BlueTeam-Tools

This github repository contains a collection of **50+ tools** and **resources** that can be useful for **blue teaming activities**.

Some of the tools may be specifically designed for blue teaming, while others are more general-purpose and can be adapted for use in a blue teaming context.

> □ *If you are a Red Teamer, check out RedTeam-Tools (https://github.com/A-poc/RedTeam-Tools)*

> ***Warning***
>
> *The materials in this repository are for informational and educational purposes only. They are not intended for use in any illegal activities.*

> ***Note***
>
> *Hide Tool List headings with the arrow.*
>
> *Click □ to get back to the list.*

Tool List

▼ **Blue Team Tips** $\textcolor{gray}{\text{3 tips}}$

- **Payload extraction with Process Hacker** *@embee_research*
- **Prevent Script Execution via Double Click** *Default Application GPO Change*
- **Detect Cryptojacking Malware with Proxy Logs** *Dave Mckay*

▼ **Network Discovery and Mapping** $\textcolor{gray}{\text{6 tools}}$

- **Nmap** *Network scanner*
- **Nuclei** *Vulnerability scanner*
- **Masscan** *Fast network scanner*
- **Angry IP Scanner** *IP/port scanner*
- **ZMap** *Large network scanner*
- **Shodan** *Internet facing asset search engine*

▼ **Vulnerability Management** $\textcolor{gray}{\text{4 tools}}$

- **OpenVAS** *Open-source vulnerability scanner*
- **Nessus Essentials** *Vulnerability scanner*
- **Nexpose** *Vulnerability management tool*
- **HackerOne** *Bug Bounty Management Platform*

▼ **Security Monitoring** $\textcolor{gray}{\text{10 tools}}$

- **Sysmon** *System Monitor for Windows*
- **Kibana** *Data visualization and exploration*
- **Logstash** *Data collection and processing*
- **parsedmarc** *Email DMARC data visualisation*
- **Phishing Catcher** *Phishing catcher using Certstream*
- **maltrail** *Malicious traffic detection system*
- **AutorunsToWinEventLog** *Windows AutoRuns Event Parser*
- **procfilter** *YARA-integrated process denial framework*

- **velociraptor** *Endpoint visibility and collection tool*
- **SysmonSearch** *Sysmon event log visualisation*

▼ **Threat Tools and Techniques** $\textcolor{gray}{\text{10 tools}}$

- **lolbas-project.github.io** *Living Off The Land Windows Binaries*
- **gtfobins.github.io** *Living Off The Land Linux Binaries*
- **filesec.io** *Attacker file extensions*
- **KQL Search** *KQL query aggregator*
- **Unprotect Project** *Malware evasion techniques knowledge base*
- **chainsaw** *Fast Windows Forensic Artefacts Searcher*
- **freq** *Domain generation algorithm malware detection*
- **yarGen** *YARA rule generator*
- **EmailAnalyzer** *Suspicious emails analyser*
- **VCG** *Code security scanning tool*

▼ **Threat Intelligence** $\textcolor{gray}{\text{3 tools}}$

- **Maltego** *Threat Intelligence Platform*
- **MISP** *Malware Information Sharing Platform*
- **ThreatConnect** *Threat data aggregation*

▼ **Incident Response Planning** $\textcolor{gray}{\text{3 tools}}$

- **NIST** *Cybersecurity Framework*
- **Incident Response Plan** *Framework for incident response*
- **Ransomware Response Plan** *Framework for ransomware response*

▼ **Malware Detection and Analysis** $\textcolor{gray}{\text{3 tools}}$

- **VirusTotal** *Malicious IOC Sharing Platform*
- **IDA** *Malware disassembler and debugger*
- **Ghidra** *Malware reverse engineering tool*

▼ **Data Recovery** $\textcolor{gray}{\text{3 tools}}$

- **Recuva** *File recovery*
- **Extundelete** *Ext3 or ext4 partition recovery*
- **TestDisk** *Data Recovery*

▼ **Digital Forensics** $\textcolor{gray}{\text{3 tools}}$

- **SANS SIFT** *Forensic toolkit*
- **The Sleuth Kit** *Disk images analysis tools*
- **Autopsy** *Digital forensics platform*

▼ **Security Awareness Training** $\textcolor{gray}{\text{3 tools}}$

- **TryHackMe** *Cyber security challenges platform*
- **HackTheBox** *Cyber security challenges platform*
- **PhishMe** *Phishing training*

▼ **Communication and Collaboration** $\textcolor{gray}{\text{2 tools}}$

- **Twitter** *Cyber Security Accounts*
- **Facebook TheatExchange** *Malicious indicators sharing platform*

Blue Team Tips

Learn from Blue Teamers with a collection of Blue Teaming Tips. These tips cover a range of tactics, tools, and methodologies to improve your blue teaming abilities.

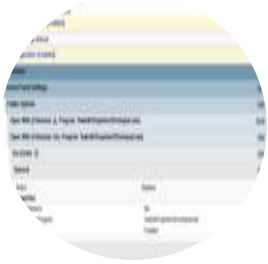
Payload extraction with Process Hacker

Description: *'Malware Analysis Tip - Use Process Hacker to watch for suspicious .NET assemblies in newly spawned processes. Combined with DnSpy - it's possible to locate and extract malicious payloads without needing to manually de-obfuscate.'*

Credit: @embee_research (https://twitter.com/embee_research)

Link: Twitter (https://twitter.com/embee_research/status/1614871485931458560)

Prevent Script Execution via Double Click



Description: *On Windows, it's common to see threat actors achieve initial execution via malicious script files masquerading as Microsoft Office files. A nice way to prevent this attack chain is to alter the default application associated with these files (HTA, JS, VBA, VBS) to* `notepad.exe`*. Now when a user is successfully tricked into clicking a HTA file on disk it will open the script in notepad and execution will not occur.*

Credit: bluesoul (https://bluesoul.me/)

Link: Blog (https://bluesoul.me/2016/05/12/use-gpo-to-change-the-default-behavior-of-potentially-malicious-file-extensions/)

Detect Cryptojacking Malware with Proxy Logs

Description: *Cryptojacking malware is becoming more suffisticated, with mining malware leveraging DLL sideloading to hide on machine and reducing CPU load to stay below detection thresholds. One thing they all have in common is they have to make connections to mining pools, this is where we can find them. Monitor your proxy and DNS logs for connections containing common mining pool strings (e.g* `*xmr.*` *OR* `*pool.com` *OR* `*pool.org` *OR* `pool.*`*).*

Credit: Dave Mckay (https://www.howtogeek.com/author/davidmckay/)

Link: Blog (https://www.howtogeek.com/devops/how-to-detect-and-defeat-cryptominers-in-your-network/)

Network Discovery and Mapping

Tools for scanning and mapping out the network, discovering devices and services, and identifying potential vulnerabilities.

Nmap (https://nmap.org)

Nmap (short for Network Mapper) is a free and open-source network scanner tool used to discover hosts and services on a computer network, and to probe for information about their characteristics.

It can be used to determine which ports on a network are open and what services are running on those ports. Including the ability to identify security vulnerabilities on the network.

Install:

You can download the latest release from here (https://nmap.org/download).

Usage:

```
# Scan a single IP
nmap 192.168.1.1

# Scan a range
nmap 192.168.1.1-254

# Scan targets from a file
nmap -iL targets.txt

# Port scan for port 21
nmap 192.168.1.1 -p 21

# Enables OS detection, version detection, script scanning, and traceroute
nmap 192.168.1.1 -A
```

Nice usage cheat sheet (https://www.stationx.net/nmap-cheat-sheet/).

Image used from https://kirelos.com/nmap-version-scan-determining-the-version-and-available-services/ (https://kirelos.com/nmap-version-scan-determining-the-version-and-available-services/)

Nuclei (https://nuclei.projectdiscovery.io/nuclei/get-started/)

A specialized tool designed to automate the process of detecting vulnerabilities in web applications, networks, and infrastructure.

Nuclei uses pre-defined templates to probe a target and identify potential vulnerabilities. It can be used to test a single host or a range of hosts, and can be configured to run a variety of tests to check for different types of vulnerabilities.

Install:

```
git clone https://github.com/projectdiscovery/nuclei.git; \
cd nuclei/v2/cmd/nuclei; \
go build; \
mv nuclei /usr/local/bin/; \
nuclei -version;
```

Usage:

```
# All the templates gets executed from default template installation path.
nuclei -u https://example.com

# Custom template directory or multiple template directory
nuclei -u https://example.com -t cves/ -t exposures/

# Templates can be executed against list of URLs
nuclei -list http_urls.txt

# Excluding single template
nuclei -list urls.txt -t cves/ -exclude-templates cves/2020/CVE-2020-XXXX.yaml
```

Full usage information can be found here (https://nuclei.projectdiscovery.io/nuclei/get-started/#running-nuclei).

Image used from https://www.appsecsanta.com/nuclei (https://www.appsecsanta.com/nuclei)

Masscan ()

A port scanner that is similar to nmap, but is much faster and can scan a large number of ports in a short amount of time.

Masscan uses a novel technique called "SYN scan" to scan networks, which allows it to scan a large number of ports very quickly.

Install: (Apt)

```
sudo apt install masscan
```

Install: (Git)

```
sudo apt-get install clang git gcc make libpcap-dev
git clone https://github.com/robertdavidgraham/masscan
cd masscan
make
```

Usage:

```
# Scan for a selection of ports (-p22,80,445) across a given subnet (192.168.1.0/24)
masscan -p22,80,445 192.168.1.0/24

# Scan a class B subnet for ports 22 through 25
masscan 10.11.0.0/16 -p22-25

# Scan a class B subnet for the top 100 ports at 100,000 packets per second
masscan 10.11.0.0/16 --top-ports 100 --rate 100000

# Scan a class B subnet, but avoid the ranges in exclude.txt
masscan 10.11.0.0/16 --top-ports 100 --excludefile exclude.txt
```

Image used from https://kalilinuxtutorials.com/masscan/ (https://kalilinuxtutorials.com/masscan/)

Angry IP Scanner (https://angryip.org/)

A free and open-source tool for scanning IP addresses and ports.

It's a cross-platform tool, designed to be fast and easy to use, and can scan an entire network or a range of IP addresses to find live hosts.

Angry IP Scanner can also detect the hostname and MAC address of a device, and can be used to perform basic ping sweeps and port scans.

Install:

You can download the latest release from here (https://angryip.org/download/).

Usage:

Angry IP Scanner can be used via the GUI.

Full usage information and documentation can be found here (https://angryip.org/documentation/).

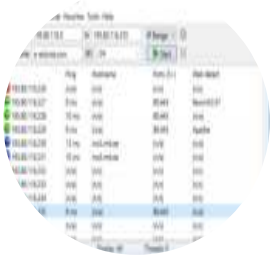


Image used from https://angryip.org/screenshots/ (https://angryip.org/screenshots/)

ZMap (https://github.com/zmap/zmap)

ZMap is a network scanner designed to perform comprehensive scans of the IPv4 address space or large portions of it.

On a typical desktop computer with a gigabit Ethernet connection, ZMap is capable scanning the entire public IPv4 address space in under 45 minutes.

Install:

You can download the latest release from here (https://github.com/zmap/zmap/releases).

Usage:

```
# Scan only 10.0.0.0/8 and 192.168.0.0/16 on TCP/80
zmap -p 80 10.0.0.0/8 192.168.0.0/16
```

Full usage information can be found here (https://github.com/zmap/zmap/wiki).

Image used from https://www.hackers-arise.com/post/zmap-for-scanning-the-internet-scan-the-entire-internet-in-45-minutes (https://www.hackers-arise.com/post/zmap-for-scanning-the-internet-scan-the-entire-internet-in-45-minutes)

Shodan ()

Shodan is a search engine for internet-connected devices.

It crawls the internet for assets, allowing users to search for specific devices and view information about them.

This information can include the device's IP address, the software and version it is running, and the type of device it is.

Install:

The search engine can be accessed at https://www.shodan.io/dashboard (https://www.shodan.io/dashboard).

Usage:

Shodan query fundamentals (https://help.shodan.io/the-basics/search-query-fundamentals)

Shodan query examples (https://www.shodan.io/search/examples)

Nice query cheatsheet (https://www.osintme.com/index.php/2021/01/16/ultimate-osint-with-shodan-100-great-shodan-queries/)

Image used from https://www.shodan.io/ (https://www.shodan.io/)

Vulnerability Management

Tools for identifying, prioritizing, and mitigating vulnerabilities in the network and on individual devices.

OpenVAS (https://openvas.org/)

OpenVAS is an open-source vulnerability scanner that helps identify security vulnerabilities in software and networks.

It is a tool that can be used to perform network security assessments and is often used to identify vulnerabilities in systems and applications so that they can be patched or mitigated.

OpenVAS is developed by the Greenbone Networks company and is available as a free and open-source software application.

Install: (Kali)

```
apt-get update
apt-get dist-upgrade
apt-get install openvas
openvas-setup
```

Usage:

```
openvas-start
```

Visit https://127.0.0.1:9392 (https://127.0.0.1:9392), accept the SSL certificate popup and login with admin credentials:

- username:admin
- password:(*Password in openvas-setup command output*)

Image used from https://www.kali.org/blog/openvas-vulnerability-scanning/ (https://www.kali.org/blog/openvas-vulnerability-scanning/)

Nessus Essentials (https://www.tenable.com/products/nessus/nessus-essentials)

Nessus is a vulnerability scanner that helps identify and assess the vulnerabilities that exist within a network or computer system.

It is a tool that is used to perform security assessments and can be used to identify vulnerabilities in systems and applications so that they can be patched or mitigated.

Nessus is developed by Tenable, Inc. and is available in both free and paid versions:

- The free version, called Nessus Essentials, is available for personal use only and is limited in its capabilities compared to the paid version.
- The paid version, called Nessus Professional, is more fully featured and is intended for use in a professional setting.

Install:

Register for a Nessus Essentials activation code here (https://www.tenable.com/products/nessus/nessus-essentials) and download.

Purchase Nessus Professional from here (https://www.tenable.com/products/nessus/nessus-professional).

Usage:

Extensive documentation can be found here (https://docs.tenable.com/nessus/Content/GetStarted.htm).

Nessus Plugins Search (https://www.tenable.com/plugins/search)

Tenable Community (https://community.tenable.com/)

Image used from https://www.tenable.com (https://www.tenable.com)

Nexpose (https://www.rapid7.com/products/nexpose/)

Nexpose is a vulnerability management tool developed by Rapid7. It is designed to help organizations identify and assess vulnerabilities in their systems and applications in order to mitigate risk and improve security.

Nexpose can be used to scan networks, devices, and applications in order to identify vulnerabilities and provide recommendations for remediation.

It also offers features such as asset discovery, risk prioritization, and integration with other tools in the Rapid7 vulnerability management platform.

Install:

For detailed installation instructions see here (https://docs.rapid7.com/nexpose/install/).

Usage:

For full login information see here (https://docs.rapid7.com/nexpose/log-in-and-activate).

For usage and scan creation instructions see here (https://docs.rapid7.com/nexpose/create-and-scan-a-site).

Image used from https://www.rapid7.com/products/nexpose/ (https://www.rapid7.com/products/nexpose/)

HackerOne (https://www.hackerone.com/)

HackerOne is a bug bounty management company that can be used to create and manage bug bounty programs for your business.

Bug bounty programs are a great way to outsource external vulnerability assessments, with the platform offering both private and public programs with the ability set program scopes and rules of engagement.

HackerOne also offer initial triage and management of external bug reports from researchers, with the ability to compensate researchers directly through the platform.

Image used from https://www.hackerone.com/product/bug-bounty-platform (https://www.hackerone.com/product/bug-bounty-platform)

Security Monitoring

Tools for collecting and analyzing security logs and other data sources to identify potential threats and anomalous activity.

Sysmon (https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon)

Sysmon is a Windows system monitor that tracks system activity and logs it to the Windows event log.

It provides detailed information about system activity, including process creation and termination, network connections, and changes to file creation time.

Sysmon can be configured to monitor specific events or processes and can be used to alert administrators of suspicious activity on a system.

Install:

Download the sysmon binary from here (https://download.sysinternals.com/files/Sysmon.zip).

Usage:

```
# Install with default settings (process images hashed with SHA1 and no network monitoring)
sysmon -accepteula -i

# Install Sysmon with a configuration file (as described below)
sysmon -accepteula -i c:\windows\config.xml

# Uninstall
sysmon -u

# Dump the current configuration
sysmon -c
```

Full event filtering information can be found here (https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon#event-filtering-entries).

The Microsoft documentation page can be found here (https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon).

Image used from https://nsaneforums.com/topic/281207-sysmon-5-brings-registry-modification-logging/ (https://nsaneforums.com/topic/281207-sysmon-5-brings-registry-modification-logging/).

Kibana (https://www.elastic.co/kibana/)

Kibana is an open-source data visualization and exploration tool that is often used for log analysis in combination with Elasticsearch.

Kibana provides a user-friendly interface for searching, visualizing, and analyzing log data, which can be helpful for identifying patterns and trends that may indicate a security threat.

Kibana can be used to analyze a wide range of data sources, including system logs, network logs, and application logs. It can also be used to create custom dashboards and alerts to help security teams stay informed about potential threats and respond quickly to incidents.

Install:

You can download Kibana from here (https://www.elastic.co/downloads/kibana).

Installation instructions can be found here (https://www.elastic.co/guide/en/kibana/current/install.html).

Usage: (Visualize and explore log data)

Kibana provides a range of visualization tools that can help you identify patterns and trends in your log data. You can use these tools to create custom dashboards that display relevant metrics and alerts.

Usage: (Threat Alerting)

Kibana can be configured to send alerts when it detects certain patterns or anomalies in your log data. You can set up alerts to notify you of potential security threats, such as failed login attempts or network connections to known malicious IP addresses.

Nice blog (https://phoenixnap.com/kb/kibana-tutorial) about querying and visualizing data in Kibana.

Image used from https://www.pinterest.co.uk/pin/analysing-honeypot-data-using-kibana-and-elasticsearch--684758318328369269/ (https://www.pinterest.co.uk/pin/analysing-honeypot-data-using-kibana-and-elasticsearch--684758318328369269/)

Logstash (https://www.elastic.co/logstash/)

Logstash is a open-source data collection engine with real-time pipelining capabilities. It is a server-side data processing pipeline that ingests data from a multitude of sources simultaneously, transforms it, and then sends it to a "stash" like Elasticsearch.

Logstash has a rich set of plugins, which allows it to connect to a variety of sources and process the data in multiple ways. It can parse and transform logs, translate data into a structured format, or send it to another tool for further processing.

With its ability to process large volumes of data quickly, Logstash is an integral part of the ELK stack (Elasticsearch, Logstash, and Kibana) and is often used to centralize, transform, and monitor log data.

Install:

Download logstash from here (https://www.elastic.co/downloads/logstash).

Usage:

Full logstash documentation here (https://www.elastic.co/guide/en/logstash/current/introduction.html).

Configuration examples here (https://www.elastic.co/guide/en/logstash/current/config-examples.html).

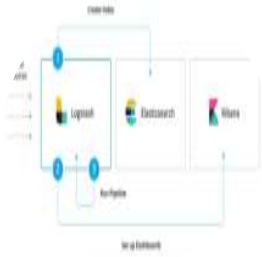


Image used from https://www.elastic.co/guide/en/logstash/current/logstash-modules.html (https://www.elastic.co/guide/en/logstash/current/logstash-modules.html)

parsedmarc (https://github.com/domainaware/parsedmarc)

A Python module and CLI utility for parsing DMARC reports.

When used with Elasticsearch and Kibana (or Splunk), it works as a self-hosted open source alternative to commercial DMARC report processing services such as Agari Brand Protection, Dmarcian, OnDMARC, ProofPoint Email Fraud Defense, and Valimail.

Features:

- Parses draft and 1.0 standard aggregate/rua reports
- Parses forensic/failure/ruf reports
- Can parse reports from an inbox over IMAP, Microsoft Graph, or Gmail API
- Transparently handles gzip or zip compressed reports
- Consistent data structures
- Simple JSON and/or CSV output
- Optionally email the results
- Optionally send the results to Elasticsearch and/or Splunk, for use with premade dashboards
- Optionally send reports to Apache Kafka

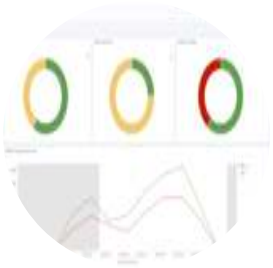


Image used from https://github.com/domainaware/parsedmarc (https://github.com/domainaware/parsedmarc)

Phishing Catcher (https://github.com/x0rz/phishing_catcher)

As a business, phishing can cause reputational and financial damage to you and your customers. Being able to proactively identify phishing infrastructure targeting your business helps to reduce the risk of these damages.

Phish catcher allows you to catch possible phishing domains in near real time by looking for suspicious TLS certificate issuances reported to the Certificate Transparency Log (CTL) via the CertStream API.

"Suspicious" issuances are those whose domain name scores beyond a certain threshold based on a configuration file.

Image used from https://github.com/x0rz/phishing_catcher (https://github.com/x0rz/phishing_catcher)

maltrail (https://github.com/stamparm/maltrail)

Maltrail is a malicious traffic detection system, utilizing publicly available lists containing malicious and/or generally suspicious trails, along with static trails compiled from various AV reports and custom user defined lists. A trail can be anything from domain name, URL, IP address or HTTP User-Agent header value.

A demo page for this tool can be found here (https://maltraildemo.github.io/).

Install:

```
sudo apt-get install git python3 python3-dev python3-pip python-is-python3 libpcap-dev build-essential procps schedtool
sudo pip3 install pcapy-ng
git clone --depth 1 https://github.com/stamparm/maltrail.git
cd maltrail
```

Usage:

```
sudo python3 sensor.py
```

Image used from https://github.com/stamparm/maltrail (https://github.com/stamparm/maltrail)

AutorunsToWinEventLog (https://github.com/palantir/windows-event-forwarding/tree/master/AutorunsToWinEventLog)

Autoruns is a tool developed by Sysinternals that allows you to view all of the locations in Windows where applications can insert themselves to launch at boot or when certain applications are opened. Malware often takes advantages of these locations to ensure that it runs whenever your computer boots up.

Autoruns conveniently includes a non-interactive command line utility. This code generates a CSV of Autoruns entries, converts them to JSON, and finally inserts them into a custom Windows Event Log. By doing this, we can take advantage of our existing WEF infrastructure to get these entries into our SIEM and start looking for signs of malicious persistence on endpoints and servers.

Install:

Download AutorunsToWinEventLog (https://github.com/palantir/windows-event-forwarding/tree/master/AutorunsToWinEventLog).

Usage:

From an Admin Powershell console run `.\Install.ps1`

This script does the following:

- Creates the directory structure at c:\Program Files\AutorunsToWinEventLog
- Copies over AutorunsToWinEventLog.ps1 to that directory
- Downloads Autorunsc64.exe from https://live.sysinternals.com (https://live.sysinternals.com)
- Sets up a scheduled task to run the script daily @ 11am

Image used from https://www.detectionlab.network/usage/autorunstowineventlog/ (https://www.detectionlab.network/usage/autorunstowineventlog/)

procfilter (https://github.com/godaddy/procfilter)

ProcFilter is a process filtering system for Windows with built-in YARA (https://github.com/virustotal/yara) integration. YARA rules can be instrumented with custom meta tags that tailor its response to rule matches. It runs as a Windows service and is integrated with Microsoft's ETW API (https://msdn.microsoft.com/en-us/library/windows/desktop/bb968803%28v=vs.85%29.aspx), making results viewable in the Windows Event Log. Installation, activation, and removal can be done dynamically and does not require a reboot.

ProcFilter's intended use is for malware analysts to be able to create YARA signatures that protect their Windows environments against a specific threat. It does not include a large signature set. Think lightweight, precise, and targeted rather than broad or all-encompassing. ProcFilter is also intended for use in controlled analysis environments where custom plugins can perform artifact-specific actions.

Install:

ProcFilter x86/x64 Release/Debug Installers (https://github.com/godaddy/procfilter/releases)

Note: Unpatched Windows 7 systems require hotfix 3033929 to load the driver component. More information can be found here.

Nice configuration template file here (https://github.com/godaddy/procfilter/blob/master/files/procfilter.ini).

Usage:

```
procfilter -start
```

Usage screenshots can be found here (https://github.com/godaddy/procfilter#screenshots).

Image used from https://github.com/godaddy/procfilter (https://github.com/godaddy/procfilter)

velociraptor (https://github.com/Velocidex/velociraptor)

Velociraptor is a unique, advanced open-source endpoint monitoring, digital forensic and cyber response platform.

It was developed by Digital Forensic and Incident Response (DFIR) professionals who needed a powerful and efficient way to hunt for specific artifacts and monitor activities across fleets of endpoints. Velociraptor provides you with the ability to more effectively respond to a wide range of digital forensic and cyber incident response investigations and data breaches:

Features:

- Reconstruct attacker activities through digital forensic analysis
- Hunt for evidence of sophisticated adversaries
- Investigate malware outbreaks and other suspicious network activities
- Monitory continuously for suspicious user activities, such as files copied to USB devices
- Discover whether disclosure of confidential information occurred outside the network
- Gather endpoint data over time for use in threat hunting and future investigations

Install:

Download the binary from the release page (https://github.com/Velocidex/velociraptor/releases).

Usage:

```
velociraptor gui
```

Full usage information can be found here (https://docs.velociraptor.app/).

Image used from https://docs.velociraptor.app (https://docs.velociraptor.app)

SysmonSearch (https://github.com/JPCERTCC/SysmonSearch)

SysmonSearch makes event log analysis more effective and less time consuming, by aggregating event logs generated by Microsoft's Sysmon.

SysmonSearch uses Elasticserach and Kibana (and Kibana plugin).

- **Elasticserach**
  Elasticsearch collects/stores Sysmon's event log.
- **Kibana**
  Kibana provides user interface for your Sysmon's event log analysis. The following functions are implemented as Kibana plugin.
  - Visualizes Function
    This function visualizes Sysmon's event logs to illustrate correlation of processes and networks.
  - Statistical Function
    This function collects the statistics of each device or Sysmon's event ID.
  - Monitor Function
    This function monitor incoming logs based on the preconfigured rules, and trigers alert.
- **StixIoC server**
  You can add search/monitor condition by uploading STIX/IOC file. From StixIoC server Web UI, you can upload STIXv1, STIXv2 and OpenIOC format files.

Install: (Linux)

```
git clone https://github.com/JPCERTCC/SysmonSearch.git
```

Modify Elasticsearch configuration (https://github.com/JPCERTCC/SysmonSearch/wiki/Install#elasticsearch-server-setup)

Modify Kibana configuration (https://github.com/JPCERTCC/SysmonSearch/wiki/Install#kibana-server-setup)

Full installation instructions can be found here (https://github.com/JPCERTCC/SysmonSearch/wiki/Install).

Usage:

Once Elasticsearch and Kibana configurations have been modified, restart the services and navigate to your Kibana interface. The SysmonSearch ribbon should be visible.

Visualize the Sysmon log to investigate suspicious behavior (https://blogs.jpcert.or.jp/ja/2018/09/SysmonSearch.html)

Image used from https://blogs.jpcert.or.jp/ja/2018/09/SysmonSearch.html (https://blogs.jpcert.or.jp/ja/2018/09/SysmonSearch.html)

Threat Tools and Techniques

Tools for identifying and implementing detections against TTPs used by threat actors.

lolbas-project.github.io (https://lolbas-project.github.io/)

Living off the land binaries (LOLBins) are legitimate Windows executables that can be used by threat actors to carry out malicious activities without raising suspicion.

Using LOLBins allows attackers to blend in with normal system activity and evade detection, making them a popular choice for malicious actors.

The LOLBAS project is a MITRE mapped list of LOLBINS with commands, usage and detection information for defenders.

Visit https://lolbas-project.github.io/ (https://lolbas-project.github.io/).

Usage:

Use the information for detection opportunities to harden your infrastructure against LOLBIN usage.

Here are some project links to get started:

- Bitsadmin.exe (https://lolbas-project.github.io/lolbas/Binaries/Bitsadmin/)
- Certutil.exe (https://lolbas-project.github.io/lolbas/Binaries/Certutil/)
- Cscript.exe (https://lolbas-project.github.io/lolbas/Binaries/Cscript/)

Image used from https://lolbas-project.github.io/ (https://lolbas-project.github.io/)

gtfobins.github.io (https://gtfobins.github.io/)

GTFOBins (short for "Get The F* Out Binaries") is a collection of Unix binaries that can be used to escalate privileges, bypass restrictions, or execute arbitrary commands on a system.

They can be used by threat actors to gain unauthorized access to systems and carry out malicious activities.

The GTFOBins project is a list of Unix binaries with command and usage information for attackers. This information can be used to implement unix detections.

Visit https://gtfobins.github.io/ (https://gtfobins.github.io/).

Usage:

Here are some project links to get started:

- base64 (https://gtfobins.github.io/gtfobins/base64/)
- curl (https://gtfobins.github.io/gtfobins/curl/)
- nano (https://gtfobins.github.io/gtfobins/nano/)

Image used from https://gtfobins.github.io/ (https://gtfobins.github.io/)

filesec.io (https://filesec.io/)

Filesec is a list of file extensions that can be used by attackers for phishing, execution, macros etc.

This is a nice resource to understand the malicious use cases of common file extentions and ways that you can defend against them.

Each file extension page contains a description, related operating system and recommendations.

Visit https://filesec.io/ (https://filesec.io/).

Usage:

Here are some project links to get started:

- .Docm (https://filesec.io/docm)
- .Iso (https://filesec.io/iso)
- .Ppam (https://filesec.io/ppam)

Image used from https://filesec.io/ (https://filesec.io/)

KQL Search (https://www.kqlsearch.com/)

KQL stands for "Kusto Query Language", and it is a query language used to search and filter data in Azure Monitor logs. It is similar to SQL, but is more optimized for log analytics and time-series data.

KQL query language is particularly useful for blue teamers because it allows you to quickly and easily search through large volumes of log data to identify security events and anomalies that may indicate a threat.

KQL Search is a web app created by @ugurkocde (https://twitter.com/ugurkocde) that aggregates KQL queries that are shared on GitHub.

You can visit the site at https://www.kqlsearch.com/ (https://www.kqlsearch.com/).

More information about Kusto Query Language (KQL) can be found here (https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/).

Image used from https://www.kqlsearch.com/ (https://www.kqlsearch.com/)

Unprotect Project (https://unprotect.it/about/)

Malware authors spend a great deal of time and effort to develop complex code to perform malicious actions against a target system. It is crucial for malware to remain undetected and avoid sandbox analysis, antiviruses or malware analysts.

With this kind of technics, malware are able to pass under the radar and stay undetected on a system. The goal of this free database is to centralize the information about malware evasion techniques.

The project aims to provide Malware Analysts and Defenders with actionable insights and detection capabilities to shorten their response times.

The project can be found at https://unprotect.it/ (https://unprotect.it/).

The project has an API - Docs here (https://unprotect.it/api/).

Image used from https://unprotect.it/map/ (https://unprotect.it/map/)

chainsaw (https://github.com/WithSecureLabs/chainsaw)

Chainsaw provides a powerful 'first-response' capability to quickly identify threats within Windows forensic artefacts such as Event Logs and MFTs. Chainsaw offers a generic and fast method of searching through event logs for keywords, and by identifying threats using built-in support for Sigma detection rules, and via custom Chainsaw detection rules.

Features:

- Hunt for threats using Sigma detection rules and custom Chainsaw detection rules
- Search and extract forensic artefacts by string matching, and regex patterns
- Lightning fast, written in rust, wrapping the EVTX parser library by @OBenamram
- Clean and lightweight execution and output formats without unnecessary bloat
- Document tagging (detection logic matching) provided by the TAU Engine Library
- Output results in a variety of formats, such as ASCII table format, CSV format, and JSON format
- Can be run on MacOS, Linux and Windows

Install:

```
git clone https://github.com/countercept/chainsaw.git
cargo build --release
git clone https://github.com/SigmaHQ/sigma
git clone https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES.git
```

Usage:

```
./chainsaw hunt EVTX-ATTACK-SAMPLES/ -s sigma/ --mapping mappings/sigma-event-logs-all.yml
```

Image used from https://twitter.com/FranticTyping/status/1433386064429916162/ (https://twitter.com/FranticTyping/status/1433386064429916162/)

freq (https://github.com/MarkBaggett/freq)

Adversaries attempt to bypass signature based/pattern matching/blacklist techniques by introducing random: filenames, service names, workstation names, domains, hostnames, SSL cert subjects and issuer subjects, etc.

Freq is a python API designed by Mark Baggett to handle mass entropy testing. It was designed to be used in conjunction with a SIEM solutions but can work with anything that can submit a web request.

The tool uses frequency tables that map how likely one character will follow another

Install:

```
git clone https://github.com/MarkBaggett/freq
cd freq
```

Usage:

```
# Running freq_server.py on port 10004 and using a frequency table of /opt/freq/dns.freq
/usr/bin/python /opt/freq/freq_server.py 10004 /opt/freq/dns.freq
```

□yarGen (https://github.com/Neo23x0/yarGen)

yarGen is a generator for YARA rules

The main principle is the creation of yara rules from strings found in malware files while removing all strings that also appear in goodware files. Therefore yarGen includes a big goodware strings and opcode database as ZIP archives that have to be extracted before the first use.

The rule generation process also tries to identify similarities between the files that get analyzed and then combines the strings to so called super rules. The super rule generation does not remove the simple rule for the files that have been combined in a single super rule. This means that there is some redundancy when super rules are created. You can suppress a simple rule for a file that was already covered by super rule by using --nosimple.

Install:

Download the latest release (https://github.com/Neo23x0/yarGen/releases).

```
pip install -r requirements.txt
python yarGen.py --update
```

Usage:

```
# Create a new strings and opcodes database from an Office 2013 program directory
yarGen.py -c --opcodes -i office -g /opt/packs/office2013

# Update the once created databases with the "-u" parameter
yarGen.py -u --opcodes -i office -g /opt/packs/office365
```

Usage examples can be found here (https://github.com/Neo23x0/yarGen#examples).

Image used from https://github.com/Neo23x0/yarGen (https://github.com/Neo23x0/yarGen)

□EmailAnalyzer (https://github.com/keraattin/EmailAnalyzer)

With EmailAnalyzer you can able to analyze your suspicious emails. You can extract headers, links and hashes from the .eml file

Install:

```
git clone https://github.com/keraattin/EmailAnalyzer
cd EmailAnalyzer
```

Usage:

```
# View headers in eml file
python3 email-analyzer.py -f <eml file> --headers

# Get hashes
python3 email-analyzer.py -f <eml file> --digests

# Get links
python3 email-analyzer.py -f <eml file> --links

# Get attachments
python3 email-analyzer.py -f <eml file> --attachments
```

Text used from https://github.com/keraattin/EmailAnalyzer (https://github.com/keraattin/EmailAnalyzer)

VCG (https://github.com/nccgroup/VCG)

VCG is an automated code security review tool that handles C/C++, Java, C#, VB and PL/SQL. It has a few features that should hopefully make it useful to anyone conducting code security reviews, particularly where time is at a premium:

- In addition to performing some more complex checks it also has a config file for each language that basically allows you to add any bad functions (or other text) that you want to search for
- It attempts to find a range of around 20 phrases within comments that can indicate broken code (“ToDo”, “FixMe”, “Kludge”, etc.)
- It provides a nice pie chart (for the entire codebase and for individual files) showing relative proportions of code, whitespace, comments, ‘ToDo’ style comments and bad code

Install:

You can install the pre-compiled binary here.

Open the project .sln, choose "Release", and build.

Usage:

```
STARTUP OPTIONS:
        (Set desired starting point for GUI. If using console mode these options will set target(s) to be scanned.)
        -t, --target <Filename|DirectoryName>:  Set target file or directory. Use this option either to load target immediately into
        -l, --language <CPP|PLSQL|JAVA|CS|VB|PHP|COBOL>:        Set target language (Default is C/C++).
        -e, --extensions <ext1|ext2|ext3>:      Set file extensions to be analysed (See ReadMe or Options screen for language-specif
        -i, --import <Filename>:        Import XML/CSV results to GUI.

OUTPUT OPTIONS:
        (Automagically export results to a file in the specified format. Use XML or CSV output if you wish to reload results into th
        -x, --export <Filename>:        Automatically export results to XML file.
        -f, --csv-export <Filename>:    Automatically export results to CSV file.
        -r, --results <Filename>:       Automatically export results to flat text file.

CONSOLE OPTIONS:
        -c, --console:          Run application in console only (hide GUI).
        -v, --verbose:          Set console output to verbose mode.
        -h, --help:             Show help.
```

Threat Intelligence

Tools for gathering and analyzing intelligence about current and emerging threats, and for generating alerts about potential threats.

Maltego (https://www.maltego.com/solutions/cyber-threat-intelligence/)

Maltego is a commercial threat intelligence and forensics tool developed by Paterva. It is used by security professionals to gather and analyze information about domains, IP addresses, networks, and individuals in order to identify relationships and connections that might not be immediately apparent.

Maltego uses a visual interface to represent data as entities, which can be linked together to form a network of relationships. It includes a range of transforms, which are scripts that can be used to gather data from various sources, such as social media, DNS records, and WHOIS data.

Maltego is often used in conjunction with other security tools, such as SIEMs and vulnerability scanners, as part of a comprehensive threat intelligence and incident response strategy.

You can schedule a demo here (https://www.maltego.com/get-a-demo/).

Maltego handbook Handbook for Cyber Threat Intelligence (https://static.maltego.com/cdn/Handbooks/Maltego-Handbook-for-Cyber-Threat-Intelligence.pdf)

Image used from https://www.maltego.com/reduce-your-cyber-security-risk-with-maltego/ (https://www.maltego.com/reduce-your-cyber-security-risk-with-maltego/)

MISP (https://www.misp-project.org/)

MISP (short for Malware Information Sharing Platform) is an open-source platform for sharing, storing, and correlating Indicators of Compromise (IOCs) of targeted attacks, threats, and malicious activity.

MISP includes a range of features, such as real-time sharing of IOCs, support for multiple formats, and the ability to import and export data to and from other tools.

It also provides a RESTful API and various data models to facilitate the integration of MISP with other security systems. In addition to its use as a threat intelligence platform, MISP is also used for incident response, forensic analysis, and malware research.

Install:

```
# Kali
wget -O /tmp/misp-kali.sh https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh && bash /tmp/misp-kali.sh

# Ubuntu 20.04.2.0-server
wget -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh
bash /tmp/INSTALL.sh
```

Full installation instructions can be found here (https://misp.github.io/MISP/).

Usage:

MISP documentation can be found here (https://www.misp-project.org/documentation/).

MISP user guide (https://github.com/MISP/misp-book)

MISP Training Cheat sheet (https://www.misp-project.org/misp-training/cheatsheet.pdf)

Image used from http://www.concordia-h2020.eu/blog-post/integration-of-misp-into-flowmon-ads/ (http://www.concordia-h2020.eu/blog-post/integration-of-misp-into-flowmon-ads/)

ThreatConnect (https://threatconnect.com/threat-intelligence-platform/)

ThreatConnect is a threat intelligence platform that helps organizations aggregate, analyze, and act on threat data. It is designed to provide a single, unified view of an organization's threat landscape and enable users to collaborate and share information about threats.

The platform includes a range of features for collecting, analyzing, and disseminating threat intelligence, such as a customizable dashboard, integration with third-party data sources, and the ability to create custom reports and alerts.

It is intended to help organizations improve their security posture by providing them with the information they need to identify, prioritize, and respond to potential threats.

You can request a demo from here (https://threatconnect.com/request-a-demo/).

ThreatConnect for Threat Intel Analysts - PDF (https://threatconnect.com/wp-content/uploads/2022/12/Intel-Analysts-Datasheet.pdf)

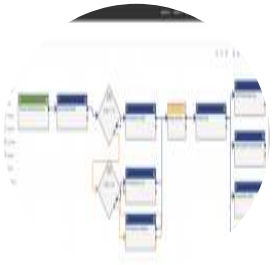


Image used from https://threatconnect.com/threat-intelligence-platform/ (https://threatconnect.com/threat-intelligence-platform/)

Incident Response Planning

Tools for creating and maintaining an incident response plan, including templates and best practices for responding to different types of incidents.

NIST (https://www.nist.gov/cyberframework)

The NIST Cybersecurity Framework (CSF) is a framework developed by the National Institute of Standards and Technology (NIST) to help organizations manage cybersecurity risks. It provides a set of guidelines, best practices, and standards for implementing and maintaining a robust cybersecurity program.

The framework is organized around five core functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a structure for understanding and addressing the various components of cybersecurity risk.

The CSF is designed to be flexible and adaptable, and it can be customized to fit the specific needs and goals of an organization. It is intended to be used as a tool for improving an organization's cybersecurity posture and for helping organizations better understand and manage their cybersecurity risks.

Useful Links:

NIST Quickstart Guide (https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide)

Framework for Improving Critical Infrastructure Cybersecurity (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)

Data Breach Response: A Guide for Business (https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business)

NIST Events and Presentations (https://www.nist.gov/cyberframework/events-and-presentations)

Twitter - @NISTcyber (https://www.twitter.com/NISTcyber)

Image used from https://www.dell.com/en-us/blog/strengthen-security-of-your-data-center-with-the-nist-cybersecurity-framework/ (https://www.dell.com/en-us/blog/strengthen-security-of-your-data-center-with-the-nist-cybersecurity-framework/)

Incident Response Plan

An incident response plan is a set of procedures that a company puts in place to manage and mitigate the impact of a security incident, such as a data breach or a cyber attack.

The theory behind an incident response plan is that it helps a company to be prepared for and respond effectively to a security incident, which can minimize the damage and reduce the chances of it happening again in the future.

There are several reasons why businesses need an incident response plan:

1. **To minimize the impact of a security incident:** An incident response plan helps a company to identify and address the source of a security incident as quickly as possible, which can help to minimize the damage and reduce the chances of it spreading.
2. **To meet regulatory requirements:** Many industries have regulations that require companies to have an incident response plan in place. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires merchants and other organizations that accept credit cards to have an incident response plan.
3. **To protect reputation:** A security incident can damage a company's reputation, which can lead to a loss of customers and revenue. An incident response plan can help a company to manage the situation and minimize the damage to its reputation.
4. **To reduce the cost of a security incident:** The cost of a security incident can be significant, including the cost of remediation, legal fees, and lost business. An incident response plan can help a company to minimize these costs by providing a roadmap for responding to the incident.

Useful Links:

National Cyber Security Centre - Incident Response overview (https://www.ncsc.gov.uk/collection/incident-management/incident-response)

SANS - Security Policy Templates (https://www.sans.org/information-security-policy/)

SANS - Incident Handler's Handbook (https://www.sans.org/white-papers/33901/)

FRSecure - Incident Response Plan Template (https://frsecure.com/incident-response-plan-template/)

Cybersecurity and Infrastructure Security Agency - CYBER INCIDENT RESPONSE (https://www.cisa.gov/cyber-incident-response)

FBI - Incident Response Policy (https://www.fbi.gov/file-repository/incident-response-policy.pdf/view)

Image used from https://www.ncsc.gov.uk/collection/incident-management/incident-response (https://www.ncsc.gov.uk/collection/incident-management/incident-response)

Ransomware Response Plan

Ransomware is a type of malicious software that encrypts a victim's files. The attackers then demand a ransom from the victim to restore access to the files; hence the name ransomware.

The theory behind a ransomware response plan is that it helps a company to be prepared for and respond effectively to a ransomware attack, which can minimize the impact of the attack and reduce the chances of it happening again in the future.

There are several reasons why businesses need a ransomware response plan:

1. **To minimize the impact of a ransomware attack:** A ransomware response plan helps a company to identify and address a ransomware attack as quickly as possible, which can help to minimize the damage and reduce the chances of the ransomware spreading to other systems.
2. **To protect against data loss:** Ransomware attacks can result in the loss of important data, which can be costly and disruptive for a business. A ransomware response plan can help a company to recover from an attack and avoid data loss.
3. **To protect reputation:** A ransomware attack can damage a company's reputation, which can lead to a loss of customers and revenue. A ransomware response plan can help a company to manage the situation and minimize the damage to its reputation.
4. **To reduce the cost of a ransomware attack:** The cost of a ransomware attack can be significant, including the cost of remediation, legal fees, and lost business. A ransomware response plan can help a company to minimize these costs by providing a roadmap for responding to the attack.

Useful Links:

National Cyber Security Centre - Mitigating malware and ransomware attacks (https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks)

NIST - Ransomware Protection and Response (https://csrc.nist.gov/Projects/ransomware-protection-and-response)

Cybersecurity and Infrastructure Security Agency - Ransomware Guide (https://www.cisa.gov/stopransomware/ransomware-guide)

Microsoft Security - Ransomware response (https://www.microsoft.com/en-us/security/blog/2019/12/16/ransomware-response-to-pay-or-not-to-pay/)

Blog - Creating a Ransomware Response Plan (https://www.msp360.com/resources/blog/designing-a-ransomware-response-plan/)

Image used from https://csrc.nist.gov/Projects/ransomware-protection-and-response (https://csrc.nist.gov/Projects/ransomware-protection-and-response)

Malware Detection and Analysis

Tools for detecting and analyzing malware, including antivirus software and forensic analysis tools.

VirusTotal (https://www.virustotal.com/gui/home/search)

VirusTotal is a website and cloud-based tool that analyzes and scans files, URLs, and software for viruses, worms, and other types of malware.

When a file, URL, or software is submitted to VirusTotal, the tool uses various antivirus engines and other tools to scan and analyze it for malware. It then provides a report with the results of the analysis, which can help security professionals and blue teams identify and respond to potential threats.

VirusTotal can also be used to check the reputation of a file or URL, and to monitor for malicious activity on a network.

Visit https://www.virustotal.com/gui/home/search (https://www.virustotal.com/gui/home/search)

Usage:

```
# Recently created documents with macros embedded, detected at least by 5 AVs
(type:doc OR type: docx) tag:macros p:5+ generated:30d+

# Excel files bundled with powershell scripts and uploaded to VT for the last 10
days
(type:xls OR type:xlsx) tag:powershell fs:10d+

# Follina-like exploit payloads
entity:file magic:"HTML document text" tag:powershell have:itw_url

# URLs related to specified parent domain/subdomain with a specific header in
the response
entity:url header_value:"Apache/2.4.41 (Ubuntu)" parent_domain:domain.org

# Suspicious URLs with a specific HTML title
entity:url ( title:"XY Company" or title:"X.Y. Company" or title:"XYCompany" ) p:5+
```

Full documentation can be found here (https://support.virustotal.com/hc/en-us/categories/360000162878-Documentation).

VT INTELLIGENCE CHEAT SHEET (https://storage.googleapis.com/vtpublic/reports/VTI%20Cheatsheet.pdf)

Image used from https://www.virustotal.com/gui/home/search (https://www.virustotal.com/gui/home/search)

IDA (https://hex-rays.com/ida-free/)

IDA (Interactive Disassembler) is a powerful tool used to reverse engineer and analyze compiled and executable code.

It can be used to examine the inner workings of software, including malware, and to understand how it functions. IDA allows users to disassemble code, decompile it into a higher-level programming language, and view and edit the resulting source code. This can be useful for identifying vulnerabilities, analyzing malware, and understanding how a program works.

IDA can also be used to generate graphs and charts that visualize the structure and flow of code, which can make it easier to understand and analyze.

Install:

Download IDA from here (https://hex-rays.com/ida-free/#download).

Usage:

IDA Practical Cheatsheet (https://github.com/AdamTaguirov/IDA-practical-cheatsheet)

IDAPython cheatsheet (https://gist.github.com/icecr4ck/7a7af3277787c794c66965517199fc9c)

IDA Pro Cheatsheet (https://hex-rays.com/products/ida/support/freefiles/IDA_Pro_Shortcuts.pdf)

Image used from https://www.newton.com.tw/wiki/IDA%20Pro (https://www.newton.com.tw/wiki/IDA%20Pro)

Ghidra (https://ghidra-sre.org/)

Ghidra is a free, open-source software reverse engineering tool developed by the National Security Agency (NSA). It is used to analyze compiled and executable code, including malware.

Ghidra allows users to disassemble code, decompile it into a higher-level programming language, and view and edit the resulting source code. This can be useful for identifying vulnerabilities, analyzing malware, and understanding how a program works.

Ghidra also includes a range of features and tools that support SRE tasks, such as debugging, code graphing, and data visualization. Ghidra is written in Java and is available for Windows, MacOS, and Linux.

Install:

1. Download the latest release from here (https://github.com/NationalSecurityAgency/ghidra/releases).
2. Extract the zip

Full installation and error fix information can be found here (https://ghidra-sre.org/InstallationGuide.html#Install).

Usage:

1. Navigate to the unzipped folder

```
# Windows
ghidraRun.bat

# Linux
./ghidraRun
```

If Ghidra failed to launch, see the Troubleshooting (https://ghidra-sre.org/InstallationGuide.html#Troubleshooting) link.

Image used from https://www.malwaretech.com/2019/03/video-first-look-at-ghidra-nsa-reverse-engineering-tool.html (https://www.malwaretech.com/2019/03/video-first-look-at-ghidra-nsa-reverse-engineering-tool.html)

Data Recovery

Tools for recovering data from damaged or corrupted systems and devices.

Recuva (https://www.ccleaner.com/recuva)

Recuva is a data recovery tool that can be used to recover deleted files from your computer.

It is often used to recover deleted files that may contain valuable information, such as deleted logs or documents that could be used to investigate a security incident.

Recuva can recover files from hard drives, USB drives, and memory cards, and it is available for Windows and Mac operating systems.

Install:

You can download the tool from here (https://www.ccleaner.com/recuva).

Usage:

Nice step by step guide (https://toolbox.iskysoft.com/data-recovery-tips/recuva-windows-10.html).

Image used from https://www.softpedia.com/blog/recuva-explained-usage-video-and-download-503681.shtml (https://www.softpedia.com/blog/recuva-explained-usage-video-and-download-503681.shtml)

Extundelete (https://extundelete.sourceforge.net/)

Extundelete is a utility that can be used to recover deleted files from an ext3 or ext4 file system.

It works by searching the file system for blocks of data that used to belong to a file, and then attempting to recreate the file using those blocks of data. It is often used to recover important files that have been accidentally or maliciously deleted.

Install:

You can download the tool from here (https://sourceforge.net/project/platformdownload.php?group_id=260221).

Usage:

```
# Prints information about the filesystem from the superblock.
--superblock

# Attemps to restore the file which was deleted at the given filename, called as "--restore-file dirname/filename".
--restore-file path/to/deleted/file

# Restores all files possible to undelete to their names before deletion, when possible. Other files are restored to a filename like
--restore-all
```

Full usage information can be found here (https://extundelete.sourceforge.net/options.html).

Image used from https://theevilbit.blogspot.com/2013/01/backtrack-forensics-ext34-file-recovery.html (https://theevilbit.blogspot.com/2013/01/backtrack-forensics-ext34-file-recovery.html).

TestDisk (https://www.cgsecurity.org/wiki/TestDisk_Download)

TestDisk is a free and open-source data recovery software tool that is designed to help recover lost partitions and make non-booting disks bootable again. It is useful for both computer forensics and data recovery.

It can be used to recover data that has been lost due to a variety of reasons, such as accidental deletion, formatting, or corruption of the partition table.

TestDisk can also be used to repair damaged boot sectors, recover deleted partitions, and recover lost files. It supports a wide range of file systems, including FAT, NTFS, and ext2/3/4, and can be used to recover data from disks that are damaged or formatted with a different file system than the one they were originally created with.

Install:

You can download the tool from here (https://www.cgsecurity.org/wiki/TestDisk_Download).

Usage:

Full usage examples here (https://www.cgsecurity.org/wiki/Data_Recovery_Examples).

Step by step guide (https://www.cgsecurity.org/wiki/TestDisk_Step_By_Step)

TestDisk Documentation PDF - 60 Pages (https://www.cgsecurity.org/testdisk.pdf)

Image used from https://www.cgsecurity.org/wiki/ (https://www.cgsecurity.org/wiki/)

Digital Forensics

Tools for conducting forensic investigations of digital devices and systems, including tools for collecting and analyzing evidence.

SANS SIFT (https://www.sans.org/tools/sift-workstation/)

SANS SIFT (SANS Investigative Forensic Toolkit) is a powerful toolkit for forensic analysis and incident response.

It is a collection of open source and commercial tools that can be used to perform forensic analysis on a wide range of systems, including Windows, Linux, and Mac OS X. The SANS SIFT kit is designed to be run on a forensic workstation, which is a specialized computer that is used to perform forensic analysis on digital evidence.

The SANS SIFT kit is particularly useful for blue teamers, as it provides a wide range of tools and resources that can be used to investigate incidents, respond to threats, and perform forensic analysis on compromised systems.

Install:

1. Visit https://www.sans.org/tools/sift-workstation/ (https://www.sans.org/tools/sift-workstation/).
2. Click the 'Login to Download' button and input (or create) your SANS Portal account credentials to download the virtual machine.
3. Once you have booted the virtual machine, use the credentials below to gain access.

```
Login = sansforensics
Password = forensics
```

Note: *Use to elevate privileges to root while mounting disk images.*

Additional install options here (https://www.sans.org/tools/sift-workstation/).

Usage:

```
# Registry Parsing - Regripper
rip.pl -r <HIVEFILE> -f <HIVETYPE>

# Recover deleted registry keys
deleted.pl <HIVEFILE>

# Mount E01 Images
ewfmount image.E01 mountpoint
mount -o

# Stream Extraction
bulk_extractor <options> -o output_dir
```

Full usage guide here (https://www.sans.org/posters/sift-cheat-sheet/).

Image used from https://securityboulevard.com/2020/08/how-to-install-sift-workstation-and-remnux-on-the-same-system-for-forensics-and-malware-analysis/ (https://securityboulevard.com/2020/08/how-to-install-sift-workstation-and-remnux-on-the-same-system-for-forensics-and-malware-analysis/)

The Sleuth Kit (https://sleuthkit.org/sleuthkit/)

The Sleuth Kit is a collection of command line tools that can be used to analyze disk images and recover files from them.

It is primarily used by forensic investigators to examine digital evidence after a computer has been seized or an image of a disk has been made. It can be useful because it can help understand what happened during a security incident and identify any malicious activity.

The tools in The Sleuth Kit can be used to extract deleted files, analyze disk partition structures, and examine the file system for evidence of tampering or unusual activity.

Install:

Download tool from here (https://sleuthkit.org/sleuthkit/download.php).

Usage:

Link to documentation (https://sleuthkit.org/sleuthkit/docs.php).

Image used from http://www.effecthacking.com/2016/09/the-sleuth-kit-digital-forensic-tool.html (http://www.effecthacking.com/2016/09/the-sleuth-kit-digital-forensic-tool.html)

Autopsy (https://www.autopsy.com/)

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools.

It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can use it to analyze disk images and recover files, as well as to identify system and user activity.

Autopsy is used by "blue teams" (the cybersecurity professionals who defend organizations against attacks) to conduct forensic analysis and incident response. It can help blue teams understand the nature and scope of an attack, and identify any malicious activity that may have occurred on a computer or network.

Install:

Download the tool from here (https://www.autopsy.com/download/).

Usage:

Autopsy User Guide (http://sleuthkit.org/autopsy/docs/user-docs/4.19.3//)

SANS - Introduction to using the AUTOPSY Forensic Browser (https://www.sans.org/blog/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser/)

Image used from https://www.kitploit.com/2014/01/autopsy-digital-investigation-analysis.html (https://www.kitploit.com/2014/01/autopsy-digital-investigation-analysis.html)

Security Awareness Training

Tools for training employees and other users on how to recognize and prevent potential security threats.

TryHackMe (https://tryhackme.com/dashboard)

TryHackMe is a platform that offers a variety of virtual machines, known as "rooms," which are designed to teach cybersecurity concepts and skills through hands-on learning.

These rooms are interactive and gamified, allowing users to learn about topics such as web vulnerabilities, network security, and cryptography by solving challenges and completing tasks.

The platform is often used for security awareness training, as it provides a safe and controlled environment for users to practice their skills and learn about different types of cyber threats and how to defend against them.

Visit https://tryhackme.com/ (https://tryhackme.com/) and create an account.

TryHackMe - Getting Started Guide (https://docs.tryhackme.com/docs/teaching/teaching-getting-started/)

Useful links:

Pre-Security Learning Path (https://tryhackme.com/path-action/presecurity/join)

introduction to Cyber Security Learning Path (https://tryhackme.com/path-action/introtocyber/join)

Visit the hacktivities (https://tryhackme.com/hacktivities) tab for a full list of available rooms and modules.

Image used from https://www.hostingadvice.com/blog/learn-cybersecurity-with-tryhackme/ (https://www.hostingadvice.com/blog/learn-cybersecurity-with-tryhackme/)

HackTheBox (https://www.hackthebox.com/)

HackTheBox is a platform for practicing and improving your hacking skills.

It consists of a set of challenges that simulate real-world scenarios and require you to use your knowledge of various hacking techniques to solve them. These challenges are designed to test your knowledge of topics such as network security, cryptography, web security, and more.

HackTheBox is often used by security professionals as a way to practice and improve their skills, and it can also be a useful resource for security awareness training. By working through the challenges and learning how to solve them, individuals can gain a better understanding of how to identify and mitigate common security threats.

Visit https://app.hackthebox.com/login (https://app.hackthebox.com/login) and create an account.

Useful links:

Blog - Introduction to Hack The Box (https://help.hackthebox.com/en/articles/5185158-introduction-to-hack-the-box)

Blog - Learn to Hack with Hack The Box: The Beginner's Bible (https://www.hackthebox.com/blog/learn-to-hack-beginners-bible)

Blog - Introduction to Starting Point (https://help.hackthebox.com/en/articles/6007919-introduction-to-starting-point)

Image used from https://www.hackthebox.com/login (https://www.hackthebox.com/login)

PhishMe (https://cofense.com/product-services/phishme/)

PhishMe is a company that provides security awareness training to help organizations educate their employees about how to identify and prevent phishing attacks.

PhishMe's training programs aim to teach employees how to recognize and report phishing attempts, as well as how to protect their personal and professional accounts from these types of attacks.

The company's training programs can be customized to fit the needs of different organizations and can be delivered through a variety of mediums, including online courses, in-person training, and simulations.

Request a demo from here (https://go.cofense.com/live-demo/).

Useful links:

Cofense Blog (https://cofense.com/blog/)

Cofense Knowledge Center (https://cofense.com/knowledge-center-hub/)

Image used from https://cofense.com/product-services/phishme/ (https://cofense.com/product-services/phishme/)

Communication and Collaboration

Tools for coordinating and communicating with team members during an incident, including chat, email, and project management software.

Twitter (https://twitter.com/)

Twitter is a great platform for sharing information about cyber security.

It's a platform that is widely used by security professionals, researchers, and experts, giving you access to an endless amount of new information.

Some great accounts to follow:

- @vxunderground (https://twitter.com/vxunderground)
- @Alh4zr3d (https://twitter.com/Alh4zr3d)
- @3xp0rtblog (https://twitter.com/3xp0rtblog)
- @C5pider (https://twitter.com/C5pider)
- @_JohnHammond (https://twitter.com/_JohnHammond)
- @mrd0x (https://twitter.com/mrd0x)
- @TheHackersNews (https://twitter.com/TheHackersNews)
- @pancak3stack (https://twitter.com/pancak3stack)
- @GossiTheDog (https://twitter.com/GossiTheDog)
- @briankrebs (https://twitter.com/briankrebs)
- @SwiftOnSecurity (https://twitter.com/SwiftOnSecurity)
- @schneierblog (https://twitter.com/schneierblog)
- @mikko (https://twitter.com/mikko)
- @campuscodi (https://twitter.com/campuscodi)

Facebook TheatExchange (https://developers.facebook.com/docs/threat-exchange/getting-started)

Facebook ThreatExchange is a platform for security professionals to share and analyze information about cyber threats.

It was designed to help organizations better defend against threats by allowing them to share threat intelligence with each other in a private and secure way.

It is intended to be used by "blue teams", who are responsible for the security of an organization and work to prevent, detect, and respond to cyber threats.

Usage:

To request access to ThreatExchange, you have to submit an application via https://developers.facebook.com/products/threat-exchange/ (https://developers.facebook.com/products/threat-exchange/).

Useful links:

Welcome to ThreatExchange! (https://developers.facebook.com/docs/threat-exchange/getting-started)

ThreatExchange UI Overview (https://developers.facebook.com/docs/threat-exchange/ui)

ThreatExchange API Reference (https://developers.facebook.com/docs/threat-exchange/reference/apis)

GitHub - ThreatExchange (https://github.com/facebook/ThreatExchange/tree/main/python-threatexchange)