

Blue Team

LaBrea.py
 ShowMeThePackets
 VisualSniff
 DeepBlueCLI
 "WhatsMyName"
 untappdScraper
 Espial
 flare
 VulnWhisperer
 Log Campaign
 Update-VMs
 QRadar Threat
 Intelligence
 DNSSpoof
 Misc
 Freq Server
 Domain Stats

Blue Team / Cyber Defense

API-ify
 Reassembler
 SET-KBLED

Blue Team / DFIR

rastrea2r
 PAE
 DAD
 Silky
 CyberCPR

DevSecOps

Puma Scan
 Serverless Prey

Industrial Control Systems

CHAPS
 ControlThings

Management

Human Metrics Matrix
 Risk Definitions
 Presenting to BOD
 NIST CSF+

SANS Faculty has a comprehensive list of Open Source tools available to support your Information Security Career, Training & Research.

Digital Forensics & Incident Response

SIFT Workstation
 REMnux
 SOF-ELK
 EZ Tools
 SRUM-DUMP
 ESE Analyst
 Werejugo
 Aurora IR
 APOLLO
 AmcacheParser
 AppCompatCacheParser
 bstrings
 EZViewer
 EvtxECmd
 Hasher
 JLECmd
 JumpList Explorer
 LECmd
 MFTECmd
 MFTEExplorer
 PECmd
 RBCmd
 RecentFileCacheParser
 Registry Explorer
 RECcmd
 SDB Explorer
 ShellBags Explorer
 SBECmd
 Timeline Explorer
 VSCMount
 WxTCmd
 iisGeoLocate

KAPE
 TimeApp
 XWFIM
 Get-ZimmermanTools
 MacMRU
 The Pyramid of Pain
 Hunting Maturity Model
 "kobackupdec"
 dpapilab
 decwindbx
 hotoloti
 ios_bfu_triage
 unssz
 w10pfdecomp
 sigs.py
 mac_robber.py
 docker_mount.py
 tln_parse.py
 sqlparse.py
 onion_peeler.py
 quicklook_parser
 chrome_parse.py
 parse_mftdump.py
 GA-Parser.py
 GA Cookie Cruncher
 "safari_parser.py"
 thunderbird_parser.py
 LMG
 DFIS
 analyzeEXT
 Linewatch

Penetration Testing

EmuRoot
 The C2 Matrix
 KillerBee
 KillerZee
 BitFit
 PPTXIndex
 PlistSubtractor
 PPTXSanity
 DynaPstalker
 PPTXUrls
 NM2LP
 MFSmartHack
 BTFind
 CoWPAtty
 PCAPHistogram
 EAPMD5Pass
 Asleep
 TIBTLE2Pcap
 Bluecrypt
 evtXResourceIDGaps
 Slingshot
 EAP-MD5-Crack
 Digestive
 Autocrack
 CrackMapExec
 SILENTRINITY
 SprayingToolkit
 Red Baron
 WitnessMe
 OffensiveDLR
 GCat
 MITMf
 DHCPShock
 wiki-dictionary-creator
 Voltaire
 Subterfuge
 Prismatic
 Diagon
 Oculus
 Tiberium
 Cryptbreaker
 Acheron
 Gryffindor
 Mailsniper for Gmail
 ads-payload
 "powercat"
 Emergence
 heimdall
 Kerberoasting
 Pause-Process

| Tool Name | Description | Author |
|--|--|----------------------------------|
| LaBrea.py | Modern implementation of LaBrea Tarpit in Python/Scapy. LaBrea allows you to set up a host that can take over all unused addresses within an IPv4 subnet, creating a low interaction honeypot (of sorts) for network worms and scans. | David Hoelzer |
| ShowMeThePackets | Collection of IDS/Network Monitoring scripts and tools covering things from data collection through analysis. | |
| VisualSniff | A simple communications visualization tool for MacOS written in Objective-C. Visualizes communicating hosts, volume, and directionality of data. | |
| DeepBlueCLI | A PowerShell Module for Threat Hunting via Windows Event Log. | Eric Conrad |
| WhatsMyName | OSINT/recon tool for user name enumeration. JSON file that is used in Spiderfoot and Recon-ng modules. | Micah Hoffman |
| untappdScraper | OSINT tool for scraping data from the untappd.com social media site. | Micah Hoffman & Brandon Evans |
| Espial | OSINT tool for asset identification, service validation and vulnerability detection. | Serge Borso |
| flare | Helps to find command and control beacons against data already ingested into Elasticsearch (supports netflow, Zeek, and likely any standard connection log). | Austin Taylor & Justin Henderson |
| VulnWhisperer | Aggregates vulnerability data and lets you report off it with ELK and allows tagging things such as PIC, HIPAA, critical asset, etc. Supports adding a score called residual_risk score which allows you to document what you feel the risk really is. | |
| Log Campaign | Scheduled task framework for automatic baselining and logging based on differences between baselines. Logging can be direct to a syslog server or to local EVTX. Custom EVTX channel is supported and log output can be plaintext or JSON. | Justin Henderson |
| Update-VMs | Automatic framework for snapshotting VMware VMs and patching them. Supports custom health checks per VM with automatic rollback of failed healthcheck and default healthcheck is to see if the server comes back online. | Josh Johnson |
| QRadar Threat Intelligence | Download a list of suspected malicious IPs and Domains. Create a QRadar Reference Set. Search Your Environment For Malicious Ips. | Nik Alleyne |
| DNSSpoof | Script to perform and teach how easy it is to build a DNS Spoofing tool using scapy. | |
| Misc Powershell & VBScript | Hundreds of PowerShell and VBScript scripts for tasks large and small related to Microsoft product security. | Jason Fossen |
| Freq Server | A Web server that integrates with SEIM systems and identifies hosts being used for Command and control by identifying domains being used for Command and Control. The tools uses character frequency analysis to identify random hostnames. | Mark Baggett |
| Domain Stats | A SEIM Integration tool that monitors DNS hostnames used by your network to identify first contact with new domains and contact with new domains that have been established in the last 2 years, effective in identifying malicious actors. | |
| Blue Team & Cyber Defense | | |
| API-ify | A Web server that provides an API that allows network defenders to consume the output of any Linux based command and integrate it into their ELK stack, splunk or other SEIM tools. | Mark Baggett |
| Reassembler | A tool that allows network defenders to reassemble and view packets using the 5 widely used fragment reassembly policies commonly found in Intrusion Detection Systems. | |
| SET-KBLED | A Powershell script that will allow you to set the Keyboard LED Color to the color of your Clevo chipset based Keyboard. When used with event log actions you have a visible early warning system. Example, have keyboards turn red when a virus is detected. | |
| Blue Team & DFIR | | |
| Rastrea2r | Rastrea2r (pronounced "rastreador" - hunter- in Spanish) is a multi-platform open source tool that allows incident responders and SOC analysts to triage suspect systems and hunt for Indicators of Compromise (IOCs) across thousands of endpoints in minutes. | Ismael Valenzuela |
| PAE | A high performance statistical analysis tool for packet headers and data. Excellent for anomaly detection, threat hunting, and beacon (protocol) detection. Supports visualization through accompanying Python script. | David Hoelzer |
| DAD | Large scale log aggregation and analysis SIEM supporting the ability to create correlation scripts based on signatures and on correlations. Supports aggregation of syslog, Windows Event Logs, and any other text based log format. | |
| Silky | Web based GUI for easy interaction with SiLK based NetFlow repositories. | |
| CyberCPR | IR Management platform for secure comms and tracking of the incident and evidence, with immutable chat, comms, hashed and encrypted central evidence files. Allowing analysts to streamline protecting their evidence and plans for network or system remediation. | Steve Armstrong |

| Tool Name | Description | Author |
|--|--|-----------------|
| SIFT Workstation | The SIFT® demonstrates that advanced incident response capabilities and deep dive digital forensic techniques to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated. | Rob Lee |
| REMnux | REMnux® is a free Linux toolkit for assisting malware analysts with reverse-engineering malicious software. This lightweight distro incorporates many tools for analyzing Windows and Linux malware and examining browser-based threats. | Lenny Zeltser |
| SOF-ELK | SOF-ELK® is a "big data analytics" platform focused on the typical needs of computer forensic investigators/analysts and information security operations personnel. The platform is a customized build of the open source Elastic stack to make large scale analysis easier. | Phil Hagen |
| EZ Tools | A suite of open source digital forensics tools that can be used in a wide variety of investigations including cross validation of tools, providing insight into technical details not exposed by other tools, and more. | Eric Zimmerman |
| AmcacheParser | Amcache.hve parser with lots of extra features. Handles locked files. | |
| AppCompatCacheParser | AppCompatCache aka ShimCache parser. Handles locked files. | |
| bstrings | Find them strings yo. Built in regex patterns. Handles locked files. | |
| EZViewer | Standalone, zero dependency viewer for .doc, .docx, .xls, .xlsx, .txt, .log, .rtf, .otd, .htm, .html, .mht, .csv, and .pdf. Any non-supported files are shown in a hex editor (with data interpreter!). | |
| EvtxECmd | Event log (evt) parser with standardized CSV, XML, and json output! Custom maps, locked file support, and more! | |
| Hasher | Hash all the things | |
| JLECmd | Jump List parser | |
| JumpList Explorer | GUI based Jump List viewer | |
| LECmd | Parse lnk files | |
| MFTECmd | \$MFT, \$Boot, \$J, \$SDS, and \$LogFile (coming soon) parser. Handles locked files | |
| MFTExplorer | \$MFT, \$Boot, \$J, \$SDS, and \$LogFile (coming soon) parser. | |
| PECmd | Prefetch parser | |
| RBCmd | Recycle Bin artifact (INFO2/\$I) parser | |
| RecentFileCacheParser | RecentFileCache parser | |
| Registry Explorer | Registry viewer with searching, multi-hive support, plugins, and more. Handles locked files | |
| RECcmd | Registry viewer with searching, multi-hive support, plugins, and more. Handles locked files | |
| SDB Explorer | Shim database GUI | |
| ShellBags Explorer | GUI for browsing shellbags data. Handles locked files | |
| SBECmd | CLI for analyzing shellbags data. | |
| Timeline Explorer | View CSV and Excel files, filter, group, sort, etc. with ease | |
| VSCMount | Mount all VSCs on a drive letter to a given mount point | |
| WxTCmd | Windows 10 Timeline database parser | |
| KAPE | Kroll Artifact Parser/Extractor: Flexible, high speed collection of files as well as processing of files. Many many features (SHORT: Rapid Triage Forensic Artifact Acquisition and Processing Tool) | |
| iisGeoLocate | Geolocate IP addresses found in IIS logs | |
| TimeApp | A simple app that shows current time (local and UTC) and optionally, public IP address. Great for testing | |
| XWFIM | X-Ways Forensics installation manager | |
| Get-ZimmermanTools | PowerShell script to auto discover and update everything above. | |
| APOLLO | Apple Pattern of Life Lazy Output'er (APOLLO) extracts and correlates data from numerous databases, then organizes it to show a detailed event log of application usage, device status, and many other pattern-of-life artifacts from Apple devices. | Sarah Edwards |
| MacMRU | Mac MRU parser | David J. Bianco |
| The Pyramid of Pain | The Pyramid of Pain is a conceptual model for the effective use of Cyber Threat Intelligence in threat detection operations, with a particular emphasis on increasing the adversaries' cost of operations. | |
| Hunting Maturity Model | The Hunting Maturity Model (HMM) is a simple model for evaluating an organization's threat hunting capability. It provides not only a "where are we now?" metric, but also a roadmap for program improvement. | |

| Tool Name | Description | Author |
|---------------------------------------|---|-------------------|
| kobackupdec | The kobackupdec is a Python3 script to decrypt Huawei HiSuite or KoBackup (Android app) backups. | Francesco Picasso |
| dpapilab | Python toolkit based on dpapick to decrypt, online and offline, DPAPI protected blobs, Windows Vaults included. | |
| decwindbx | Windows toolkit to decrypt Dropbox .dbx databases. | |
| hotoloti | Zena Forensics blog scripts set (regripper plugins, volatility mimikatz/rekall plugin, event log, etc.) | |
| unssz | Python script to decrypt Samsung / Seagate Secure Zone crypto containers (without knowing the password...). | |
| w10pfdecomp | Windows 10 Prefetch (native) decompression | |
| ios_bfu_triage | Bash script to extract data from a "chekcra1ned" iOS device. | Mattia Epifani |
| sigs.py | Generate md5, sha1, sha256, sha512, sha3-384 signatures from files (potentially recursively) | Jim Clausing |
| mac_robber.py | mac_robber rewritten in python | |
| docker_mount.py | Script to read-only mount docker layered filesystems (currently supports underlying aufs and overlay2) | |
| tln_parse.py | Python script to replace parse.exe in Mari's KAPE mini-timeline workflow to give me good yyyy-dd-mm UTC timestamps. | |
| sqlparse.py | Python and EXE to recover delete entries in SQLite Databases | |
| onion_peeler.py | Python tool to batch query IP addresses to see if they are Tor exit nodes | |
| quicklook_parser | Python tool to parse the Mac QuickLook index.sqlite database. Contains information about thumbnails generated on a Mac. | Mari DeGrazia |
| chrome_parse.py | Parse Chrome history and downloads into TSV or TLN format. | |
| parse_mftdump.py | Parses the output of mftdump.exe to bodyfile format | |
| GA-Parser.py | Python script to parse out Google Analytic Values from E01, RAM, etc. | |
| GA Cookie Cruncher | Parses out Google Analytic values for IE, FireFox, Chrome and Safari. | |
| safari_parser.py | Parses Safari history, downloads, bookmarks and topsites. | |
| thunderbird_parser.py | Parses out email from the Thunderbird client, to include deleted emails. | Mark Baggett |
| SRUM-DUMP | Windows GUI Forensics tool produces XLSX spreadsheet with detailed information on all processes that have run in the last 30 days on Windows computers. | |
| ESE Analyst | Command line based tool that dumps and analyzes databases used on Windows systems that stores various forensics information. Plugins are used to dump different types of data. | |
| Werejugo | A Windows Forensics tool that analyzes the registry, event logs and wireless network configurations to identify physical locations of where the laptop has been used. | |
| Aurora IR | Spreadsheet of Doom on steroids with some nice little graphing features, task tracking, and much more. I'll be adding new features soon. | Mathias Fuchs |
| LMG | Script to automate memory capture and profile creation for Linux systems | Hal Pomeranz |
| DFIS | EXT3 file recovery tools, timelining tools, and more | |
| analyzeEXT | Recover EXT filesystem info from carved directory blocks | |
| Linewatch | Spot outliers in large data runs | |
| DFIR & Blue Team | | |
| Rastrea2r | Rastrea2r (pronounced "rastreador" - hunter- in Spanish) is a multi-platform open source tool that allows incident responders and SOC analysts to triage suspect systems and hunt for Indicators of Compromise (IOCs) across thousands of endpoints in minutes. | Ismael Valenzuela |
| PAE | A high performance statistical analysis tool for packet headers and data. Excellent for anomaly detection, threat hunting, and beacon (protocol) detection. Supports visualization through accompanying Python script. | David Hoelzer |
| DAD | Large scale log aggregation and analysis SIEM supporting the ability to create correlation scripts based on signatures and on correlations. Supports aggregation of syslog, Windows Event Logs, and any other text based log format. | |
| Silky | Web based GUI for easy interaction with SiLK based NetFlow repositories. | |
| CyberCPR | IR Management platform for secure comms and tracking of the incident and evidence. With immutable chat, comms, hashed and encrypted central evidence files. The platform unburdens analysts from having to think about protecting their evidence and plans for network or system remediation. | Steve Armstrong |

| Tool Name | Description | Author |
|---|---|------------------|
| Slingshot | Slingshot is an Ubuntu-based Linux distribution with the MATE Desktop Environment built for use in the SANS penetration testing curriculum and beyond. Designed to be stable, reliable and lean, Slingshot is built with Vagrant and Ansible. | Ryan O'Grady |
| The C2 Matrix | Matrix of Command and Control Frameworks for Penetration Testing, Red Teaming, and Purple Teaming | Jorge Orchilles |
| Kerberoasting | Portions of Kerberos tickets may be encrypted using the password hash of the target service, and is thus vulnerable to offline Brute Force attacks that may expose plaintext credentials. | Tim Medin |
| KillerBee | KillerBee is a framework, programming API, and suite of tools for testing the security of ZigBee wireless networks | Joshua Wright |
| KillerZee | KillerZee is a framework, programming API, and suite of tools for testing the security of Z-Wave wireless networks | |
| BitFit | BitFit is a tool for guaranteeing an integrity check for distributed data files. | |
| PPTXIndex | PPTXIndex generates a Microsoft Word indexed document from PowerPoint PPTX files. | |
| PlistSubtractor | PlistSubtractor simplifies the process of assessing nested plist data | |
| PPTXSanity | PPTXSanity evaluates all of the links in a PowerPoint file to check for dead links | |
| DynaPstalker | DynaPstalker assists when fuzzing a Windows process by color-coding reached blocks for use in IDA Pro. | |
| PPTXUrls | PPTXUrls generates a HTML report of all links in one or more PowerPoint files. | |
| NM2LP | NM2LP converts NetMon wireless packet capture data to libpcap format. | |
| MFSmartHack | MFSmartHack is a suite of tools for hacking MIFARE DESFire and ULC high frequency RFID cards | |
| BTFind | BTFind is a graphical and audio interface for tracking the location of Bluetooth and Bluetooth Low Energy devices | |
| CoWPAtty | CoWPAtty is a WPA2-PSK password cracking tool. | |
| PCAPHistogram | PCAPHistogram assesses the payload of libpcap packet capture data, generating a histogram to characterize data entropy. | |
| EAPMD5Pass | EAPMD5Pass is a password cracking tool for EAP-MD5 packet captures. | |
| Asleep | Asleep is a Cisco LEAP and generic MS-CHAPv2 password cracking tool. | |
| TIBTLE2Pcap | TIBTLE2Pcap converts Bluetooth and Bluetooth Low Energy packet captures using the proprietary TI SmartRF format into libpcap-compatible files. | |
| Bluecrypt | Bluecrypt is a simple implementation of the Bluetooth authentication cryptographic functions including E0, E21 and E22. Includes some wrapper functions to make Bluetooth authentication functions a little simpler. | |
| evtxResourceIDGaps | evtxResourceIDGaps is a script to evaluate Windows EVTX logging data to identify evidence of tampered logging data. | |
| EAP-MD5-Crack | A python implementation of an EAP authentication cracking. PCAP in, password out. | Mark Baggett |
| Digestive | Dictionary cracking tool for HTTP Digest challenge/response hashes | Eric Conrad |
| Autocrack | This python script is a Hashcat wrapper to help automate the cracking process. The script includes multiple functions to select a set of wordlists and rules, as well as the ability to run a bruteforce attack, with custom masks, before the wordlist/rule attacks. | Timothy McKenzie |
| CrackMapExec | A swiss army knife for pentesting internal networks, allows pentesters to perform post-exploitation at scale. | Marcello Salvati |
| SILENTRINITY | A modern, asynchronous, multiplayer & multiserver C2/post-exploitation framework powered by Python 3 and .NET's DLR. | |
| SprayingToolkit | Scripts to make password spraying attacks against Lync/S4B & OWA a lot quicker, less painful and more efficient | |
| Red Baron | Automate creating resilient, disposable, secure and agile infrastructure for Red Teams | |
| WitnessMe | Web Inventory tool, takes screenshots of webpages using Pypeteer (headless Chrome/Chromium) and provides some extra bells & whistles to make life easier. | |
| OffensiveDLR | Toolbox containing research notes & PoC code for weaponizing .NET's DLR | |
| GCat | A PoC backdoor that uses Gmail as a C&C server | |
| MITMf | Framework for Man-In-The-Middle attacks | |
| DHCPShock | Spoofs a DHCP server and exploits all clients vulnerable to the 'ShellShock' bug. | |
| wiki-dictionary-creator | Creates a wordlist based on a Wikipedia sites articles. Allows you to select Wikipedia language. Creates wordlists based on the article titles. | |
| VoIP Hopper | VoIP Hopper is a network infrastructure penetration testing tool to test the (in)security of VLANS as well as mimic the behavior of IP Phones to automatically VLAN Hop and demonstrate risks within IP Telephony network infrastructures. | Jason Ostrom |

Penetration Testing Tools 2 of 2 + Additional Curricula

| Tool Name | Description | Author |
|--------------------------------------|--|--------------------|
| Voltaire | Voltaire is a web-based indexing tool for GIAC certification examinations. Creating an index with Voltaire is a three phase process involving: documentation/note-taking, sorting & normalization, and word processing. This readme is meant to guide users through the process. | Matthew Toussain |
| Subterfuge | Subterfuge is a Framework to take the arcane art of Man-in-the-Middle Attack and make it as simple as point and shoot. It demonstrates vulnerabilities in the ARP Protocol by harvesting credentials that go across the network, and even exploiting machines through race conditions. | |
| Prismatica | Project Prismatica is a focused framework for Command and Control that is dedicated to extensibility. Our core objective is to provide a convenient platform with modular Transports, Backends, and Implants to enable rapid retooling opportunities and enhance Red Team ops. | |
| Diagon | The Diagon Attack Framework is a Prismatica application containing the Ravenclaw, Gryffindor, and Slytherin remote access tools (RATs). | |
| Oculus | Oculus is a malleable python-based C2 system allowing for instantiation of listeners for the purpose of communication with remote access tools (RATs). | |
| Tiberium | A Command and Control scanning tool | |
| Gryffindor | The Gryffindor RAT was released at Derbycon 2018. | |
| Mailsniper for Gmail | MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange and Gsuite environment for specific terms (passwords, insider intel, network architecture information, etc.). It can be used as a non-administrative user to search their own email, or by an Exchange administrator to search the mailboxes of every user in a domain. | |
| Emergence | The Emergence fabric is an interface where interaction and integration of disparate information security subsystems gain combined intelligence. | |
| Acheron | Acheron is a RESTful vulnerability assessment and management framework built around search and dedicated to terminal extensibility. | |
| Cryptbreaker | Cryptbreaker is web application that utilizes Amazon Web Services (AWS) to perform cloud-based cracking of LM and NTLM hashes (the primary storage mechanism for hashes in a Windows Domain environment). | Geoffrey Pamerleau |
| ads-payload | Powershell script which will take any payload and put it in the a bat script which delivers the payload. The payload is delivered using environment variables, alternating-data-streams and wmic. | Chris Dale |
| powercat | Netcat implementation in PowerShell 2.0 to allow maximum portability on all PowerShell enabled hosts. | Mick Douglas |
| Pause-Process | PowerShell script which allows one to pause/unpause a running application. Makes use of existing OS functionality so there is no need to install any additional components. Can be used to allow defenders to respond at a lower threshold. | |
| heimdall | Python tool to distribute commands across many cloud instances. Originally intended for highly distributed recon scanning (non evasive, just performant). Basically wrapper around Terraform | Derek Rook |
| EmuRoot | Android_Emuroot is a Python script that allows to grant root privileges to Google API Playstore emulator shells on the fly to help Reverse Engineers to go deeper into their investigations. | Mouad Abouhali |

Other Curricula Tools

| DevSecOps | | |
|--------------------------------------|---|------------------------------|
| Puma Scan | Puma Scan is an open source software security analyzer for C# applications. Puma Scan provides a Visual Studio extension for scanning source code in the development environment and displaying vulnerabilities as spell check and compiler warnings. | Eric Johnson |
| Serverless Prey | Serverless Prey is a collection of serverless functions (FaaS) for GCP Functions, Azure Functions, and AWS Lambda. Once launched to the environment and invoked, these functions establish a TCP reverse shell for the purposes of introspecting the container runtimes of the various function runtimes. | Eric Johnson / Brandon Evans |
| Industrial Control Systems | | |
| CHAPS | Configuration Hardening Assessment PowerShell Script (CHAPS) is a PowerShell script for checking system security settings where additional software and assessment tools, such as Microsoft Policy Analyzer, cannot be installed. | Don C. Weber |
| ControlThings | An umbrella project that includes several sub-projects, including a Linux distribution (ControlThings Platform) for conducting security assessments on ICS/IIoT environments and other tools to interact with various protocols and technologies including ctmodbus, ctserial, ctui, ctspi, ct2c, etc... | Justin Searle |
| Management | | |
| Human Metrics Matrix | Interactive matrix cataloging different types of human metrics, to include compliance, behavior, cultural and strategic | Lance Spitzner |
| Risk Definitions | Breakdown, definitions and examples of the three different variables of risk | |
| Presenting to BOD | Slide deck on how to prepare for and present to Board of Directors on Cybersecurity | |
| NIST CSF+ | Framework management tool - service catalog, 5-year plan | Brian Ventura |