SECURITY CHEATSHEET

Blue Team Resources

IP Check

Virus Total - https://www.virustotal.com
Alien Vault OTX - https://otx.alienvault.com/browse/global/indicators
GreyNoise `VPN Detection` - https://viz.greynoise.io
Threat Fox - https://threatfox.abuse.ch/browse/
IP Quality Score `VPN Detection` - https://www.ipqualityscore.com/free-ip-lookup-proxy-vpn-test
Shodan - https://www.shodan.io/
Censys - https://censys.io/ipv4
Cisco TALOS - https://talosintelligence.com/
AbuseIPDB - https://www.abuseipdb.com/
Whatismyipaddress Blacklist Check - https://whatismyipaddress.com/blacklist-check
The Anti Abuse Project - http://www.anti-abuse.org/multi-rbl-check/
InQuest Labs - https://labs.inquest.net/repdb
MalwareIURL - https://www.malwareurl.com/listing-urls.php
ThreatMiner `Currently Down` - https://www.threatminer.org/
IPinfo - https://ipinfo.io/
BrowserLeaks - https://browserleaks.com
VPN & Proxy Detection `VPN Detection` - https://vpn-proxy-detection.ipify.org/
IP Teoh `VPN Detection` - https://ip.teoh.io/vpn-detection
VPNAPI.io `VPN Detection` - https://vpnapi.io/vpn-detection

Pulsedive - https://pulsedive.com/
IOC.One - https://ioc.one/

URL Check

Virus Total - https://www.virustotal.com
Alien Vault OTX - https://otx.alienvault.com/browse/global/indicators
SecurityTrails - https://securitytrails.com/domain/google.com/dns
URLHaus - https://urlhaus.abuse.ch/browse/
URLScan - https://urlscan.io/
IP Quality Score - https://www.ipqualityscore.com/threat-feeds/malicious-url-scanner
Sucuri - https://sitecheck.sucuri.net/
InQuest Labs - https://labs.inquest.net/iocdb
Threat Fox - https://threatfox.abuse.ch/browse/
MalwareURL - https://www.malwareurl.com/listing-urls.php
ThreatMiner - https://www.threatminer.org/
Pulsedive - https://pulsedive.com/
WhereGoes - https://wheregoes.com/
RedirectDetective - https://redirectdetective.com/
RedirectTracker - https://www.redirecttracker.com/
Bulkblacklist - https://www.bulkblacklist.com/
DocGuard - https://app.docguard.io/
IOC.One - https://ioc.one/

Malware Check & Dynamic Analysis

Virus Total - https://www.virustotal.com

Alien Vault OTX - https://otx.alienvault.com/browse/global/indicators

Threat Fox - https://threatfox.abuse.ch/browse/

Malware Baazar - https://bazaar.abuse.ch/browse/

Hybrid Analysis - https://www.hybrid-analysis.com/

Any Run - https://app.any.run/

Joe Sandbox - https://www.joesandbox.com/#windows

Comodo Valkyrie - https://valkyrie.comodo.com

Browserling - https://www.browserling.com/

Cuckoo Sandbox Online - https://sandbox.pikker.ee/

Cuckoo Sandbox Local - https://cuckoosandbox.org/download

Drakvuf Local Sandbox - https://github.com/CERT-Polska/drakvuf-sandbox

Noriben Local Sandbox - https://github.com/Rurik/Noriben

Triage - https://tria.ge/reports/public

CAPE - https://capesandbox.com/

Intezer - https://analyze.intezer.com/scan

IRIS-H Digital Forensics - https://iris-h.services/pages/dashboard

Malshare - https://malshare.com/

YOMI - https://yomi.yoroi.company/upload

InQuest Labs - https://labs.inquest.net/dfi

Manalyzer - https://manalyzer.org/

ThreatMiner - https://www.threatminer.org/

Pulsedive - https://pulsedive.com/

IObit - https://cloud.iobit.com/index.php

Amnpardaz Sandbox - https://jevereg.amnpardaz.com/

DocGuard - https://app.docguard.io/

Sophos Intelix - https://intelix.sophos.com/

Cyber Threat Intelligence

Vuldb - https://vuldb.com/

Alien Vault OTX - https://otx.alienvault.com/browse/global/indicators

IBM X-Force Exchange- https://exchange.xforce.ibmcloud.com/

Feedly - https://feedly.com/

Inoreader - https://www.inoreader.com/

PulseDive Threat Feed - https://pulsedive.com/explore/threats/

PulseDive Ransomware Feed - https://pulsedive.com/threat/Ransomware

Ransomlook.io - https://www.ransomlook.io/

Ransomware Live - https://www.ransomware.live/

HudsonRock Tools - https://www.hudsonrock.com/threat-intelligence-cybercrime-tools

Malpedia - https://malpedia.caad.fkie.fraunhofer.de/

IntelX - https://intelx.io/tools?tab=general

SANS Internet Storm Center - https://isc.sans.edu/

SOCRadar Labs - https://socradar.io/labs

Threat Fox - https://threatfox.abuse.ch/browse/

ThreatMiner - https://www.threatminer.org/

Malware Baazar - https://bazaar.abuse.ch/browse/

Virus Total - https://www.virustotal.com/gui/home/search

Shodan - https://www.shodan.io/

Censys - https://censys.io/ipv4

Any-run - https://any.run/malware-trends/

Risk IQ Community - https://community.riskiq.com/home

Mandiant Threat Intelligence - https://www.mandiant.com/advantage/threat-intelligence/free-version

VmWare Carbon Black - https://community.carbonblack.com/

Crowdstrike Threat Profile - https://www.crowdstrike.com/adversaries/?ref=adversary.crowdstrike.com

SecureWorks Threat Profile - https://www.secureworks.com/research/threat-profiles

Dragos Threat Profile - https://www.dragos.com/threat-groups/

Lab52 Threat Mapping Tool - https://lab52.io/

vx-underground APT repository - https://vx-underground.org/samples/Families/APT/

Threat Actor Map - https://aptmap.netlify.app/

Nation State Cyber Operation Map - https://www.cfr.org/cyber-operations/

Intezer OST Map - https://intezer.com/ost-map/

Ransom Wiki - https://ransom.wiki/

Kaspersky CyberTrace Feeds - https://support.kaspersky.com/datafeeds/about/13850

Cyber Operations Tracker - https://www.cfr.org/cyber-operations/

MISP Galaxy Threat Map - https://raw.githubusercontent.com/MISP/misp-galaxy/main/clusters/threat-actor.json

InTheWild Feed Vuln Feed - https://inthewild.io/feed

RESCURE Threat Feeds - https://rescure.me/feeds.html

IOC.One - https://ioc.one/

Dark Web Hub - https://slcyber.io/dark-web-hub/

Cyber Threat Intelligence Articles

1. Cyber Threat Intelligence for Autodidacts
2. Intelligence Structured Analytical Techniques (SAT)
3. Intelligence Report Writing
4. Intelligence Profiling
5. Dark Web Monitoring
6. The Cyber Threat Intelligence Life Cycle: A Case Study
7. Teaching the Intelligence Process: The Killing of Bin Laden as a Case Study

Learning Spots & CTF - Blue Team

Let's Defend - https://letsdefend.io/

Cyber Defenders - https://cyberdefenders.org/

Blue Team Labs - https://blueteamlabs.online/

Forensic Analysis Resources

Incident Response Linux Cheatsheet - https://www.hackingarticles.in/incident-response-linux-cheatsheet/

Red Team Resources

OSINT

OSINT Framework - https://osintframework.com/
OSINT Cheatsheet - https://www.cheatsheet.wtf/osint/
FullContact API - https://platform.fullcontact.com/developers/api-keys
Intelius - https://www.intelius.com/
GoodHire - https://www.goodhire.com/
Webmii - https://webmii.com
GrayHat Warfare - https://buckets.grayhatwarfare.com/
ICANN Lookup - https://lookup.icann.org/en
cqcounter Whois - http://www.cqcounter.biz/whois/
Subdomain Finder - https://subdomainfinder.c99.nl/
Asint Collection - https://start.me/p/b5Aow7/asint_collection
DNSdumpster - https://dnsdumpster.com/
DNSTwister - https://dnstwister.report/
Blackbird - https://blackbird-osint.herokuapp.com/
Search 0t Rocks - https://search.0t.rocks/ (Currently down)
Breach Directory - https://breachdirectory.org/
PimEyes - https://pimeyes.com/pt
TinEye - https://tineye.com/

Pentest References and CheatSheets

Hacking Articles - https://www.hackingarticles.in/
Hack Tricks - https://book.hacktricks.xyz/
Cloud Hack Tricks - https://cloud.hacktricks.xyz/
Pentest Book - https://chryzsh.gitbooks.io/pentestbook/content/
Total OSCP Guide - https://sushant747.gitbooks.io/total-oscp-guide/content/
Hack The Box OSCP Preparation - https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/
Steflan Security - https://steflan-security.com
SecWiki - https://wiki.zacheller.dev/
Hausec - https://hausec.com/
HighOnCoffee - https://highon.coffee/blog/
/home/six2dez/.pentest-book - https://pentestbook.six2dez.com/
0xffsec Handbook - https://0xffsec.com/handbook/
haax's Cheatsheet - https://cheatsheet.haax.fr/
golinuxcloud - https://www.golinuxcloud.com/kali-linux-bootable-usb/
Pentest Monkey - http://pentestmonkey.net/
Web App Testing Guide - https://owasp.org/www-project-web-security-testing-guide/stable/
explainshell - https://explainshell.com/

Learning Spots & CTF - Red Team

HackTheBox - https://www.hackthebox.eu/
TryHackMe - https://tryhackme.com/
VulnHub - https://www.vulnhub.com/
PortSwigger - https://portswigger.net/web-security/all-materials
Hacker101 - https://ctf.hacker101.com/

HackMyVM - https://hackmyvm.eu/

AndroidCTF - https://ctf.hpandro.raviramesh.info/

Cracking Hashes

CrackStation - https://crackstation.net/

Hashes.com - https://hashes.com/en/decrypt/hash

Hashkiller - https://hashkiller.io

Reverse Shell Utility

Revshell - https://www.revshells.com/

IP Logger

IP Logger - https://iplogger.org/

Grabify - https://grabify.link

Privilege Escalation & Interactive Shell

GTFOBins - https://gtfobins.github.io/#

Exploit Development Resources & Articles

1. Exploit Development - Everything you need to know
2. How to build your own exploits, Part 1
3. How to build your own exploits, Part 2
4. How to build your own exploits, Part 3

5. How to create a Metasploit Exploit in a few minutes
6. Metasploit - Building a Module
7. The art of creating backdoors and exploits with Metasploit

Other Useful Red Team Articles

1. Privilege escalation in Linux using Capabilities
2. Wordpress Reverse Shell
3. Wordpress User Cracking
4. Web Apps Testing Guide by OWASP
5. Phishing attack using SET and Ettercap

In between...

Webhook Testers

Webhook Site - https://webhook.site/

Webhook Test - https://webhook-test.com/

Typed Webhook Tools - https://typedwebhook.tools/

Bins

PrivateBin - https://privatebin.net/

Dontpad - https://dontpad.com/

File Sharing

Send - https://send.vis.ee/

Wormhole - https://wormhole.app/

WeTransfer - https://wetransfer.com/

OnionShare - https://onionshare.org/ (require download)

BiteBlob - https://biteblob.com/

Password Sharing

PWPush - https://pwpush.com/p/new

URL Shorteners

Tinyurl - https://tinyurl.com/

Shorturl - https://www.shorturl.at

T.ly - https://t.ly/

Private Comms

Signal - https://signal.org/

Session - https://getsession.org/

Tox - https://tox.chat/

Matrix - https://matrix.org/

Jabber - https://www.jabber.org/

Temp Phone Numbers

TextVerified - https://www.textverified.com/

VPNs

Nord - https://nordvpn.com/
Surfshark - https://surfshark.com/
Proton - https://protonvpn.com/
Express - https://www.expressvpn.com/

Android Emulation

BlissOS - https://blissos.org/
MemuPlay - https://www.memuplay.com/

AI

Perplexity - https://www.perplexity.ai
NotebookLM - https://notebooklm.google.com/
Microsoft Copilot - https://copilot.microsoft.com/
ChatGPT - https://chatgpt.com/
Deepseek - https://chat.deepseek.com/
Google Gemini - https://gemini.google.com/

Scanning / Pentesting

- OpenVAS - OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.
- Metasploit Framework - A tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.
- Kali - Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. Kali Linux is preinstalled with numerous penetration-testing programs, including nmap (a port scanner), Wireshark (a packet analyzer), John the Ripper (a password cracker), and Aircrack-ng (a software suite for penetration-testing wireless LANs).
- tsurugi - heavily customized Linux distribution that designed to support DFIR investigations, malware analysis and OSINT activities. It is based on Ubuntu 20.04(64-bit with a 5.15.12 custom kernel)
- pig - A Linux packet crafting tool.
- scapy - Scapy: the python-based interactive packet manipulation program & library.
- Pompem - Pompem is an open source tool, which is designed to automate the search for exploits in major databases. Developed in Python, has a system of advanced search, thus facilitating the work of pentesters and ethical hackers. In its current version, performs searches in databases: Exploit-db, 1337day, Packetstorm Security...
- Nmap - Nmap is a free and open source utility for network discovery and security auditing.
- Amass - Amass performs DNS subdomain enumeration by scraping the largest number of disparate data sources, recursive brute forcing, crawling of web archives, permuting and altering names, reverse DNS sweeping and other techniques.
- Anevicon - The most powerful UDP-based load generator, written in Rust.

- Finshir - A coroutines-driven Low & Slow traffic generator, written in Rust.
- Legion - Open source semi-automated discovery and reconnaissance network penetration testing framework.
- Sublist3r - Fast subdomains enumeration tool for penetration testers
- RustScan - Faster Nmap scanning with Rust. Take a 17 minute Nmap scan down to 19 seconds.
- Boofuzz - Fuzzing engine and fuzz testing framework.
- monsoon - Very flexible and fast interactive HTTP enumeration/fuzzing.
- Netz- Discover internet-wide misconfigurations, using zgrab2 and others.
- Deepfence ThreatMapper - Apache v2, powerful runtime vulnerability scanner for kubernetes, virtual machines and serverless.
- Deepfence SecretScanner - Find secrets and passwords in container images and file systems.
- Cognito Scanner - CLI tool to pentest Cognito AWS instance. It implements three attacks: unwanted account creation, account oracle and identity pool escalation

Monitoring / Logging

- BoxyHQ - Open source API for security and compliance audit logging.
- justniffer - Justniffer is a network protocol analyzer that captures network traffic and produces logs in a customized way, can emulate Apache web server log files, track response times and extract all "intercepted" files from the HTTP traffic.
- httpry - httpry is a specialized packet sniffer designed for displaying and logging HTTP traffic. It is not intended to perform analysis itself, but to capture, parse, and log the traffic for later analysis. It can be run in real-time displaying the traffic as it is parsed, or as a daemon process that logs to an output file. It is written to be as lightweight and flexible as possible, so that it can be easily adaptable to different applications.
- ngrep - ngrep strives to provide most of GNU grep's common features, applying them to the network layer. ngrep is a pcap-aware tool that will allow you to specify extended regular or hexadecimal expressions to match against data

payloads of packets. It currently recognizes IPv4/6, TCP, UDP, ICMPv4/6, IGMP and Raw across Ethernet, PPP, SLIP, FDDI, Token Ring and null interfaces, and understands BPF filter logic in the same fashion as more common packet sniffing tools, such as tcpdump and snoop.

- passivedns - A tool to collect DNS records passively to aid Incident handling, Network Security Monitoring (NSM) and general digital forensics. PassiveDNS sniffs traffic from an interface or reads a pcap-file and outputs the DNS-server answers to a log file. PassiveDNS can cache/aggregate duplicate DNS answers in-memory, limiting the amount of data in the logfile without loosing the essens in the DNS answer.
- sagan - Sagan uses a 'Snort like' engine and rules to analyze logs (syslog/event log/snmptrap/netflow/etc).
- ntopng - Ntopng is a network traffic probe that shows the network usage, similar to what the popular top Unix command does.
- Falco - The cloud-native runtime security project and de facto Kubernetes threat detection engine now part of the CNCF.

IDS / IPS / Host IDS / Host IPS

- Snort - Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS)created by Martin Roesch in 1998. Snort is now developed by Sourcefire, of which Roesch is the founder and CTO. In 2009, Snort entered InfoWorld's Open Source Hall of Fame as one of the "greatest [pieces of] open source software of all time".
- Zeek - Zeek is a powerful network analysis framework that is much different from the typical IDS you may know.
    - zeek2es - An open source tool to convert Zeek logs to Elastic/OpenSearch. You can also output pure JSON from Zeek's TSV logs!
- DrKeithJones.com - A blog on cyber security and network security monitoring.

- OSSEC - Comprehensive Open Source HIDS. Not for the faint of heart. Takes a bit to get your head around how it works. Performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, MacOS, Solaris, HP-UX, AIX and Windows. Plenty of reasonable documentation. Sweet spot is medium to large deployments.
- Suricata - Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF and its supporting vendors.
- Security Onion - Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Zeek, OSSEC, Sguil, Squert, Snorby, ELSA, Xplico, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!
- sshwatch - IPS for SSH similar to DenyHosts written in Python. It also can gather information about attacker during the attack in a log.
- Stealth - File integrity checker that leaves virtually no sediment. Controller runs from another machine, which makes it hard for an attacker to know that the file system is being checked at defined pseudo random intervals over SSH. Highly recommended for small to medium deployments.
- AIEngine - AIEngine is a next generation interactive/programmable Python/Ruby/Java/Lua packet inspection engine with capabilities of learning without any human intervention, NIDS(Network Intrusion Detection System) functionality, DNS domain classification, network collector, network forensics and many others.
- Denyhosts - Thwart SSH dictionary based attacks and brute force attacks.
- Fail2Ban - Scans log files and takes action on IPs that show malicious behavior.
- SSHGuard - A software to protect services in addition to SSH, written in C
- Lynis - an open source security auditing tool for Linux/Unix.

- wazuh - Wazuh is a free and open source XDR platform used for threat prevention, detection, and response. It is capable of protecting workloads across on-premises, virtualized, containerized, and cloud-based environments. Great tool foor all kind of deployments, it includes SIEM capabitilies (indexing + searching + WUI).

Honey Pot / Honey Net

- Conpot - ICS/SCADA Honeypot. Conpot is a low interactive server side Industrial Control Systems honeypot designed to be easy to deploy, modify and extend. By providing a range of common industrial control protocols we created the basics to build your own system, capable to emulate complex infrastructures to convince an adversary that he just found a huge industrial complex. To improve the deceptive capabilities, we also provided the possibility to server a custom human machine interface to increase the honeypots attack surface. The response times of the services can be artificially delayed to mimic the behaviour of a system under constant load. Because we are providing complete stacks of the protocols, Conpot can be accessed with productive HMI's or extended with real hardware. Conpot is developed under the umbrella of the Honeynet Project and on the shoulders of a couple of very big giants.
- Glastopf - Glastopf is a Honeypot which emulates thousands of vulnerabilities to gather data from attacks targeting web applications. The principle behind it is very simple: Reply the correct response to the attacker exploiting the web application.
- Kojoney - Kojoney is a low level interaction honeypot that emulates an SSH server. The daemon is written in Python using the Twisted Conch libraries.
- Bifrozt - Bifrozt is a NAT device with a DHCP server that is usually deployed with one NIC connected directly to the Internet and one NIC connected to the internal network. What differentiates Bifrozt from other standard NAT devices is its ability to work as a transparent SSHv2 proxy between an attacker and your honeypot. If you deployed an SSH server on Bifrozt's internal network it would log all the

interaction to a TTY file in plain text that could be viewed later and capture a copy of any files that were downloaded. You would not have to install any additional software, compile any kernel modules or use a specific version or type of operating system on the internal SSH server for this to work. It will limit outbound traffic to a set number of ports and will start to drop outbound packets on these ports when certain limits are exceeded.

- HoneyDrive - HoneyDrive is the premier honeypot Linux distro. It is a virtual appliance (OVA) with Xubuntu Desktop 12.04.4 LTS edition installed. It contains over 10 pre-installed and pre-configured honeypot software packages such as Kippo SSH honeypot, Dionaea and Amun malware honeypots, Honeyd low-interaction honeypot, Glastopf web honeypot and Wordpot, Conpot SCADA/ICS honeypot, Thug and PhoneyC honeyclients and more. Additionally it includes many useful pre-configured scripts and utilities to analyze, visualize and process the data it can capture, such as Kippo-Graph, Honeyd-Viz, DionaeaFR, an ELK stack and much more. Lastly, almost 90 well-known malware analysis, forensics and network monitoring related tools are also present in the distribution.
- Cuckoo Sandbox - Cuckoo Sandbox is an Open Source software for automating analysis of suspicious files. To do so it makes use of custom components that monitor the behavior of the malicious processes while running in an isolated environment.
- T-Pot Honeypot Distro - T-Pot is based on the network installer of Ubuntu Server 16/17.x LTS. The honeypot daemons as well as other support components being used have been containerized using docker. This allows us to run multiple honeypot daemons on the same network interface while maintaining a small footprint and constrain each honeypot within its own environment.

Full Packet Capture / Forensic

- Xplico - The goal of Xplico is extract from an internet traffic capture the applications data contained. For example, from a pcap file Xplico extracts each email (POP, IMAP, and SMTP protocols), all HTTP contents, each VoIP call (SIP), FTP, TFTP, and so on. Xplico isn't a network protocol analyzer. Xplico is an open source Network Forensic Analysis Tool (NFAT).
- OpenFPC - OpenFPC is a set of tools that combine to provide a lightweight full-packet network traffic recorder & buffering system. It's design goal is to allow non-expert users to deploy a distributed network traffic recorder on COTS hardware while integrating into existing alert and log management tools.

Sniffer

- wireshark - Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.
- netsniff-ng - netsniff-ng is a free Linux networking toolkit, a Swiss army knife for your daily Linux network plumbing if you will. Its gain of performance is reached by zero-copy mechanisms, so that on packet reception and transmission the kernel does not need to copy packets from kernel space to user space and vice versa.
- Live HTTP headers - Live HTTP headers is a free firefox addon to see your browser requests in real time. It shows the entire headers of the requests and can be used to find the security loopholes in implementations.

Security Information & Event Management

- Prelude - Prelude is a Universal "Security Information & Event Management" (SIEM) system. Prelude collects, normalizes, sorts, aggregates, correlates and reports all security-related events independently of the product brand or license giving rise to such events; Prelude is "agentless".
- OSSIM - OSSIM provides all of the features that a security professional needs from a SIEM offering – event collection, normalization, and correlation.
- FIR - Fast Incident Response, a cybersecurity incident management platform.
- LogESP - Open Source SIEM (Security Information and Event Management system).

VPN

- OpenVPN - OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.
- Firezone - Open-source VPN server and egress firewall for Linux built on WireGuard that makes it simple to manage secure remote access to your company’s private networks. Firezone is easy to set up (all dependencies are bundled thanks to Chef Omnibus), secure, performant, and self hostable.

Fast Packet Processing

- DPDK - DPDK is a set of libraries and drivers for fast packet processing.
- PFQ - PFQ is a functional networking framework designed for the Linux operating system that allows efficient packets capture/transmission (10G and beyond), in-kernel functional processing and packets steering across sockets/end-points.

- PF_RING - PF_RING is a new type of network socket that dramatically improves the packet capture speed.
- PF_RING ZC (Zero Copy) - PF_RING ZC (Zero Copy) is a flexible packet processing framework that allows you to achieve 1/10 Gbit line rate packet processing (both RX and TX) at any packet size. It implements zero copy operations including patterns for inter-process and inter-VM (KVM) communications.
- PACKET_MMAP/TPACKET/AF_PACKET - It's fine to use PACKET_MMAP to improve the performance of the capture and transmission process in Linux.
- netmap - netmap is a framework for high speed packet I/O. Together with its companion VALE software switch, it is implemented as a single kernel module and available for FreeBSD, Linux and now also Windows.

Firewall

- pfSense - Firewall and Router FreeBSD distribution.
- OPNsense - is an open source, easy-to-use and easy-to-build FreeBSD based firewall and routing platform. OPNsense includes most of the features available in expensive commercial firewalls, and more in many cases. It brings the rich feature set of commercial offerings with the benefits of open and verifiable sources.
- fwknop - Protects ports via Single Packet Authorization in your firewall.

Anti-Spam

- rspamd - Fast, free and open-source spam filtering system.
- SpamAssassin - A powerful and popular email spam filter employing a variety of detection technique.
- Scammer-List - A free open source AI based Scam and Spam Finder with a free API

Docker Images for Penetration Testing & Security

- `docker pull kalilinux/kali-linux-docker` official Kali Linux
- `docker pull owasp/zap2docker-stable` - official OWASP ZAP
- `docker pull wpscanteam/wpscan` - official WPScan
- `docker pull remnux/metasploit` - docker-metasploit
- `docker pull citizenstig/dvwa` - Damn Vulnerable Web Application (DVWA)
- `docker pull wpscanteam/vulnerablewordpress` - Vulnerable WordPress Installation
- `docker pull hmlio/vaas-cve-2014-6271` - Vulnerability as a service: Shellshock
- `docker pull hmlio/vaas-cve-2014-0160` - Vulnerability as a service: Heartbleed
- `docker pull opendns/security-ninjas` - Security Ninjas
- `docker pull diogomonica/docker-bench-security` - Docker Bench for Security
- `docker pull ismisepaul/securityshepherd` - OWASP Security Shepherd
- `docker pull danmx/docker-owasp-webgoat` - OWASP WebGoat Project docker image
- `docker-compose build && docker-compose up` - OWASP NodeGoat
- `docker pull citizenstig/nowasp` - OWASP Mutillidae II Web Pen-Test Practice Application
- `docker pull bkimminich/juice-shop` - OWASP Juice Shop
- `docker pull jeroenwillemsen/wrongsecrets`- OWASP WrongSecrets
- `docker run -dit --name trd -p 8081:80 cylabs/cy-threat-response` - Cyware Threat Response Docker

Endpoint

Anti-Virus / Anti-Malware

- Linux Malware Detect - A malware scanner for Linux designed around the threats faced in shared hosted environments.
- rkhunter - A Rootkit Hunter for Linux

- ClamAv - ClamAV® is an open-source antivirus engine for detecting trojans, viruses, malware & other malicious threats.

Configuration Management

- Fleet device management - Fleet is the lightweight, programmable telemetry platform for servers and workstations. Get comprehensive, customizable data from all your devices and operating systems.
- Rudder - Rudder is an easy to use, web-driven, role-based solution for IT Infrastructure Automation & Compliance. Automate common system administration tasks (installation, configuration); Enforce configuration over time (configuring once is good, ensuring that configuration is valid and automatically fixing it is better); Inventory of all managed nodes; Web interface to configure and manage nodes and their configuration; Compliance reporting, by configuration and/or by node.

Authentication

- google-authenticator - The Google Authenticator project includes implementations of one-time passcode generators for several mobile platforms, as well as a pluggable authentication module (PAM). One-time passcodes are generated using open standards developed by the Initiative for Open Authentication (OATH) (which is unrelated to OAuth). These implementations support the HMAC-Based One-time Password (HOTP) algorithm specified in RFC 4226 and the Time-based One-time Password (TOTP) algorithm specified in RFC 6238. Tutorials: How to set up two-factor authentication for SSH login on Linux

Mobile / Android / iOS

- SecMobi Wiki - A collection of mobile security resources which including articles, blogs, books, groups, projects, tools and conferences. *
- Mobile Security Wiki - A collection of mobile security resources.

Threat Intelligence

- abuse.ch - ZeuS Tracker / SpyEye Tracker / Palevo Tracker / Feodo Tracker tracks Command&Control servers (hosts) around the world and provides you a domain- and an IP-blocklist.
- Cyware Threat Intelligence Feeds - Cyware's Threat Intelligence feeds brings to you the valuable threat data from a wide range of open and trusted sources to deliver a consolidated stream of valuable and actionable threat intelligence. Our threat intel feeds are fully compatible with STIX 1.x and 2.0, giving you the latest information on malicious malware hashes, IPs and domains uncovered across the globe in real-time.
- Emerging Threats - Open Source - Emerging Threats began 10 years ago as an open source community for collecting Suricata and SNORT® rules, firewall rules, and other IDS rulesets. The open source community still plays an active role in Internet security, with more than 200,000 active users downloading the ruleset daily. The ETOpen Ruleset is open to any user or organization, as long as you follow some basic guidelines. Our ETOpen Ruleset is available for download any time.
- PhishTank - PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.
- SBL / XBL / PBL / DBL / DROP / ROKSO - The Spamhaus Project is an international nonprofit organization whose mission is to track the Internet's spam operations and sources, to provide dependable realtime anti-spam protection for

Internet networks, to work with Law Enforcement Agencies to identify and pursue spam and malware gangs worldwide, and to lobby governments for effective anti-spam legislation.

- Internet Storm Center - The ISC was created in 2001 following the successful detection, analysis, and widespread warning of the Li0n worm. Today, the ISC provides a free analysis and warning service to thousands of Internet users and organizations, and is actively working with Internet Service Providers to fight back against the most malicious attackers.
- AutoShun - AutoShun is a Snort plugin that allows you to send your Snort IDS logs to a centralized server that will correlate attacks from your sensor logs with other snort sensors, honeypots, and mail filters from around the world.
- DNS-BH - The DNS-BH project creates and maintains a listing of domains that are known to be used to propagate malware and spyware. This project creates the Bind and Windows zone files required to serve fake replies to localhost for any requests to these, thus preventing many spyware installs and reporting.
- AlienVault Open Threat Exchange - AlienVault Open Threat Exchange (OTX), to help you secure your networks from data loss, service disruption and system compromise caused by malicious IP addresses.
- Tor Bulk Exit List - CollecTor, your friendly data-collecting service in the Tor network. CollecTor fetches data from various nodes and services in the public Tor network and makes it available to the world. If you're doing research on the Tor network, or if you're developing an application that uses Tor network data, this is your place to start. TOR Node List / DNS Blacklists / Tor Node List
- leakedin.com - The primary purpose of leakedin.com is to make visitors aware about the risks of loosing data. This blog just compiles samples of data lost or disclosed on sites like pastebin.com.
- FireEye OpenIOCs - FireEye Publicly Shared Indicators of Compromise (IOCs)
- OpenVAS NVT Feed - The public feed of Network Vulnerability Tests (NVTs). It contains more than 35,000 NVTs (as of April 2014), growing on a daily basis. This feed is configured as the default for OpenVAS.

- Project Honey Pot - Project Honey Pot is the first and only distributed system for identifying spammers and the spambots they use to scrape addresses from your website. Using the Project Honey Pot system you can install addresses that are custom-tagged to the time and IP address of a visitor to your site. If one of these addresses begins receiving email we not only can tell that the messages are spam, but also the exact moment when the address was harvested and the IP address that gathered it.
- virustotal - VirusTotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners. At the same time, it may be used as a means to detect false positives, i.e. innocuous resources detected as malicious by one or more scanners.
- IntelMQ - IntelMQ is a solution for CERTs for collecting and processing security feeds, pastebins, tweets using a message queue protocol. It's a community driven initiative called IHAP (Incident Handling Automation Project) which was conceptually designed by European CERTs during several InfoSec events. Its main goal is to give to incident responders an easy way to collect & process threat intelligence thus improving the incident handling processes of CERTs.
- CIFv2 - CIF is a cyber threat intelligence management system. CIF allows you to combine known malicious threat information from many sources and use that information for identification (incident response), detection (IDS) and mitigation (null route).
- MISP - Open Source Threat Intelligence Platform - MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators. A threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. The MISP project includes software, common libraries (taxonomies, threat-actors and various malware), an extensive data model to share new information using objects and default feeds.
- PhishStats - Phishing Statistics with search for IP, domain and website title.

- Threat Jammer - REST API service that allows developers, security engineers, and other IT professionals to access curated threat intelligence data from a variety of sources.
- Cyberowl - A daily updated summary of the most frequent types of security incidents currently being reported from different sources.

Social Engineering

- Gophish - An Open-Source Phishing Framework.

Web

Organization

- OWASP - The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software.
- Portswigger - PortSwigger offers tools for web application security, testing & scanning. Choose from a wide range of security tools & identify the very latest vulnerabilities.

Web Application Firewall

- ModSecurity - ModSecurity is a toolkit for real-time web application monitoring, logging, and access control.

Scanning / Pentesting

- Spyse - Spyse is an OSINT search engine that provides fresh data about the entire web. All the data is stored in its own DB for instant access and interconnected with each other for flexible search. Provided data: IPv4 hosts,

sub/domains/whois, ports/banners/protocols, technologies, OS, AS, wide SSL/TLS DB and more.

- sqlmap - sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.
- ZAP - The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing. ZAP provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.
- OWASP Testing Checklist v4 - List of some controls to test during a web vulnerability assessment. Markdown version may be found here.
- w3af - w3af is a Web Application Attack and Audit Framework. The project's goal is to create a framework to help you secure your web applications by finding and exploiting all web application vulnerabilities.

Runtime Application Self-Protection

- Sqreen - Sqreen is a Runtime Application Self-Protection (RASP) solution for software teams. An in-app agent instruments and monitors the app. Suspicious user activities are reported and attacks are blocked at runtime without code modification or traffic redirection.
- OpenRASP - An open source RASP solution actively maintained by Baidu Inc. With context-aware detection algorithm the project achieved nearly no false positives. And less than 3% performance reduction is observed under heavy server load.

Development

- API Security in Action - Book covering API security including secure development, token-based authentication, JSON Web Tokens, OAuth 2, and Macaroons. (early access, published continuously, final release summer 2020)
- Secure by Design - Book that identifies design patterns and coding styles that make lots of security vulnerabilities less likely. (early access, published continuously, final release fall 2017)
- Understanding API Security - Free eBook sampler that gives some context for how API security works in the real world by showing how APIs are put together and how the OAuth protocol can be used to protect them.
- OAuth 2 in Action - Book that teaches you practical use and deployment of OAuth 2 from the perspectives of a client, an authorization server, and a resource server.

Usability

- Usable Security Course - Usable Security course at coursera. Quite good for those looking for how security and usability intersects.

DevOps

- Securing DevOps - A book on Security techniques for DevOps that reviews state of the art practices used in securing web applications and their infrastructure.

Operating Systems

Privacy & Security

- Qubes OS - Qubes OS is a free and open-source security-oriented operating system meant for single-user desktop computing.

- Whonix - Operating System designed for anonymity.
- Tails OS - Tails is a portable operating system that protects against surveillance and censorship.

Crypto

Tools used for solving Crypto challenges

- PkCrack - A tool for Breaking PkZip-encryption.
- QuipQuip - An online tool for breaking substitution ciphers or vigenere ciphers (without key).

Bruteforcers

Tools used for various kind of bruteforcing (passwords etc.)

- Hashcat - Password Cracker
- Hydra - A parallelized login cracker which supports numerous protocols to attack
- John The Ripper - Password Cracker.
- Ophcrack - Windows password cracker based on rainbow tables.
- Turbo Intruder - Burp Suite extension for sending large numbers of HTTP requests

Exploits

Tools used for solving Exploits challenges

- Metasploit - Penetration testing software.
    - Cheatsheet

Forensics

Tools used for solving Forensics challenges

- Aircrack-Ng - Crack 802.11 WEP and WPA-PSK keys.
    - `apt-get install aircrack-ng`
- Audacity - Analyze sound files (mp3, m4a, whatever).
    - `apt-get install audacity`
- Bkhive and Samdump2 - Dump SYSTEM and SAM files.
    - `apt-get install samdump2 bkhive`
- CFF Explorer - PE Editor.
- Exif Tool - Read, write and edit file metadata.
- Extundelete - Used for recovering lost data from mountable images.

- Foremost - Extract particular kind of files using headers.
    - `apt-get install foremost`
- Fsck.ext4 - Used to fix corrupt filesystems.
- Malzilla - Malware hunting tool.
- NetworkMiner - Network Forensic Analysis Tool.
- PDF Streams Inflater - Find and extract zlib files compressed in PDF files.
- Pngcheck - Verifies the integrity of PNG and dump all of the chunk-level information in human-readable form.
    - `apt-get install pngcheck`
- ResourcesExtract - Extract various filetypes from exes.
- Snow - A Whitespace Steganography Tool.
- Volatility - To investigate memory dumps.
- Wireshark - Used to analyze pcap or pcapng files

Online resources

- Security related Operating Systems @ Rawsec - Complete list of security related operating systems
- Best Linux Penetration Testing Distributions @ CyberPunk - Description of main penetration testing distributions
- Security @ Distrowatch - Website dedicated to talking about, reviewing and keeping up to date with open source operating systems
- Hardening Windows 10 - Guide for hardening Windows 10

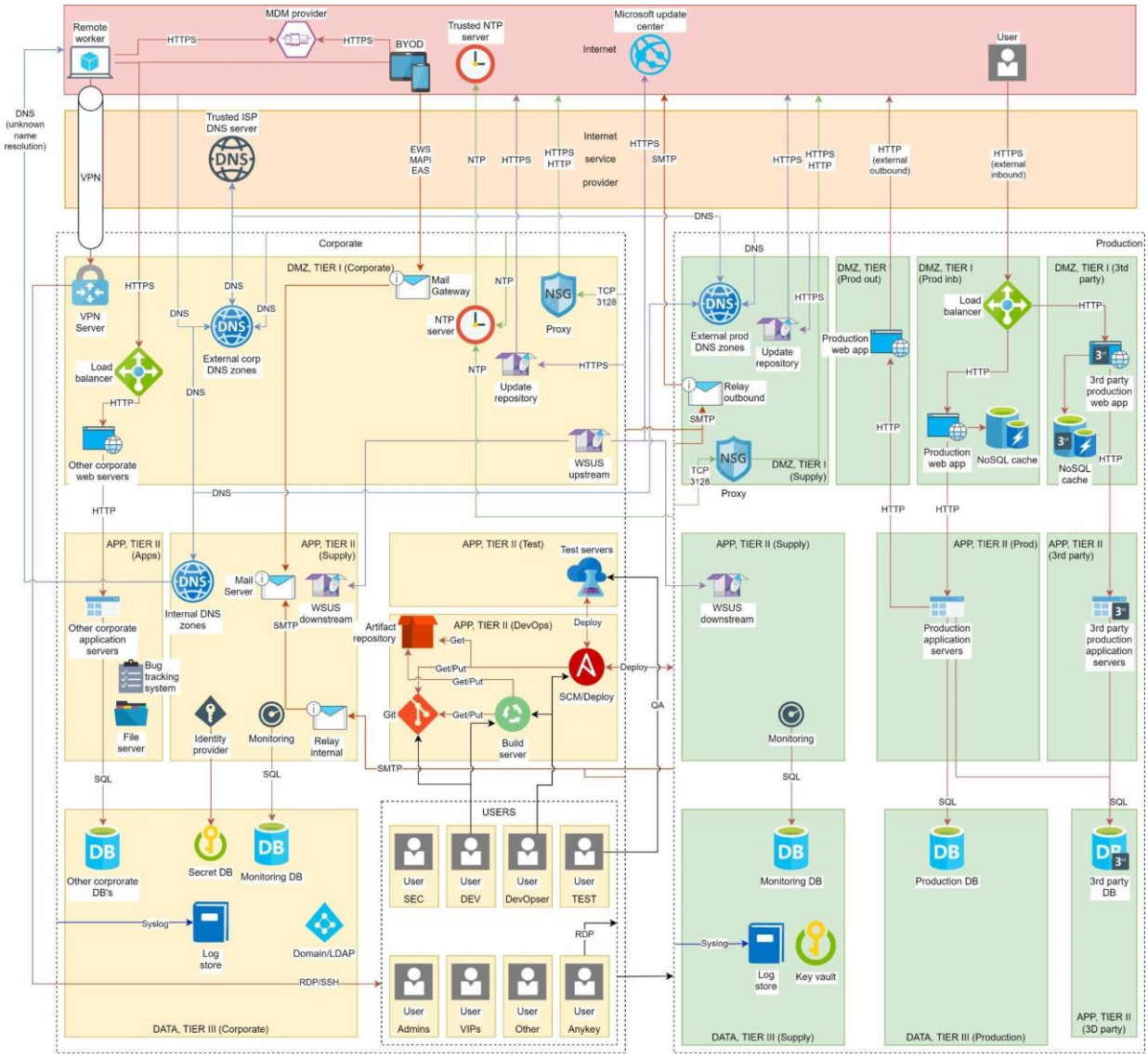
EBooks

- Docker Security - Quick Reference: For DevOps Engineers - A book on understanding the Docker security defaults, how to improve them (theory and practical), along with many tools and techniques.
- How to Hack Like a Pornstar - A step by step process for breaking into a BANK, Sparc Flow, 2017
- How to Hack Like a Legend - A hacker's tale breaking into a secretive offshore company, Sparc Flow, 2018
- How to Investigate Like a Rockstar - Live a real crisis to master the secrets of forensic analysis, Sparc Flow, 2017
- Real World Cryptography - This early-access book teaches you applied cryptographic techniques to understand and apply security at every level of your systems and applications.
- AWS Security - This early-access book covers commong AWS security issues and best practices for access policies, data protection, auditing, continuous monitoring, and incident response.
- The Art of Network Penetration Testing - Book that is a hands-on guide to running your own penetration test on an enterprise network. (early access, published continuously, final release December 2020)

- Spring Boot in Practice - Book that is a practical guide which presents dozens of relevant scenarios in a convenient problem-solution-discussion format.. (early access, published continuously, final release fall 2021)
- Self-Sovereign Identity - A book about how SSI empowers us to receive digitally-signed credentials, store them in private wallets, and securely prove our online identities. (early access, published continuously, final release fall 2021)
- Data Privacy - A book that teaches you to implement technical privacy solutions and tools at scale. (early access, published continuously, final release January 2022)
- Cyber Security Career Guide - Kickstart a career in cyber security by learning how to adapt your existing technical and non-technical skills. (early access, published continuously, final release Summer 2022)
- Secret Key Cryptography - A book about cryptographic techniques and Secret Key methods. (early access, published continuously, final release Summer 2022)
- The Security Engineer Handbook - A short read that discusses the dos and dont's of working in a security team, and the many tricks and tips that can help you in your day-to-day as a security engineer.
- Cyber Threat Hunting - Practical guide to cyber threat hunting.
- Edge Computing Technology and Applications - A book about the business and technical foundation you need to create your edge computing strategy.
- Spring Security in Action, Second Edition - A book about designing and developing Spring applications that are secure right from the start.
- Azure Security - A practical guide to the native security services of Microsoft Azure.
- Node.js Secure Coding: Defending Against Command Injection Vulnerabilities - Learn secure coding conventions in Node.js by executing command injection attacks on real-world npm packages and analyzing vulnerable code.
- Node.js Secure Coding: Prevention and Exploitation of Path Traversal Vulnerabilities - Master secure coding in Node.js with real-world vulnerable dependencies and experience firsthand secure coding techniques against Path Traversal vulnerabilities.

- [Grokking Web Application Security] - A book about building web apps that are ready for and resilient to any attack.

Level 1 of network segmentation: basic segmentation

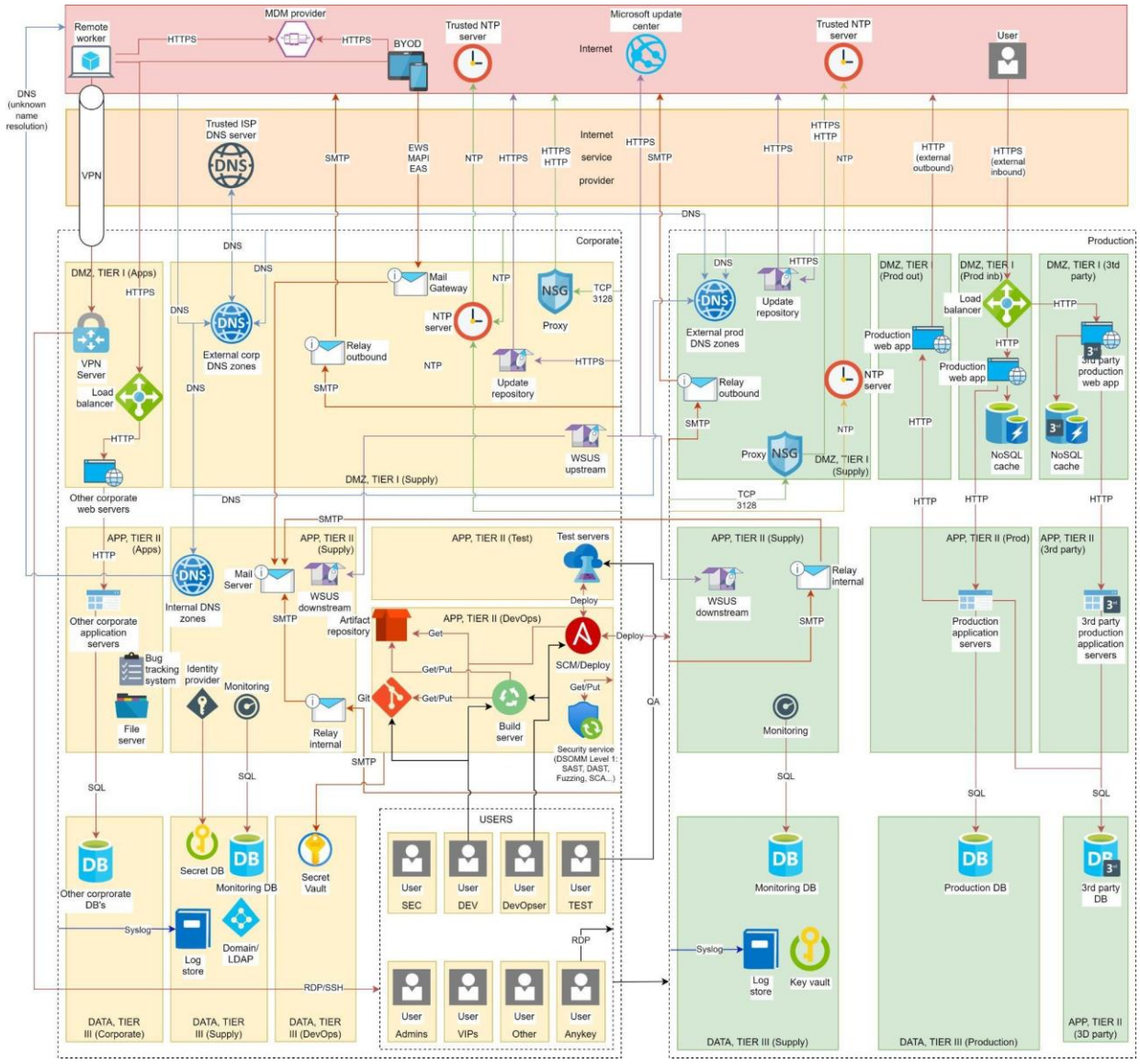


Attack vector protection

Installation the maximum number of information protection tools, real time monitoring suspicious events and immediate response.

OR!

Segmentation according to level 2 requirements



“AT YOUR LOWEST YOU LEARN A LOT….. !!”

--DARSANI. V