



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.

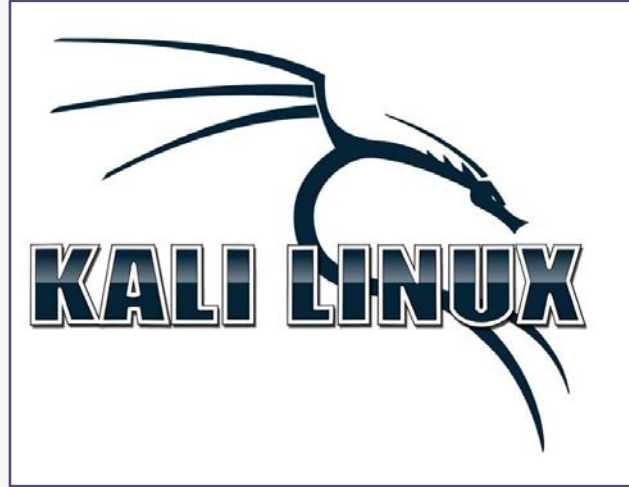


#include <std_disclaimer>

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
2021-10-06T03:54:35.827724Z -> 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	Manage Containers	Manage Images	Info & Stats
<p>Start a new Container from an image</p> <pre>docker run IMAGE docker run nginx</pre> <p>...and assign it a name</p> <pre>docker run --name CONTAINER IMAGE docker run --name web nginx</pre> <p>...and map a port</p> <pre>docker run -p HOSTPORT:CONTAINERPORT IMAGE docker run -p 8080:80 nginx</pre> <p>...and map all ports</p> <pre>docker run -P IMAGE docker run -P nginx</pre> <p>...and start container in background</p> <pre>docker run -d IMAGE docker run -d nginx</pre> <p>...and assign it a hostname</p> <pre>docker run --hostname HOSTNAME IMAGE docker run --hostname srv nginx</pre> <p>...and add a dns entry</p> <pre>docker run --add-host HOSTNAME:IP IMAGE</pre> <p>...and map a local directory into the container</p> <pre>docker run -v HOSTDIR:TARGETDIR IMAGE docker run -v ~/.usr/share/nginx/html nginx</pre> <p>...but change the entrypoint</p> <pre>docker run -it --entrypoint EXECUTABLE IMAGE docker run -it --entrypoint bash nginx</pre>	<p>Show a list of running containers</p> <pre>docker ps</pre> <p>Show a list of all containers</p> <pre>docker ps -a</pre> <p>Delete a container</p> <pre>docker rm CONTAINER docker rm web</pre> <p>Delete a running container</p> <pre>docker rm -f CONTAINER docker rm -f web</pre> <p>Delete stopped containers</p> <pre>docker container prune</pre> <p>Stop a running container</p> <pre>docker stop CONTAINER docker stop web</pre> <p>Start a stopped container</p> <pre>docker start CONTAINER docker start web</pre> <p>Copy a file from a container to the host</p> <pre>docker cp CONTAINER:SOURCE TARGET docker cp web:/index.html index.html</pre> <p>Copy a file from the host to a container</p> <pre>docker cp TARGET CONTAINER:SOURCE docker cp index.html web:/index.html</pre> <p>Start a shell inside a running container</p> <pre>docker exec -it CONTAINER EXECUTABLE docker exec -it web bash</pre> <p>Rename a container</p> <pre>docker rename OLD_NAME NEW_NAME docker rename 096 web</pre> <p>Create an image out of container</p> <pre>docker commit CONTAINER docker commit web</pre>	<p>Download an image</p> <pre>docker pull IMAGE[:TAG] docker pull nginx</pre> <p>Upload an image to a repository</p> <pre>docker push IMAGE docker push myimage:1.0</pre> <p>Delete an image</p> <pre>docker rmi IMAGE</pre> <p>Show a list of all Images</p> <pre>docker images</pre> <p>Delete dangling images</p> <pre>docker image prune</pre> <p>Delete all unused images</p> <pre>docker image prune -a</pre> <p>Build an image from a Dockerfile</p> <pre>docker build DIRECTORY docker build .</pre> <p>Tag an image</p> <pre>docker tag IMAGE NEWIMAGE docker tag ubuntu ubuntu:18.04</pre> <p>Build and tag an image from a Dockerfile</p> <pre>docker build -t IMAGE DIRECTORY docker build -t myimage .</pre> <p>Save an image to .tar file</p> <pre>docker save IMAGE > FILE docker save nginx > nginx.tar</pre> <p>Load an image from a .tar file</p> <pre>docker load -i TARBFILE docker load -i nginx.tar</pre>	<p>Show the logs of a container</p> <pre>docker logs CONTAINER docker logs web</pre> <p>Show stats of running containers</p> <pre>docker stats</pre> <p>Show processes of container</p> <pre>docker top CONTAINER docker top web</pre> <p>Show installed docker version</p> <pre>docker version</pre> <p>Get detailed info about an object</p> <pre>docker inspect NAME docker inspect nginx</pre> <p>Show all modified files in container</p> <pre>docker diff CONTAINER docker diff web</pre> <p>Show mapped ports of a container</p> <pre>docker port CONTAINER docker port web</pre>

Foundations (git)

- Normal routines
- Compromise and reconnaissance

Git Cheat Sheet

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

GIT BASICS

<code>git init <directory></code>	Create empty Git repo in specified directory. Run with no arguments to initialize the current directory as a git repository.
<code>git clone <repo></code>	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.
<code>git config user.name <name></code>	Define author name to be used for all commits in current repo. Devs commonly use <code>--global</code> flag to set config options for current user.
<code>git add <directory></code>	Stage all changes in <directory> for the next commit. Replace <directory> with a <file> to change a specific file.
<code>git commit -m "message"</code>	Commit the staged snapshot, but instead of launching a text editor, use <message> as the commit message.
<code>git status</code>	List which files are staged, unstaged, and untracked.
<code>git log</code>	Display the entire commit history using the default format. For customization see additional options.
<code>git diff</code>	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		Assertions	
^	Start of string, or start of line in multi-line pattern	?=	Lookahead assertion
\A	Start of string	?!	Negative lookahead
\$	End of string, or end of line in multi-line pattern	?<=	Lookbehind assertion
\Z	End of string	?!= or ?<!	Negative lookbehind
\b	Word boundary	?>	Once-only Subexpression
\B	Not word boundary	?()	Condition [if then]
<	Start of word	?()	Condition [if then else]
\>	End of word	?#	Comment
Character Classes		Quantifiers	
\c	Control character	* 0 or more	{3} Exactly 3
\s	White space	+ 1 or more	{3,} 3 or more
\S	Not white space	? 0 or 1	{3,5} 3, 4 or 5
\d	Digit	Add a ? to a quantifier to make it ungreedy.	
\D	Not digit	Escape Sequences	
\w	Word	\	Escape following character
Groups and Ranges		Pattern Modifiers	
.	Any character except new line (\n)	g	Global match
(a b)	a or b	i *	Case-insensitive
(...)	Group	m *	Multiple lines
(?...)	Passive (non-capturing) group	s *	Treat string as single line
[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.			

Foundations (the rest)

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

Zenmap (nmap UI)

The screenshot displays the Zenmap (nmap UI) interface. At the top, the 'Command' tab is selected, showing the command: `nmap -T Paranoid -sF -sV -6 -O <target>`. Below this, the 'Scan' tab is active, showing various scan options. The 'Scan options' section includes:

- TCP scan: **FIN scan** (dropdown menu)
- Special scans: (empty dropdown menu)
- Timing: **Paranoid** (dropdown menu)
- ☐ FTP bounce attack
- ☐ Idle Scan (Zombie)
- ☒ Services version detection
- ☒ Operating system detection
- ☐ Disable reverse DNS resolution
- ☒ IPv6 support
- ☐ Maximum Retries: **1** (spin box)

At the bottom, there are three buttons: **Help** (with a question mark icon), **Cancel** (with a red X icon), and **OK** (with a green checkmark icon).

Defense

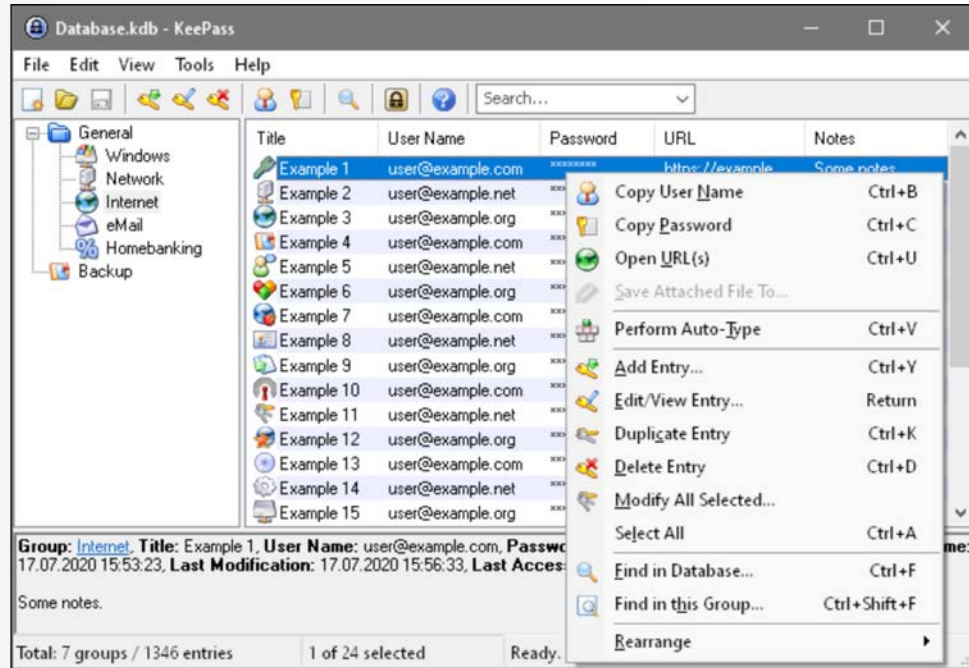
- Keepass and pass
- pfsense
- OSSEC
- Security Onion
- OpenVAS

Defense (Keepass 2.x)

Open source password manager

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

Are password managers safe?



Defense (pass)

Open source password manager

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

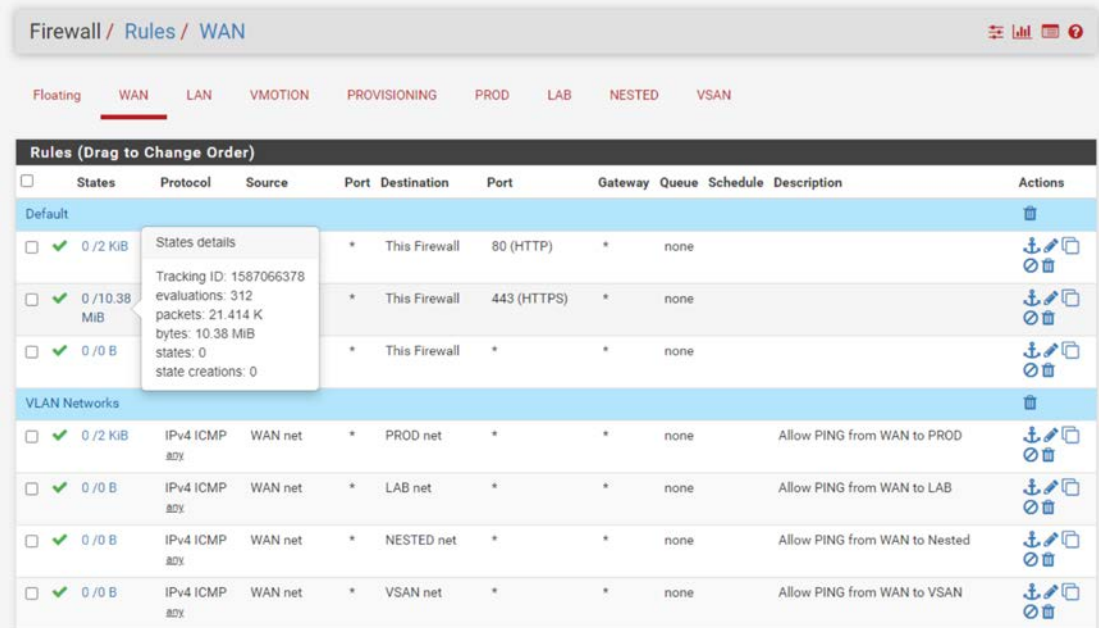
```
zx2c4@laptop ~ $ pass
Password Store
├─ Business
│   ├─ some-silly-business-site.com
│   └─ another-business-site.net
├─ Email
│   ├─ donenfeld.com
│   └─ zx2c4.com
└─ France
    ├─ bank
    ├─ freebox
    └─ mobilephone
```

```
[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

Floating **WAN** LAN VMOTION PROVISIONING PROD LAB NESTED VSAN

Rules (Drag to Change Order)

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

States details

Tracking ID: 1587066378

evaluations: 312

packets: 21.414 K

bytes: 10.38 MiB

states: 0

state creations: 0

Visualize - <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/>

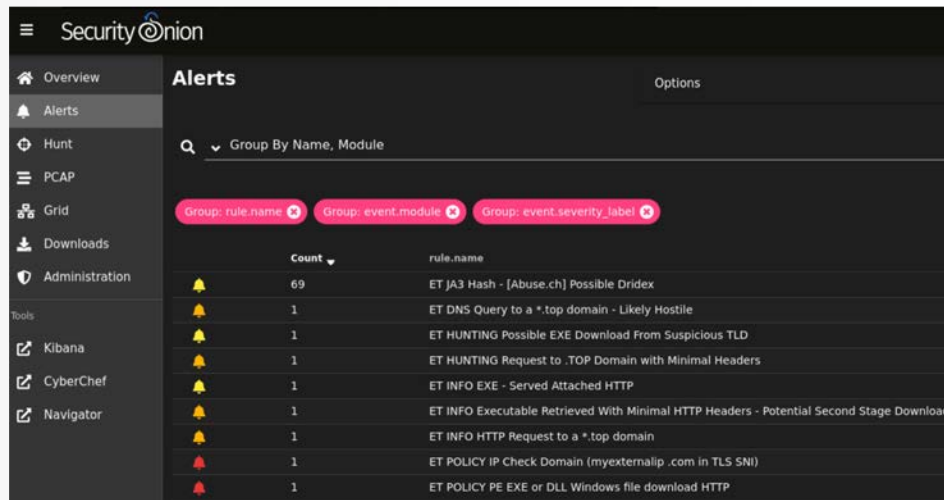


Visualize - <https://github.com/Graylog2/graylog-guide-ossec>

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



The screenshot shows the Security Onion Alerts dashboard. The left sidebar contains navigation links: Overview, Alerts, Hunt, PCAP, Grid, Downloads, Administration, Tools, Kibana, CyberChef, and Navigator. The main panel is titled 'Alerts' and has a search bar with the text 'Group By Name, Module'. Below the search bar are three filter buttons: 'Group: rule.name', 'Group: event.module', and 'Group: event.severity_label'. The table below shows a list of alerts with columns for 'Count' and 'rule.name'.

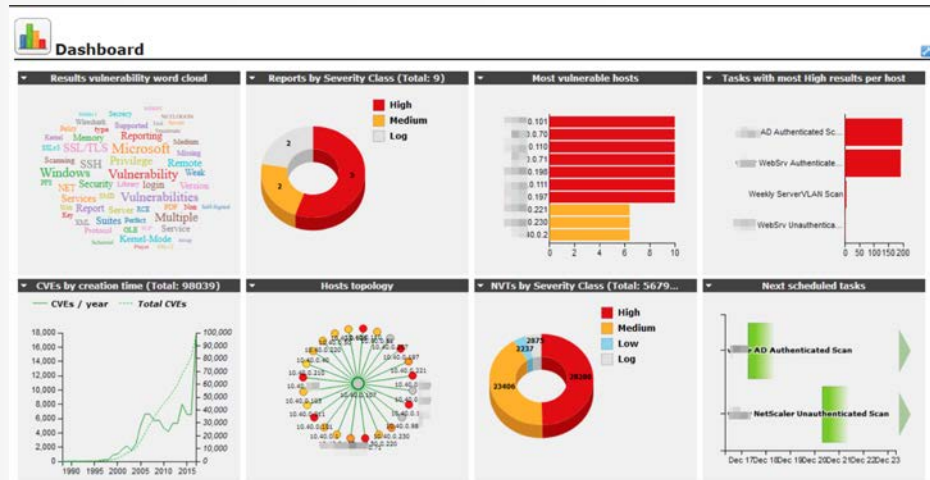
	Count	rule.name
🟡	69	ET JA3 Hash - [Abuse.ch] Possible Dridex
🟡	1	ET DNS Query to a *.top domain - Likely Hostile
🟡	1	ET HUNTING Possible EXE Download From Suspicious TLD
🟡	1	ET HUNTING Request to .TOP Domain with Minimal Headers
🟡	1	ET INFO EXE - Served Attached HTTP
🟡	1	ET INFO Executable Retrieved 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

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 analyzer) - <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>

HACKER TARGET	
SCANNERS	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>

TLS/SSL Certificates as well

General Information	
Hostnames	office1.cc.iup.edu
Domains	<input type="text" value="IUP.EDU"/>
Country	United States
City	Indiana
Organization	Indiana University of Pennsylvania
ISP	Indiana University of Pennsylvania
ASN	AS62989

Open Ports	
80	443
// 80 / TCP	
HTTP/1.1 302 Moved Temporarily Content-Type: text/html Date: Sat, 09 Oct 2021 13:51:39 GMT Location: https://144.80.128.103/ Connection: Keep-Alive Content-Length: 0	
// 443 / TCP	
HTTP/1.1 302 Moved Temporarily Content-Type: text/html Date: Wed, 20 Oct 2021 13:40:53 GMT Location: https://login.microsoftonline.com/?whr=iup.edu Connection: Keep-Alive Content-Length: 0	

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?

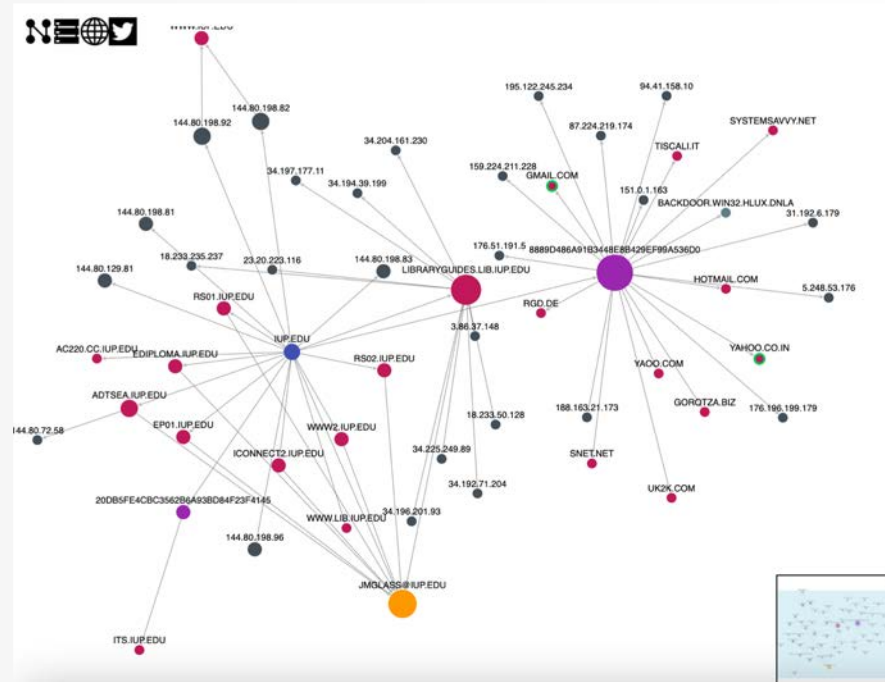
4364878188	2021-04-12	2021-04-12	2022-04-12	degreeworks.iup.edu	degreeworks.iup.edu
4364866557	2021-04-12	2021-04-12	2022-04-12	dworks2-dev.cc.iup.edu	dworks2-dev.cc.iup.edu
4364866545	2021-04-12	2021-04-12	2022-04-12	dworks2-dev.cc.iup.edu	dworks2-dev.cc.iup.edu
4364859613	2021-04-12	2021-04-12	2022-04-12	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
					erapppp02.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

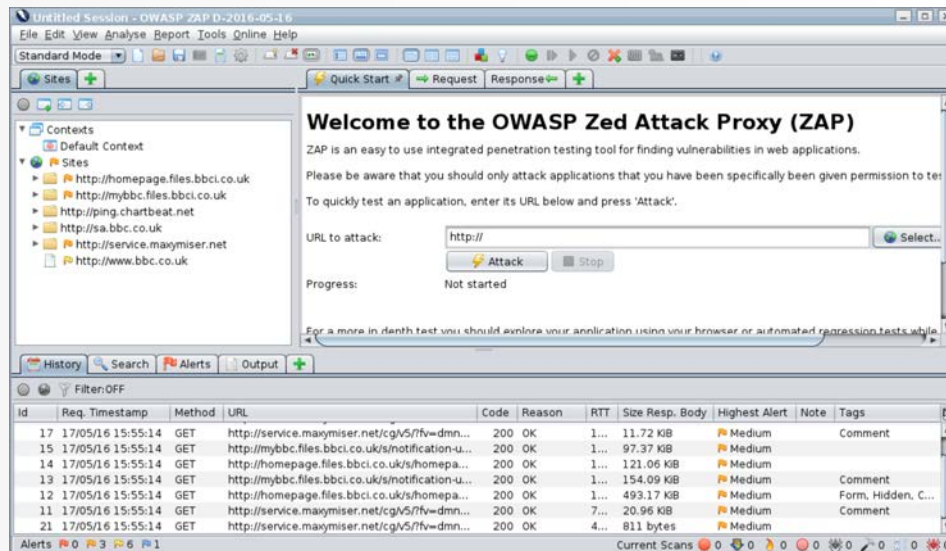
Process list
=====
```

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

Zed Attack Proxy (OWASP)

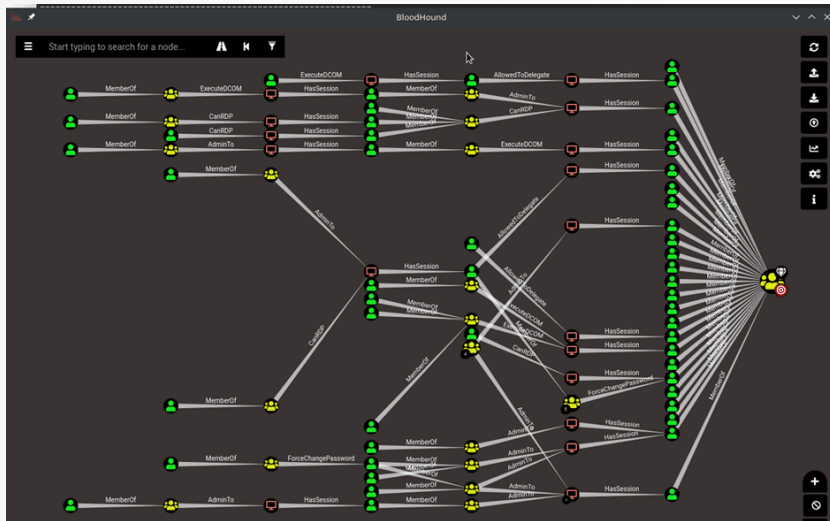
- <https://owasp.org/www-project-top-ten/>



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

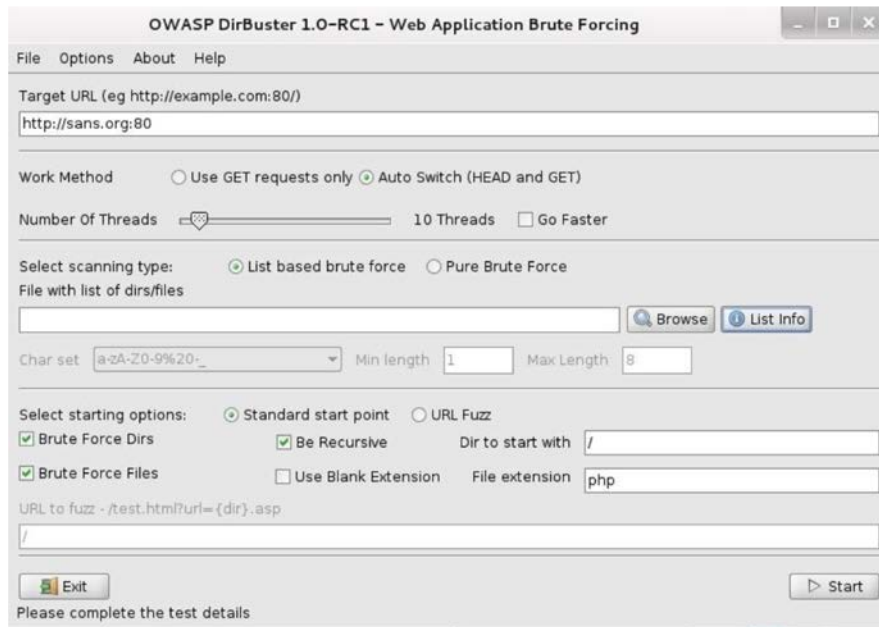
- config+      Use this config file
- Display+    Turn on/off display outputs
- dbcheck     check database and other key files for syntax errors
- Format+     save file (-o) format
- Help        Extended help information
- host+       target host
- id+         Host authentication to use, format is id:pass 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

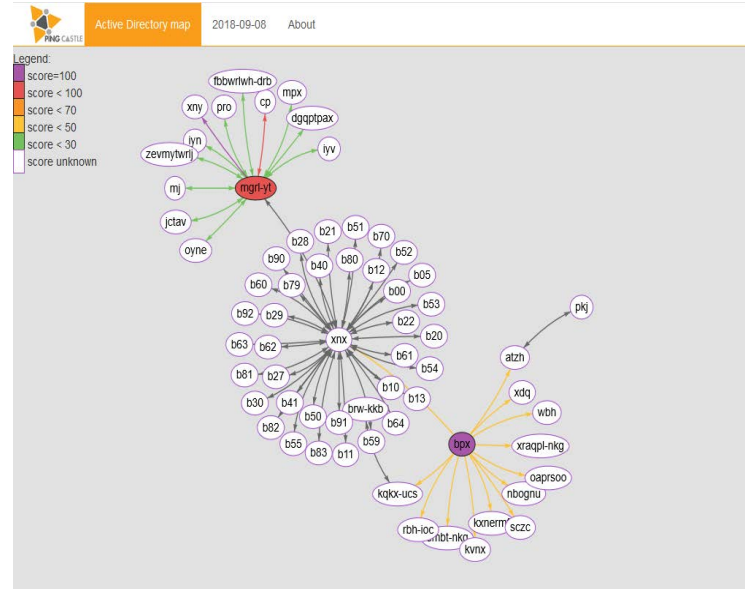
- Directory traversal attack
- Webserver structure
- Hidden*/Confidential files
- Brute force wordlists
- <https://sourceforge.net/projects/dirbuster/>



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>



```
[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 'razer.yaml': force_post: unknown type - only 'post' is v
[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	@prrrrrinncee	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		IP RELATED OPTIONS		TCP/UDP RELATED OPTIONS		ICMP CODES	
-q	-quiet	-a	-spoof	-s	-baseport [random],+1 on received	0	Echo Reply
-I	-interface	-r	-rand-source	-P	-destport [0] if have, have:	1	Unassigned
-D	-debug	-t	-rand-dest	++port	increased for each reply	2	Unassigned
-c	-count	-t	-ttl	++port	increased for each sent	3	Destination Unreachable
-i	-interval	-n	-id	-keep	still source port	4	Source Quench
	count response packets	-H	-ipprot	-w	-win set win size [64]	5	Redirect
-b	-beep	-W	-winid	-O	-topenf -b -badchksm	6	Alternate Host Address
	beep every received packet (no icmp)	-r	-rel	-M	-setseq -L -setack	7	Unassigned
-n	-numeric	-f	-frag	-Q	-seqnum collect seq numbers	8	Echo
-z	-bind	-x	-morefrag	-t	-tcp-timestamp set timestamp	9	Router Advertisement
	use ctrl+z to increment TTL	-y	-dontrfrag			10	Router Selection
-Z	-unbind	-g	-fragoff			11	Time Exceeded
	10 packets / sec	-G	-rroule			12	Parameter Problem
-f	-fast	-m	-mtu			13	Timestamp
	1 packet / μ s	-o	-tos			14	Timestamp Reply
-flood	as fast as possible					15	Information Request
COMMON OPTIONS		ICMP RELATED OPTIONS		TCP FLAGS		16	Information Reply
-d	-data	-C	-icmptype	-F	-fin	-S	-syn
-E	-file	-K	-icmpcode	-P	-push	-A	-ack
-s	-sign	-i	-icmp-ipv6	-X	-xmas	-Y	-ymas
-j	-dump		-icmp-iphlen				
-J	-print		-icmp-iphlen ip				
-B	-safe		-icmp-iplid				
-u	-end		-icmp-iproto				
-T	-traceroute		-icmp-cskum				
	traceroute mode, also:		-icmp-t				
-t	-keep-ttl		-icmp-t				
-tr	-tr-stop		-icmp-t				
-tr-no-rtt			-icmp-t				
-tpextcode			-icmp-t				
	set exit code to tcp->th_flag of last packet		-icmp-addr				
				PROTOCOL SELECTION -0 -rawip -1 -icmp -2 -ucp -8 -scan with: group ec: 20-53 comma delimited ex: 1,3,4 known: for /etc/services negated with !ex: !-53,!4 -9 -listen string match		20-29 Traceroute 30 Datagram Conversion Error 31 Mobile Host Redirect 32 IPv6 Where-Are-You 33 IPv6 I-Am-Here 34 Mobile Registration Request 35 Mobile Registration Reply 36 Domain Name Request 37 Domain Name Reply 38 SKIP 39 Phlatris 40-255 Reserved	

[?]: default value

SecurityByDefault.com

Uptime: hping2 -p 80 -S --top-timestamp host
 PortsCan: hping -l eth0 -s scan 20-25,80,443 -S host
 Sncan: hping -p 80 -i 0x10000 -a source -S host
 Backdoor: S → hping3 -l eth1 -9 -secret /bin/sh
 C → hping3 -R ip -e secret -C command file -d 100 -c 1

The diagram illustrates the structure of a TCP packet. It is divided into several sections: Source Port (4 bytes), Destination Port (4 bytes), Sequence Number (4 bytes), Acknowledgment Number (4 bytes), Data Offset (4 bytes), Reserved (6 bytes), Window (4 bytes), Checksum (4 bytes), Urgent Pointer (4 bytes), Options (variable length), Padding (variable length), and Data (variable length). The packet is shown as a sequence of bytes, with each section represented by a specific number of bytes.

The diagram illustrates the structure of an IP packet. It is divided into several sections: Version (4 bytes), IHL (4 bytes), TOS (4 bytes), DSCP/ECN (4 bytes), Identification (4 bytes), Flags (4 bytes), Time To Live (4 bytes), Protocol (4 bytes), Source Address (4 bytes), Destination Address (4 bytes), and Padding (variable length). The packet is shown as a sequence of bytes, with each section represented by a specific number of bytes.

The diagram illustrates the structure of a UDP packet. It is divided into several sections: Source Port (4 bytes), Destination Port (4 bytes), Length (4 bytes), Checksum (4 bytes), and Data (variable length). The packet is shown as a sequence of bytes, with each section represented by a specific number of bytes.

The diagram illustrates the structure of an ICMP packet. It is divided into several sections: Type (4 bytes), Code (4 bytes), and Checksum (4 bytes). The packet is shown as a sequence of bytes, with each section represented by a specific number of bytes.

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

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

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

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

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

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

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

Bitwise Operators

<code>-band</code>	Bitwise AND
<code>-bor</code>	Bitwise OR (inclusive)
<code>-bxor</code>	Bitwise OR (exclusive)
<code>-bnot</code>	Bitwise NOT
<code>-shl, -shr</code>	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 converter. 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

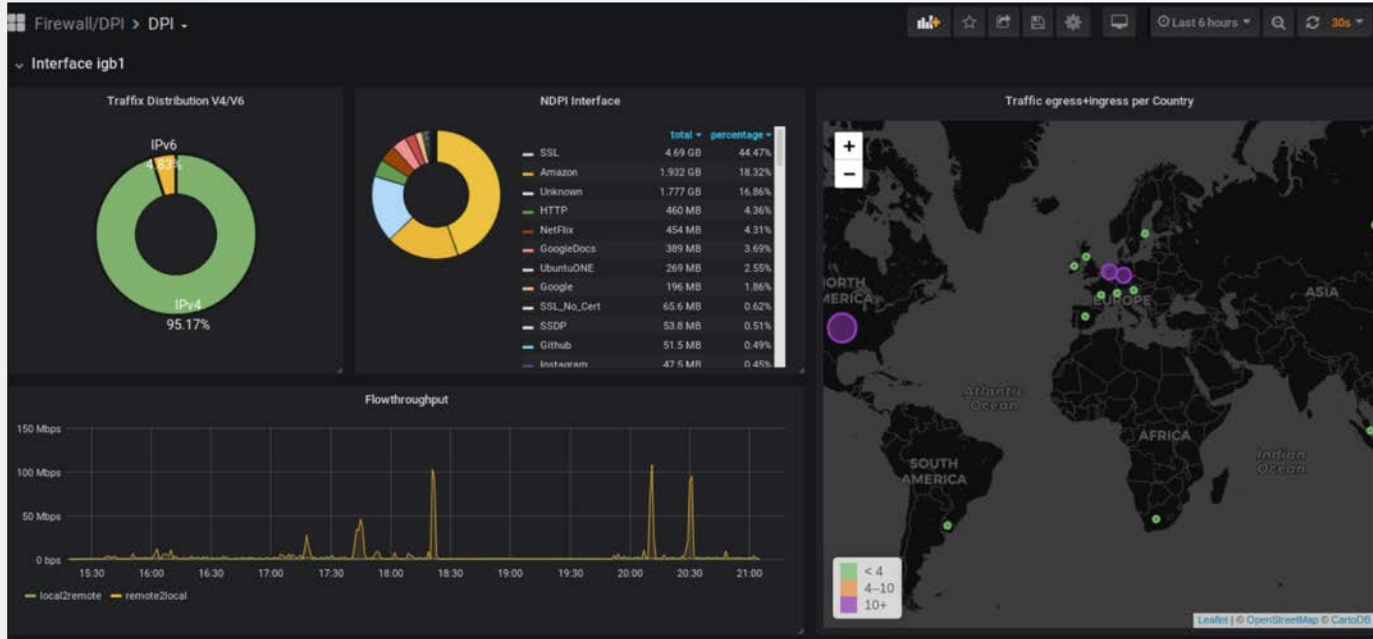
Redirection Operators

`>, >>` 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.

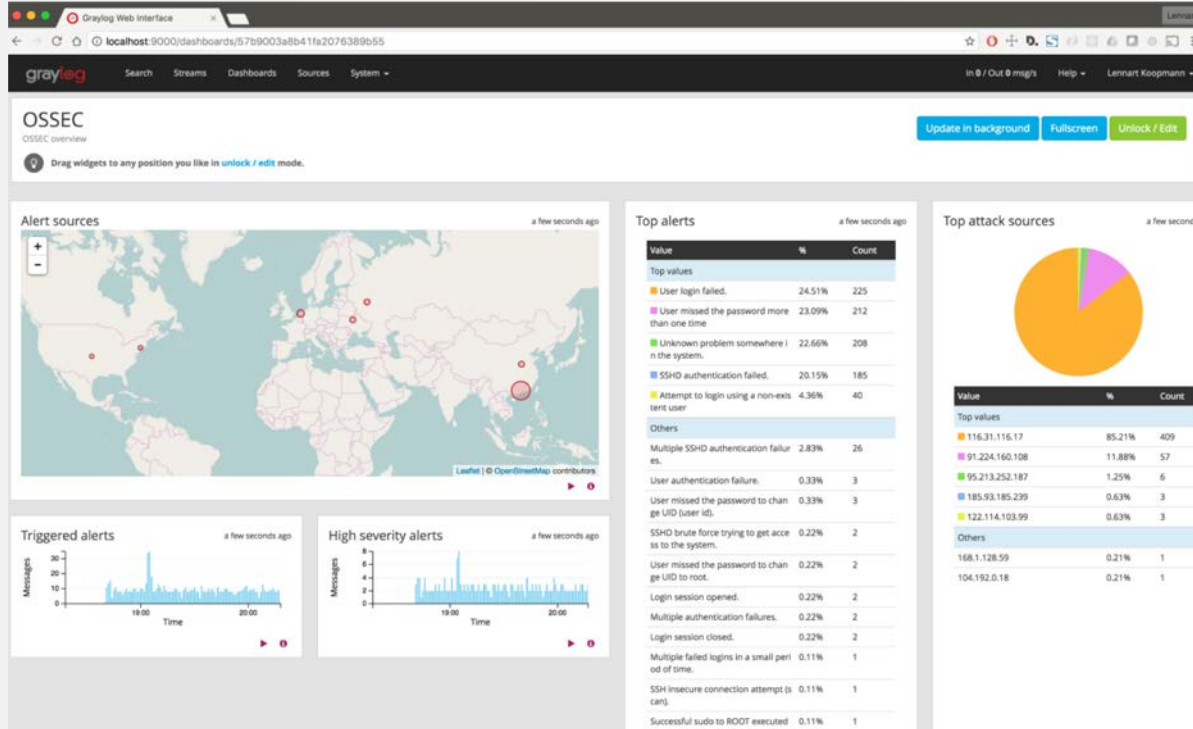
Output streams
* All output
1 Success output
2 Errors
3 Warning messages
4 Verbose output
5 Debug messages

`# 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



OSSEC Visualization



OSINT Framework

OSINT Framework

