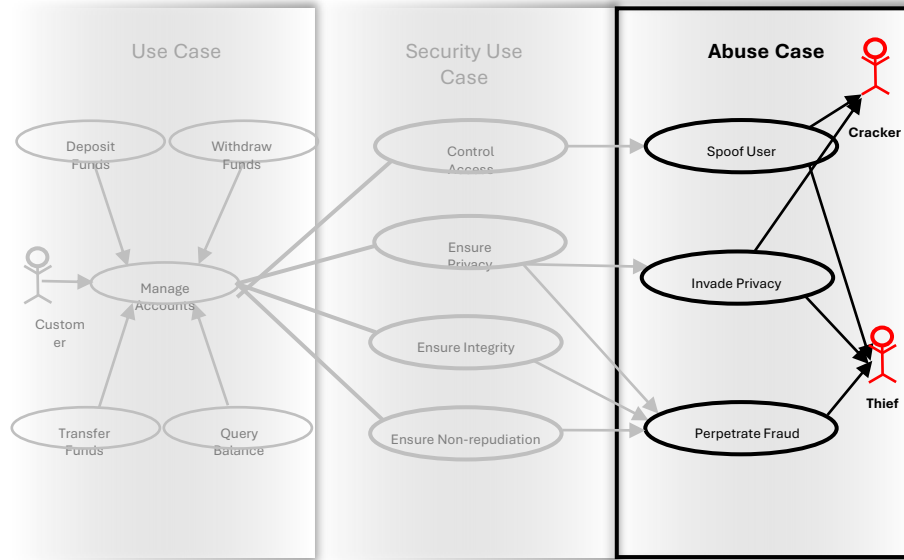
## Use Case for ATM System



# Security Use Case for Online Bidding System



## Abuse Case for ATM System

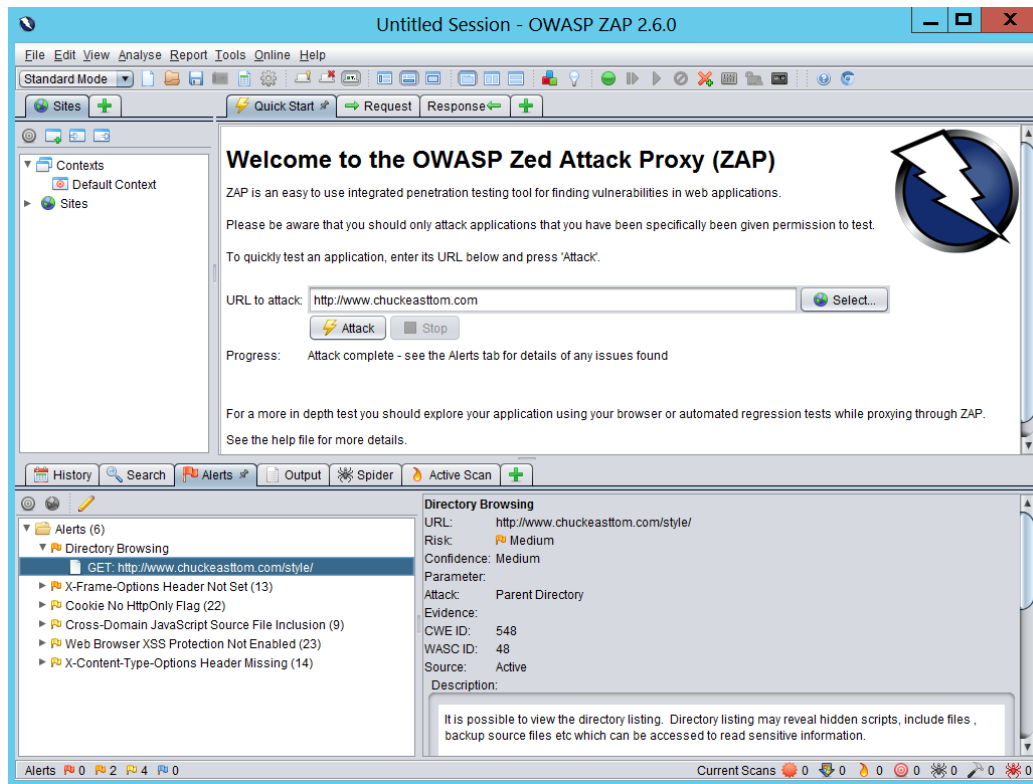


# OWASP ZAP

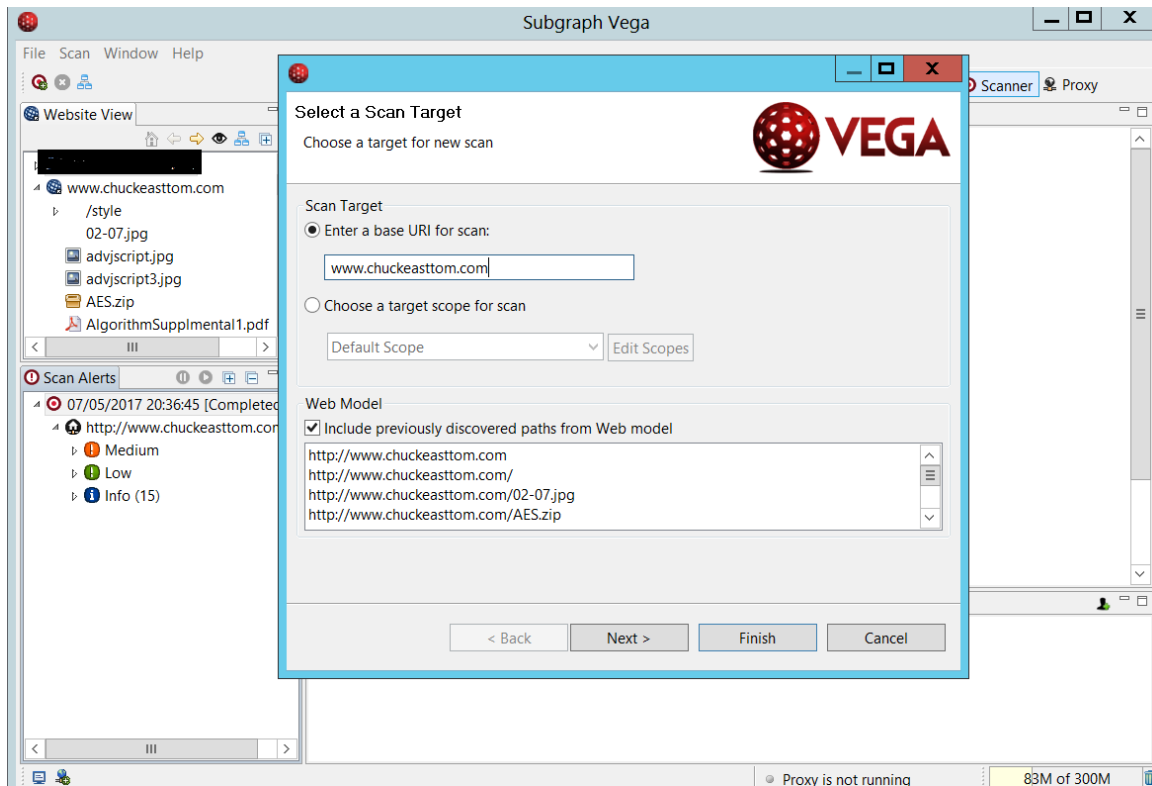
The screenshot displays the OWASP Zed Attack Proxy (ZAP) interface. The main window shows a 'Welcome to the OWASP Zed Attack Proxy (ZAP)' message. Below the message, there is a text input field for the URL to attack, containing 'http://www.chuckeasttom.com'. There are 'Attack' and 'Stop' buttons. The progress bar indicates 'Spidering the URL to discover the content' and is at 35% completion. The bottom section shows a table of processed requests.

Processed	Method	URI	Flags
●	GET	https://www.google.com/patents/US8713057	Out of Scope
●	GET	https://www.google.com/patents/US8819827	Out of Scope
●	GET	https://www.google.com/patents/US8825845	Out of Scope
●	GET	https://www.google.com/patents/US8825810	Out of Scope
●	GET	https://www.google.com/patents/US9313167	Out of Scope
●	GET	http://patft.uspto.gov/netacgi/nph-Parser?OS=Ineasttom&RS=IN...	Out of Scope
●	GET	http://patft.uspto.gov/netacgi/nph-Parser?OS=easttom&RS=east...	Out of Scope
●	GET	http://patft.uspto.gov/netacgi/nph-Parser?OS=easttom&RS=east...	Out of Scope
●	GET	http://www.chuckeasttom.com/chuckspeakings.jpg	
●	GET	https://www.iacr.org/archive/ches2004/31560162/31560162.pdf	Out of Scope
●	GET	http://news.cnet.com/news/0-1007-200-316690.html?tag=rtdnws	Out of Scope
●	GET	http://www.chuckeasttom.com/02-07.jpg	

# OWASP ZAP



# VEGA



# VEGA

The screenshot displays the Subgraph Vega web security platform interface. The main window is titled "Subgraph Vega" and features a menu bar with "File", "Scan", "Window", and "Help". The interface is divided into several panels:

- Website View:** Shows a directory tree for "www.chuckeasttom.com" with subdirectories like "/style" and files such as "02-07.jpg", "advjscrip3.jpg", "advjscrip3.jpg", "AES.zip", and "AlgorithmSupplmental1.pdf".
- Scan Alerts:** Lists scan results, including a completed scan on "07/05/2017 20:36:45" for "http://www.chuckeasttom.com" with a "Medium" risk level and a "Local Filesystem Paths Found" alert.
- Scan Info:** Displays the "Local Filesystem Paths Found" alert details, including a table for classification and risk levels.
- Identities:** A section for managing identities, currently empty.

The "Local Filesystem Paths Found" alert details are as follows:

Local Filesystem Paths Found	
▶ AT A GLANCE	
Classification	Information
Resource	/
Risk	Medium

Below the "AT A GLANCE" section, the "REQUEST" section shows "GET /" and the "RESOURCE CONTENT" section shows the path "/11b/smb/js/hosting/cp/js\_source/whv".

The status bar at the bottom indicates "Proxy is not running" and "89M of 300M".

---

# Open Source Tools

- **Avignon:** Tests HTML, ASP.Net <http://avignon.sourceforge.net/>
- **Doit: Simple Web Application Testing:** testing web forms.  
<http://doit.sourceforge.net/>
- **SWAT (Simple Web Automation Toolkit)**  
<http://sourceforge.net/projects/ulti-swat/>
- **Multiple tools** <http://aptest.com/resources.html>

# shodanhq

Like living on the edge? Try out the beta website for Shodan.


Shodan Exploits Scanhub Maps Blog Membership Settings

SHODAN "default password" Search

Home Search Directory Data Analytics/ Exports Developer Center Labs

Vote

Results 1 - 10 of about

Services		
<a href="#">Telnet</a>	3,229	<a href="#">163.20.255.9</a>
<a href="#">HTTP</a>	656	Tiawan Academic Network (TANet) Information Center Added on 12.11.2013
<a href="#">FTP</a>	646	 Taipei
<a href="#">HTTP Alternate</a>	37	<a href="#">Details</a>
<a href="#">Telnet (2323)</a>	14	r7513-mp.ntpc.edu.tw

**Top Countries**

<a href="#">United States</a>	1,016
<a href="#">China</a>	452
<a href="#">Germany</a>	335
<a href="#">Japan</a>	329
<a href="#">Mexico</a>	243

-----  
Cisco Router and Security Device Manager (SDM) is installed on this device.  
This feature requires the one-time use of the username "cisco"  
with the **password** "cisco". The **default** username and **password** have a privilege level  
  
Please change these publicly known initial credentials using SDM or the IOS CLI.  
Here are the Cisco IOS commands.  
  
username <myuser> privilege 15 secret 0 <my**password**>  
no username...

[83.240.190.74](#)  
PT Comunicacoes

---

# shodanhq

- Search for default passwords
  - default password country:US
  - default password hostname:chuckeasttom.com
  - default password city:Plano
- Find Apache servers
  - apache city:"San Francisco"
- Find Webcams
  - webcamxp city:Chicago
- OLD IIS
  - "iis/5.0"

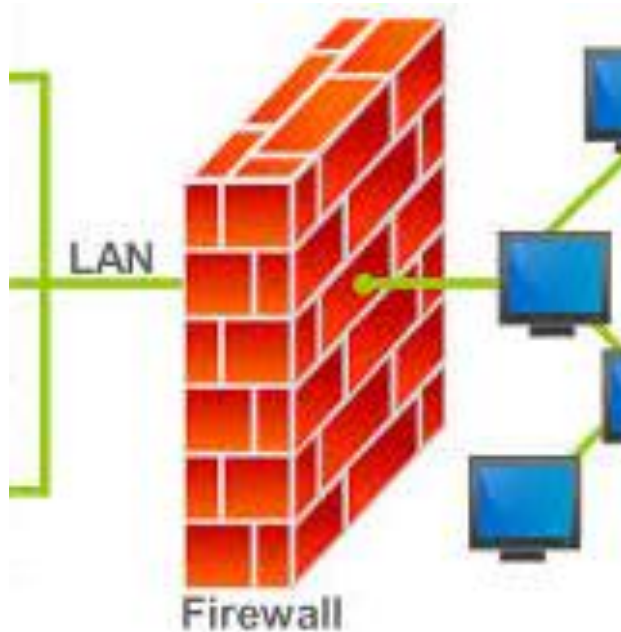
---

# shodanhq

- Filters
  - Country
  - City (does not always work)
  - Hostname
  - net (Ip range)
  - OS
  - Port

---

# Port Scanning Counter Measures



- Configure firewall and IDS to block probes
- Block ICMP
- Perform your own scanning
- Filter at routers
- Update router, IDS, and Firewall

---

# Scanning Tools

SuperScan (<https://www.mcafee.com>)

PRTG Network Monitor (<https://www.paessler.com>)

OmniPeek (<https://www.savvius.com>)

MiTeC Network Scanner (<http://www.mitec.cz>)

NEWT Professional (<http://www.komodolabs.com>)

MegaPing (<http://www.magnetosoft.com>)

SolarWinds Engineer's Toolset (<http://www.solarwinds.com>)

NetScanTools Pro (<https://www.netscantools.com>)

Colasoft Ping Tool (<http://www.colasoft.com>)

Visual Ping Tester (<http://www.pingtester.net>)

OpUtils (<https://www.manageengine.com>)



---

# Mobile Scanning Tools

Hackode

<https://play.google.com>

zANTI

<https://www.zimperium.com>

cSploit

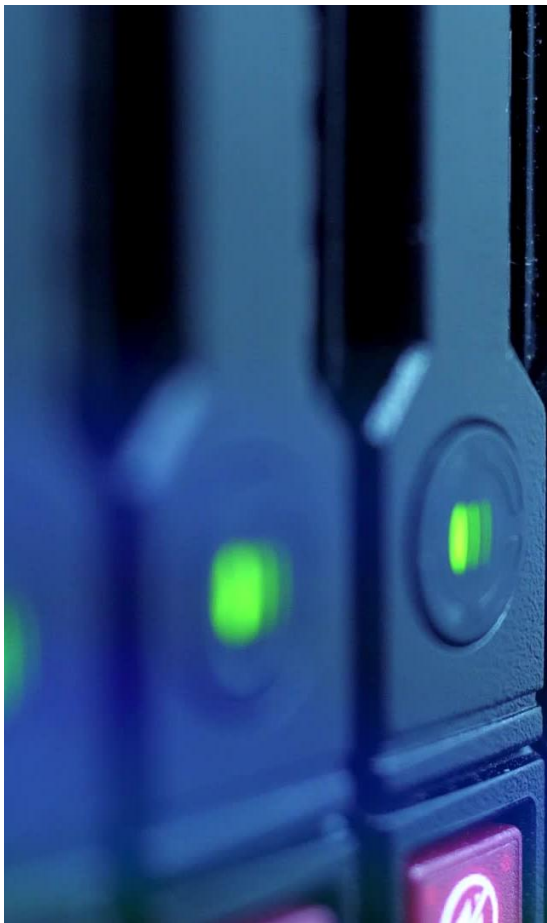
<http://www.csploit.org>

FaceNiff

<http://www.effecthacking.com>

PortDroid Network Analysis

<https://play.google.com>



---

# Google Vulnerability Searching

- Find shared directories on servers  
*intitle:"index of" myshare*
- Find apache servers with a specific version of SSL "OpenSSL" AND "1.0.1 Server at" OR "1.0.1a Server at" OR "1.0.1b Server at" OR "1.0.1c Server at" OR "1.0.1d Server at" OR "1.0.1e Server at" OR "1.0.1f Server at"
- <https://www.exploit-db.com/>



---

# Find Web Cams

- Most basic *inurl:view/index.shtml*
- Alternatives
  - *intitle:liveapplet inurl:LvAppl*
  - *inurl:view/view.shtml*
  - *inurl:axis-cgi/mjpg (motion-JPEG)*
  - *inurl:view/indexFrame.shtml*
- More
  - [http://www.webcamvue.com/find\\_webcams.asp](http://www.webcamvue.com/find_webcams.asp)
- Search in site
- *inurl:view/index.shtml site:sunderland.ac.uk*



---

# Web Cams Default password

- ACTi:** *admin/123456* or *Admin/123456*
- Axis (traditional):** *root/pass*,
- Axis (new):** requires password creation during first login
- Cisco:** No default password, requires creation during first login
- IQinVision:** *root/system*
- Mobotix:** *admin/meinsm*
- Panasonic:** *admin/12345*
- Samsung Electronics:** *root/root* or *admin/4321*
- Samsung Techwin (old):** *admin/1111111* or *admin/4321*
- Sony:** *admin/admin*
- TRENDnet:** *admin/admin*
- Toshiba:** *root/ikwd*
- Vivotek:** *root/<blank>*
- WebcamXP:** *admin/ <blank>*



---

# Find Email Servers

- You can lookup email servers for any given domain
  - <http://mxlookup.online-domain-tools.com/>
  - <http://www.hashemian.com/tools/domain-email.php>
- Check to see if the email you have exists
  - <http://mailtester.com/>



---

# Find hacked accounts

- <https://pwnedlist.com/query>
- <https://haveibeenpwned.com/>
- <https://lastpass.com/adobe/>
- <http://nullprogram.com/gmail-bloom-filter/>



---

# Tools

- Beam Us Up SEO Spider SEO (<http://beamusup.com>)
- WildShark SEO Spider Tool (<https://wildshark.co.uk>)
- Visual SEO Studio (<https://visual-seo.com>)
- SpiderFoot (<http://www.spiderfoot.net>)
- ExtractMetadata (<http://www.extractmetadata.com>)
- FOCA (<https://www.elevenpaths.com>)
- Meta Tag Analyzer (<https://www.seocentro.com>)
- BuzzStream (<http://tools.buzzstream.com>)
- Analyse Metadata (<http://www.exadium.com>)
- Exiftool (<http://www.sno.phy.queensu.ca>)
- VisualPing (<https://visualping.io>)
- Follow That Page (<https://www.followthatpage.com>)
- <http://www.whoisanalyzer.com>
- <https://www.whois.com.au>
- <https://whois.icann.org>