Cybersecurity

????

- OpenVAS
- Nessus
- Learning
- Security Websites
- Cyber Attacks
- Suricata
- Snort
- VirusTotal
- Cheat Sheets
- Pentest ????
- Cybersecurity Certificate
- Cybersecurity Tools
- Honey Pot ????

OpenVAS

Installation

Docker

- Docker Hub: https://hub.docker.com/repository/docker/immauss/openvas
- https://immauss.github.io/openvas/

```
mkdir  openvas-data
docker run -d -p 9392:9392 -e PASSWORD="Your admin password here" -v $(pwd)/openvas-data:/data
--name openvas immauss/openvas
```

Kali Linux

- Install OpenVAS on Kali Linux

HowTo

?? Feed

- https://community.greenbone.net/t/how-to-update-keep-the-feed-up-to-date/1431
- https://kenwu0310.wordpress.com/2019/09/17/openvas-%E6%87%89%E7%94%A8-%E6%9B%B4%E6%96%B0%E6%BC%8F%E6%B4%9E%E5%AE%9A%E7%BE%A9/

Nessus

Tutorials

- How to Install and Configure Nessus Vulnerability Scanner on Kali Linux
- How to install, configure and use Nessus Vulnerability Scanner on CentOS 8
- Plugin ??????

?????

- ??????? 90 ????????
- ?? 90 ?????????????????????????????? 16 ??? IP ?????
- ??????? IP ?????????????? High(?) ????????? IP ??????

Installation

Install on RedHat 8

1. ?????? Nessus Essentials ???????
2. ????? Nessus ??? `Nessus-10.1.2-es8.x86_64.rpm`?
3. ??????? `dnf update`?
4. ?? RPM ? `rpm -ivh Nessus-10.1.2-es8.x86_64.rpm`?
5. ???? `https://server.ip:8834`?
6. ????????????
7. ???

Install with the docker

DockerHub: https://hub.docker.com/r/tenableofficial/nessus

```
docker pull tenableofficial/nessus:<version>


docker run --name "nessus-pro" -d -p 8834:8834  -e ACTIVATION_CODE=<activation code> \
-e USERNAME=admin -e PASSWORD=admin tenableofficial/nessus:<version>
```

Update the Nessus ???

Offline

1. ????? Nessus : Download Nessus | Tenable®
   NOTE: ??????? RPM ?????????? RPM ???
2. ??????? Nessus ???????????

? RPM ????

```
rpm -Uvh Nessus-10.4.1-es8.x86_64.rpm
systemctl stop nessusd
systemctl start nessusd
```

Online

```
/opt/nessus/sbin/nessuscli update
```

??????

Nessus Admin > Settings > About

Update the plugins

Online

```
/opt/nessus/sbin/nessuscli update --plugins-only
```

Offline

- Install Nessus and Plugins Offline (with pictures) - InfosecMatter
- Offline Update Page Details (Nessus) (tenable.com)
- Install Plugins Manually (Nessus) (tenable.com)

For ?????

> NOTE: ??? activation code ????????????? plugin ???????????????? activation code???????????? plugin ?????

1. ?????? Activation Code (NOTE: ??????????????????)
2. ??? Nessus ???? Challenge Code
3. ???????????????????? plugin ??????: https://plugins.nessus.org/v2/offline.php
   (TIP: ?????? plugin ??? `all-2.0.tar.gz` ????????????????????)

?? Challenge Code (NOTE: ???????Challenge Code ????)

```
/opt/nessus/sbin/nessuscli fetch --challenge
```

? plugin ???????????

```
/opt/nessus/sbin/nessuscli update all-2.0.tar.gz
```

?? plugin ???

Nessus Admin > Settings > About

- Last Updated: ?????
- Plugin Set: ??????
- Policy Template version: ??????

?????

1. ????????????????????????????????? CPU ??????????????
2. ?? scan ?????? plugin???????????????

??????

??????????

- Generating the Custom URL for downloading plugins for an Offline Nessus Installation (tenable.com)
- Manage Nessus Offline (Nessus) (tenable.com)

FAQ

?? plugin ????

> Error: failed to write decompressed tar archive * Failed to update from all-2.0.new.tar.gz. Invalid manifest.

????????? `/opt/nessus` ??????????

?? plugin #51192(SSL Certificate Cannot Be Trusted)

????????????????????? custom_CA ????????????? Nessus ???

> TIP: ?????? PEM ?? BAS64 ??????????? `-----BEGIN CERTIFICATE-----` ?????? `-----END CERTIFICATE-----` ??????

Nessus Web > Settings > Custom CA

```
-----BEGIN CERTIFICATE-----
...
...
...
-----END CERTIFICATE-----
```

Log4Shell ?????

Nessus ?????????????????????? HTTP ? HTTPS ????????? Plugin 156014 ? 156016 ? Log4Shell ?????

??? Plugin ????? (Callback)???????? Scanner (Nessus server) ? Target (Being scanned hosts) ???????? Tenable Controlled Server?

??????????????????????????????

???????Overview of Callbacks in Log4j Remote Detection Plugins The... | Tenable Connect

Nessus ??????????? (Tenable.io)??????????Log4Shell ?????????? Plugin?

1. Plugin 156014 : ??????????????????????
2. Plugin 155998 : ??????????????????????

???? Plugin ???????????

Learning

Threat Intelligence

Detection & Analysis Tools

- VirusTotal is a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content. VirusTotal also offers additional services and tools for enterprise use.
- Jotti's malware scan is a free service that lets you scan suspicious files with several antivirus programs. There are some limitations to the number of files that you can submit.
- Urlscan.io is a free service that scans and analyzes URLs and provides a detailed report summarizing the URL information.
- MalwareBazaar is a free repository for malware samples. Malware samples are a great source of threat intelligence that can be used for research purposes.
- OpenCTI is an open source platform allowing organizations to manage their cyber threat intelligence knowledge and observables.

AI Cybersecurity

- [pyimagesearch] Build a Network Intrusion Detection System with Variational Autoencoders
- reverse-skills - ?????????????

Security Jobs

Interview

- This blog offers lots of helpful tips, information, and practice scenarios on preparing for technical interviews in the cybersecurity field.

Glossary

- Google-Cybersecurity-Certificate-glossary.docx

Security Websites

CVE Database

- https://www.cve.org/ (Formerly: https://cve.mitre.org)
- https://nvd.nist.gov/ (???????)
- https://euvd.enisa.europa.eu/ (???????)
- https://www.twcert.org.tw/tw/lp-132-1.html (????????)
- https://www.cvedetails.com/
- https://www.kb.cert.org/vuls/ (CERT/CC Vulnerability Notes Database)

Vendor

- RedHat: https://access.redhat.com/security
- iThome: https://www.ithome.com.tw/security
- HPE: https://support.hpe.com/hpesc/public/docDisplay?docId=sd00001284en_us
- IBM: https://www.ibm.com/trust/security-psirt
- VMware: https://www.broadcom.com/support/vmware-security-advisories
- Cisco: https://sec.cloudapps.cisco.com/security/center/publicationListing.x
- HCL Notes: https://support.hcltechsw.com/csm?id=community_topic&sys_id=d1514ac91be8cc5c83cb86e9cd4bcba8
- Ubuntu: https://ubuntu.com/security/cves
- Debian: https://security-tracker.debian.org/tracker/
- Microsoft: https://msrc.microsoft.com/update-guide/vulnerability
- Apple: https://support.apple.com/en-us/HT201222
- Google Cloud: https://cloud.google.com/support/bulletins

Government

- ?????????????? TWCERT/CC
- ???????? (TVN)
- ???????? Virus Check
- ???????????
- ????????????(?)

- ?????????????(?)
- ????? Administration for Cyber Security, moda
- ?????????
- US. CISA
- US. NIST National Vulnerability Database
- CERT-EU

Security Organization

- HelpNetSecurity
- BleepingComputer
- No More Ransom
- Cyberattacks & Data Breaches recent news | Dark Reading
- CSO Online
- Krebs on Security

Security Online Tools

- URL and website scanner - urlscan.io
- VirusTotal - Home
- AbuseIPDB - IP address abuse reports - Making the Internet safer, one IP at a time
- Cisco Talos Intelligence Group - Comprehensive Threat Intelligence
- IBM X-Force Exchange
- Palo Alto Networks URL filtering - Test A Site
- Symantec Sitereview
- IP Address Tools, Network Tools, DNS Tools | IPVoid
- Check if a Website is Malicious/Scam or Safe/Legit | URLVoid
- Web Check

NCHC ????

- Malware Knowledge Base (nchc.org.tw)
- ????????

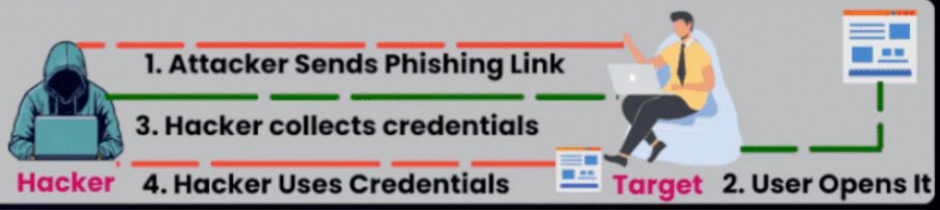
Cyber Attacks

Top 8 Cyber Attacks - 2024

Cyber Security News

1 Phishing Attack

The use of deceptive emails, texts, or websites to gain sensitive information.



2 Ransomware

Malware that can encrypt data and make you pay to get them back.

3 Denial-of-Service (DoS)

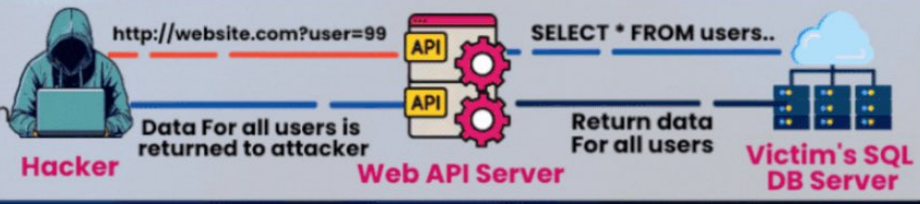
Loading excessive load on a machine or network so that it stops working normally.

4 Man-in-the-Middle (MitM)

Engaging in covert interception and manipulation of communication between two parties without noticing it.

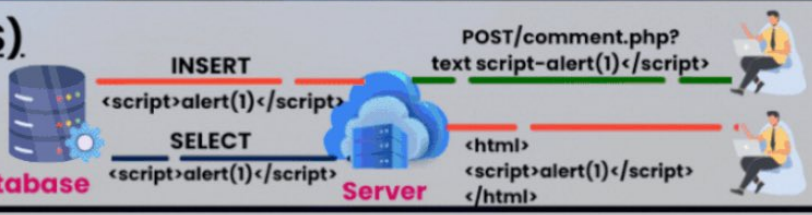
5 SQL Injection

To get the Access to the database, Vulnerabilities in Database queries can be exploited



6 Cross-Site Scripting (XSS)

Putting malicious code into websites that other people visit.

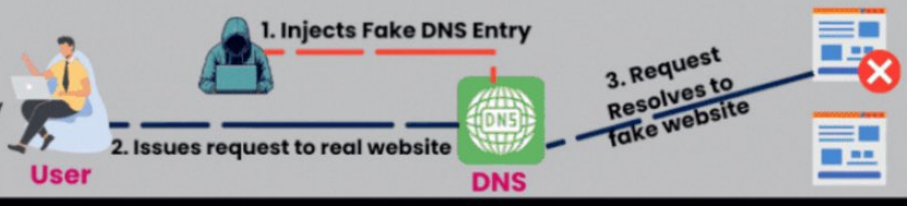


7 Zero-Day Exploits

Attacks take advantage of unknown vulnerabilities before programmers can fix them.

8 DNS Spoofing

Sending DNS queries to malicious sites so that they can be accessed without permission.



Suricata

Introduction

Suricata is a high performance, open source network analysis and threat detection software used by most private and public organizations, and embedded by major vendors to protect their assets.

Suricata is far more than an IDS/IPS.

- Home - Suricata
- ??Suricata???? ??????????? | ??? (netadmin.com.tw)

Suricata features

There are three main ways Suricata can be used:

- **Intrusion detection system** (**IDS**): As a network-based IDS, Suricata can monitor network traffic and alert on suspicious activities and intrusions. Suricata can also be set up as a host-based IDS to monitor the system and network activities of a single host like a computer.
- **Intrusion prevention system** (**IPS**): Suricata can also function as an intrusion prevention system (IPS) to detect and block malicious activity and traffic. Running Suricata in IPS mode requires additional configuration such as enabling IPS mode.
- **Network security monitoring** (**NSM**): In this mode, Suricata helps keep networks safe by producing and saving relevant network logs. Suricata can analyze live network traffic, existing packet capture files, and create and save full or conditional packet captures. This can be useful for forensics, incident response, and for testing signatures. For example, you can trigger an alert and capture the live network traffic to generate traffic logs, which you can then analyze to refine detection signatures.

Signatures (Rules)

Suricata uses **signatures analysis**, which is a detection method used to find events of interest. Signatures consist of three components:

- **Action**: The first component of a signature. It describes the action to take if network or system activity matches the signature. Examples include: alert, pass, drop, or reject.
- **Header**: The header includes network traffic information like source and destination IP addresses, source and destination ports, protocol, and traffic direction.

- **Rule options:** The rule options provide you with different options to customize signatures.

Here's an example of a Suricata signature:


```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established,to_server;
content:"GET"; http_method; sid:12345; rev:3;)
```

Action

Note that the `drop` action also generates an alert, but it drops the traffic. A `drop` action only occurs when Suricata runs in IPS mode.

The `pass` action allows the traffic to pass through the network interface. The pass rule can be used to override other rules. An exception to a drop rule can be made with a pass rule. For example, the following rule has an identical signature to the previous example, except that it singles out a specific IP address to allow only traffic from that address to pass:

```
pass http 172.17.0.77 any -> $EXTERNAL_NET any (msg:"BAD USER-
AGENT";flow:established,to_server;content:!"Mozilla/5.0"; http_user_agent; sid: 12365; rev:1;)
```

The `reject` action does not allow the traffic to pass. Instead, a TCP reset packet will be sent, and Suricata will drop the matching packet. A TCP reset packet tells computers to stop sending messages to each other.

> **Note:** Rule order refers to the order in which rules are evaluated by Suricata. Rules are loaded in the order in which they are defined in the configuration file. However, Suricata processes rules in a different default order: pass, drop, reject, and alert. Rule order affects the final verdict of a packet.

Header

`$HOME_NET` is a Suricata variable defined in `/etc/suricata/suricata.yaml` that you can use in your rule definitions as a placeholder for your local or home network to identify traffic that connects to or from systems within your organization.

Rule options

- The `msg:` option provides the alert text. In this case, the alert will print out the text `“GET on wire”`, which specifies why the alert was triggered.
- The `flow:established,to_server` option determines that packets from the client to the server should be matched. (In this instance, a server is defined as the device responding to the initial SYN packet with a SYN-ACK packet.)
- The `content:"GET"` option tells Suricata to look for the word `GET` in the content of the `http.method` portion of the packet.
- The `sid:12345` (signature ID) option is a unique numerical value that identifies the rule.
- The `rev:3` option indicates the signature's revision which is used to identify the signature's version. Here, the revision version is 3.

Confiuration file

Configuration files let you customize exactly how you want your IDS to interact with the rest of your environment.

Suricata's configuration file is `suricata.yaml`, which uses the YAML file format for syntax and structure.

Log files

There are two log files that Suricata generates when alerts are triggered:

- **eve.json**: The eve.json file is the standard Suricata log file. This file contains detailed information and metadata about the events and alerts generated by Suricata stored in JSON format. For example, events in this file contain a unique identifier called flow_id which is used to correlate related logs or alerts to a single network flow, making it easier to analyze network traffic. The eve.json file is used for more detailed analysis and is considered to be a better file format for log parsing and SIEM log ingestion.
- **fast.log**: The fast.log file is used to record minimal alert information including basic IP address and port details about the network traffic. The fast.log file is used for basic logging and alerting and is considered a legacy file format and is not suitable for incident response or threat hunting tasks.

The main difference between the eve.json file and the fast.log file is the level of detail that is recorded in each. The fast.log file records basic information, whereas the eve.json file contains additional verbose information.

Trigger a custom rule

With a packet capture file

- The `-r sample.pcap` option specifies an input file to mimic network traffic. In this case, the `sample.pcap` file.
- The `-S custom.rules` option instructs Suricata to use the rules defined in the `custom.rules` file.
- The `-k none` option instructs Suricata to disable all checksum checks.

```
sudo suricata -r sample.pcap -S custom.rules -k none
```

Check the logs

```
# For fast.log
cat /var/log/suricata/fast.log

# For eve.log, using jq command to display the JSON format
jq . /var/log/suricata/eve.json | less
jq -c "[.timestamp,.flow_id,.alert.signature,.proto,.dest_ip]" /var/log/suricata/eve.json
jq "select(.flow_id==1200997752018164)" /var/log/suricata/eve.json
```

Resources

- Suricata user guide
- Suricata features
- Rule management
- Rule performance analysis
- Suricata threat hunting webinar
- Introduction to writing Suricata rules
- Eve.json jq examples

Snort

Introduction

Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

- Snort - Network Intrusion Detection & Prevention System
- [Day18] ?????????????Snort ??????? - iT ???::??????????? IT ???? (ithome.com.tw)

VirusTotal

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

URL: https://www.virustotal.com/

Analyze the report

1. **Detection:** This tab provides a list of third-party security vendors and their detection verdicts on an artifact. Detection verdicts include: malicious, suspicious, unsafe, and others. Notice how many security vendors have reported this hash as malicious and how many have not.
2. **Details**: This tab provides additional information extracted from a static analysis of the IoC. Notice the additional hashes associated with this malware like MD5, SHA-1, and more.
3. **Relations**: This tab contains information about the network connections this malware has made with URLs, domain names, and IP addresses. The **Detections** column indicates how many vendors have flagged the URL or IP address as malicious.
4. **Behavior**: This tab contains information related to the observed activity and behaviors of an artifact after executing it in a controlled environment, such as a sandboxed environment. A sandboxed environment is an isolated environment that allows a file to be executed and observed by analysts and researchers. Information about the malware's behavioral patterns is provided through sandbox reports. Sandbox reports include information about the specific actions the file takes when it's executed in a sandboxed environment, such as registry and file system actions, processes, and more. Notice the different types of tactics and techniques used by this malware and the files it created.

> *“* ***Pro tip****: Sandbox reports are useful in understanding the behavior of a file, but they might contain information that is not relevant to the analysis of the file. By default, VirusTotal shows all sandbox reports in the Behavior tab. You can select individual sandbox reports to view. This is helpful because you can view the similarities and differences between reports so that it's easier to identify which behaviors are likely to be associated with the file.*

Determine whether the file is malicious

- The **Vendors' ratio** is the metric widget displayed at the top of the report. This number represents how many security vendors have flagged the file as malicious over all. A file with a high number of vendor flags is more likely to be malicious.

- The **Community Score** is based on the collective inputs of the VirusTotal community. The community score is located below the vendor's ratio and can be displayed by hovering your cursor over the red **X**. A file with a negative community score is more likely to be malicious.
- Under the **Detection** tab, the **Security vendors' analysis** section provides a list of detections for this file made by security vendors, like antivirus tools. Vendors who *have not* identified the file as malicious are marked with a checkmark. Vendors who *have* flagged the file as malicious are marked with an exclamation mark. Files that are flagged as malicious might also include the name of the malware that was detected and other additional details about the file. This section provides insights into a file's potential maliciousness.

Review these three sections to determine if there is a consistent assessment of the file's potential maliciousness such as: a high vendors' ratio, a negative community score, and malware detections in the security vendors' analysis section.

Screenshots

61 / 74

Community Score -209

61/74 security vendors flagged this file as malicious

Reanalyze Similar More

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

Size 430.00 KB | Last Analysis Date 14 hours ago | EXE

peexe spreader checks-user-input runtime-modules service-scan long-sleeps detect-debug-environment direct-cpu-clock-access

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 28+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.flagpro/fragtor | Threat categories trojan | Family labels flagpro fragtor busyice

Security vendors' analysis | Do you want to automate checks?

AhnLab-V3	Malware/Win32.Generic.C4209910	Alibaba	Backdoor:Win32/Kryptik.8648de52
AliCloud	Backdoor:Win/FlagPro.B	ALYac	Trojan.Agent.Flagpro
Antiy-AVL	Trojan[APT]/Win32.Blacktech	Arcabit	Trojan.Fragtor.D5A915
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	HEUR/AGEN.1312459	BitDefender	Gen:Variant.Fragtor.370965
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.flagpro	Cybereason	Malicious.e29b71

61 / 74

Community Score -209

61/74 security vendors flagged this file as malicious

Reanalyze Similar More

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

Size 430.00 KB | Last Analysis Date 14 hours ago | EXE

peexe spreader checks-user-input runtime-modules service-scan long-sleeps detect-debug-environment direct-cpu-clock-access

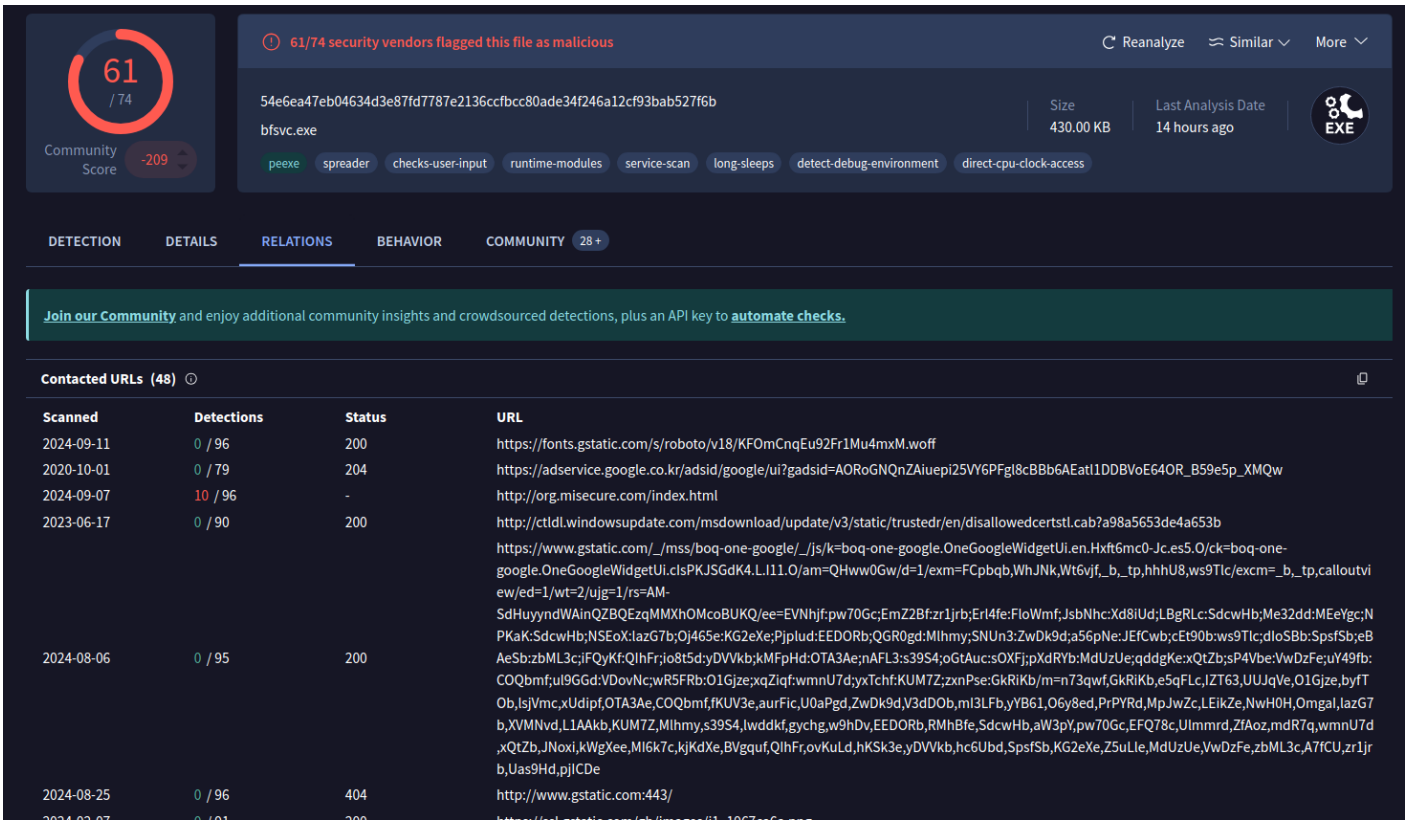
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 28+

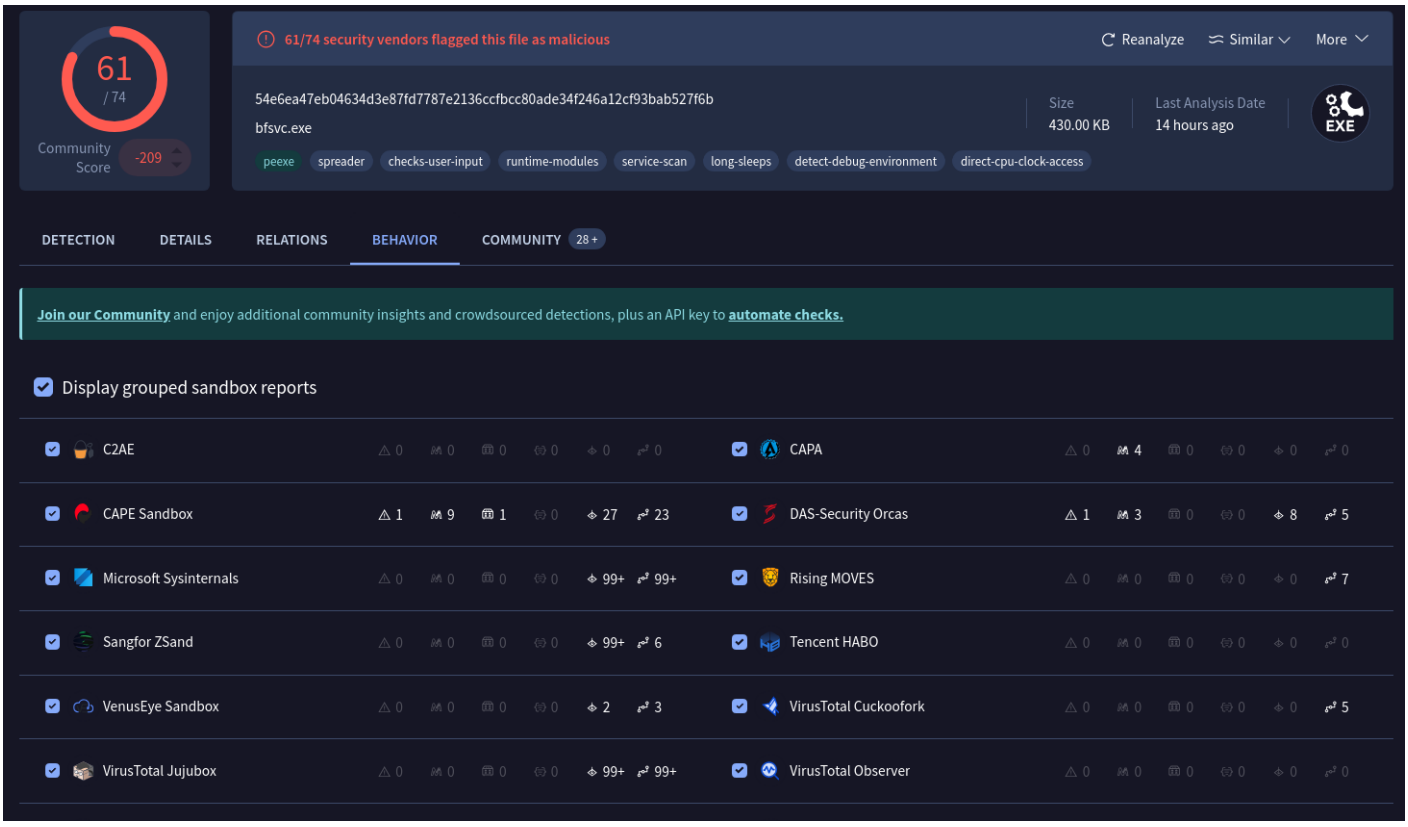
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

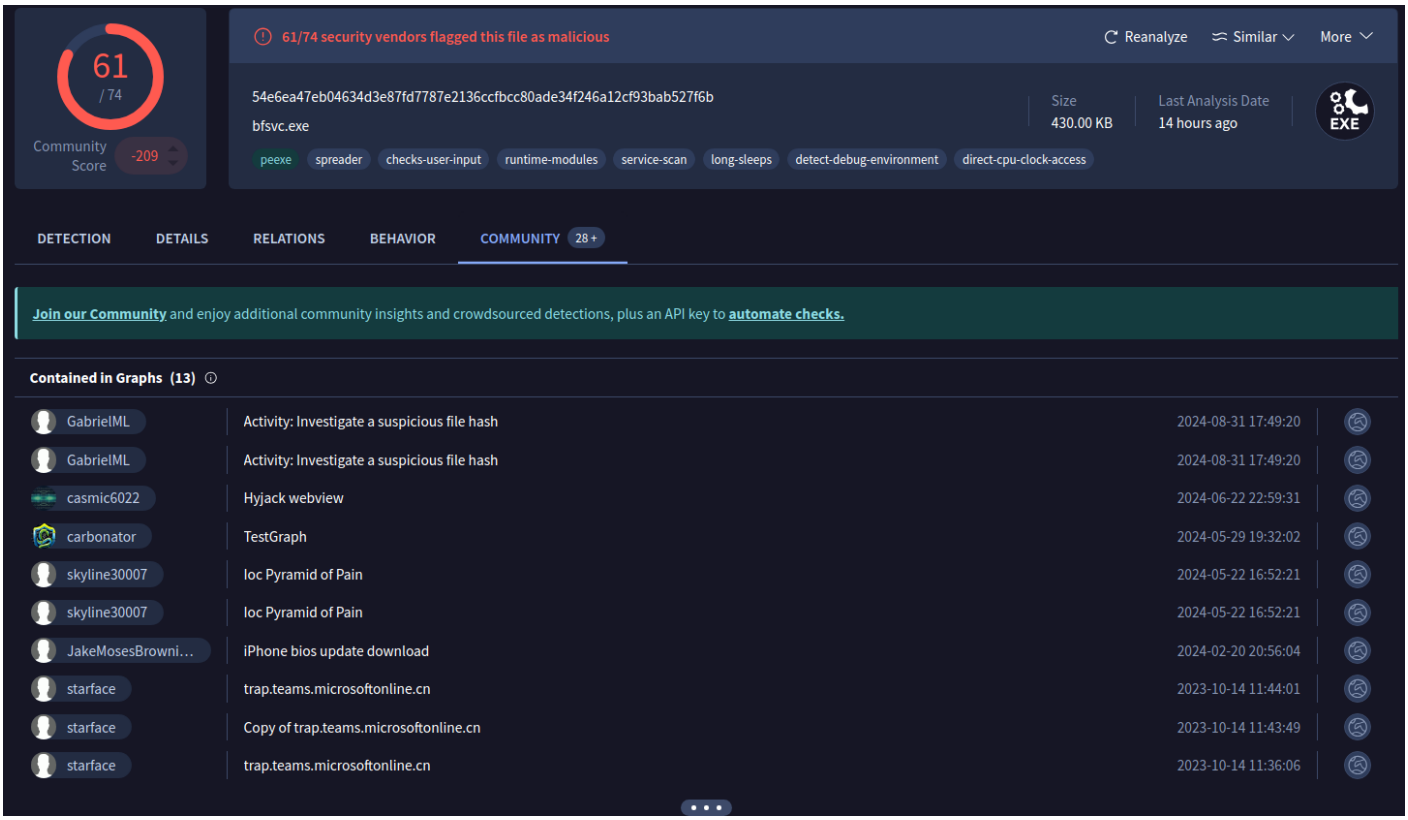
Basic properties

MD5	287d612e29b71c90aa54947313810a25
SHA-1	8f35a9e70dbec8f1904991773f394cd4f9a07f5e
SHA-256	54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
Vhash	045056655d15551023z12z577z305bz2fz
Authentihash	019439328ea87e4559b653ad7df933d20623bdd00d3793abc7ff35e57db24853
Imphash	a59ed1599cc2f8311b215c83c51a2cc4
Rich PE header hash	1f4064adca28866f7447aaf031074807
SSDEEP	6144:CdaRD0n4URr6zIKgDCVh84DLn5X3lWiDSVS1dGSLaYWis:XRonpRroIKgDCY4DLVIW3UiSL4R
TLSH	T13594AD933541C371CA177D7695789AAD4B3F8D3816BAB987B3B83B8F5C303918636902
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) | Win64 Executable (generic) (15.9%) | Win32 Dynamic Link Library (generic) (9.9%) | Win16 NE executable (generic) (7…
DetectItEasy	PE32 | Compiler: EP:Microsoft Visual C/C++ (2008-2010) [EXE32] | Compiler: Microsoft Visual C/C++ (15.00.21022) [LTCG/C++] | Linker: Microsoft Linker (9.00.21022) | To…
Magika	PEBIN
File size	430.00 KB (440320 bytes)

History


61
/ 74
Community Score
-209
61/74 security vendors flagged this file as malicious
Reanalyze
Similar
More
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
bfsvc.exe
peexe
spreader
checks-user-input
runtime-modules
service-scan
long-sleeps
detect-debug-environment
direct-cpu-clock-access
Size
430.00 KB
Last Analysis Date
14 hours ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 28+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Contacted URLs (48)
Scanned
Detections
Status
URL
2024-09-11
0 / 96
200
https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff
2020-10-01
0 / 79
204
https://adservice.google.co.kr/adsid/google/ui?gadsid=AORoGNQnZAiuepi25VY6PFgl8cBBb6AEatl1DDBVoE64OR_B59e5p_XMQw
2024-09-07
10 / 96
-
http://org.misecure.com/index.html
2023-06-17
0 / 90
200
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?a98a5653de4a653b
2024-08-06
0 / 95
200
https://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en.Hxft6mc0-Jc.es5.O/ck=boq-one-google.OneGoogleWidgetUi.clsPKJSGdK4.L.I11.O/am=QHww0Gw/d=1/exm=FCpbqb,WhJNk,Wt6vjf,_b,_tp,hhhU8,ws9Tlc/excm=_b,_tp,calloutview/ed=1/wt=2/ujg=1/rs=AM-SdHuyyndWAinQZBQEzqMMXhOMcoBUKQ/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:MIhmy;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:wmnU7d;yxTchf:KUM7Z;zxnPse:GkRiKb/m=n73qwf,GkRiKb,e5qFLc,IZT63,UUJqVe,O1Gjze,byfTOb,lsjVmc,xUdipf,OTA3Ae,COQbmf,fKUV3e,aurFic,U0aPgd,ZwDk9d,V3dDOb,mI3LFb,yYB61,O6y8ed,PrPYRd,MpJwZc,LEikZe,NwH0H,Omgal,lazG7b,XVMNvd,L1AAkb,KUM7Z,MIhmy,s39S4,lwddkf,gychg,w9hDv,EEDORb,RMhBfe,SdcwHb,aW3pY,pw70Gc,EFQ78c,Ulmmrd,ZfAoz,mdR7q,wmnU7d,xQtZb,JNoxi,kWgXee,MI6k7c,kjKdXe,BVgquf,QIhFr,ovKuLd,hKSk3e,yDVVkb,hc6Ubd,SpsfSb,KG2eXe,Z5uLle,MdUzUe,VwDzFe,zbML3c,A7fCU,zr1jrb,Uas9Hd,pjICDe
2024-08-25
0 / 96
404
http://www.gstatic.com:443/


61
/ 74
Community Score
-209
61/74 security vendors flagged this file as malicious
Reanalyze
Similar
More
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
bfsvc.exe
peexe
spreader
checks-user-input
runtime-modules
service-scan
long-sleeps
detect-debug-environment
direct-cpu-clock-access
Size
430.00 KB
Last Analysis Date
14 hours ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 28+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Display grouped sandbox reports
C2AE
CAPA
CAPE Sandbox
DAS-Security Orcas
Microsoft Sysinternals
Rising MOVES
Sangfor ZSand
Tencent HABO
VenusEye Sandbox
VirusTotal Cuckoofork
VirusTotal Jujubox
VirusTotal Observer


61
/ 74
Community Score
-209
61/74 security vendors flagged this file as malicious
Reanalyze
Similar
More
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
bfsvc.exe
peexe
spreader
checks-user-input
runtime-modules
service-scan
long-sleeps
detect-debug-environment
direct-cpu-clock-access
Size
430.00 KB
Last Analysis Date
14 hours ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 28 +
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Contained in Graphs (13)
GabrielML
Activity: Investigate a suspicious file hash
2024-08-31 17:49:20
GabrielML
Activity: Investigate a suspicious file hash
2024-08-31 17:49:20
casmic6022
Hyjack webview
2024-06-22 22:59:31
carbonator
TestGraph
2024-05-29 19:32:02
skyline30007
Ioc Pyramid of Pain
2024-05-22 16:52:21
skyline30007
Ioc Pyramid of Pain
2024-05-22 16:52:21
JakeMosesBrowni…
iPhone bios update download
2024-02-20 20:56:04
starface
trap.teams.microsoftonline.cn
2023-10-14 11:44:01
starface
Copy of trap.teams.microsoftonline.cn
2023-10-14 11:43:49
starface
trap.teams.microsoftonline.cn
2023-10-14 11:36:06

Cheat Sheets

Cybersecurity Acronyms

CYBERSECURITY ACRONYMS (PART 1)

@SECURITYTRYBEE

*CIA - CONFIDENTIALITY, INTEGRITY, AVAILABILITY

*IDS - INTRUSION DETECTION SYSTEM

*IPS - INTRUSION PREVENTION SYSTEM

*WAF - WEB APPLICATION FIREWALL

*PII - PERSONAL IDENTIFIABLE INFORMATION

*DOS - DENIAL OF SERVICE

*DDOS - DISTRIBUTED DENIAL OF SERVICE

*DNS - DOMAIN NAME SYSTEM

*ZTA - ZERO TRUST ARCHITECTURE

*NAT - NETWORK ADDRESS TRANSLATION

*CTF - CAPTURE THE FLAG

*ACL - ACCESS CONTROL LIST

*CDN - CONTENT DELIVERY NETWORK

*CVE - COMMON VULNERABILITIES AND EXPOSURES

Common types of password attacks

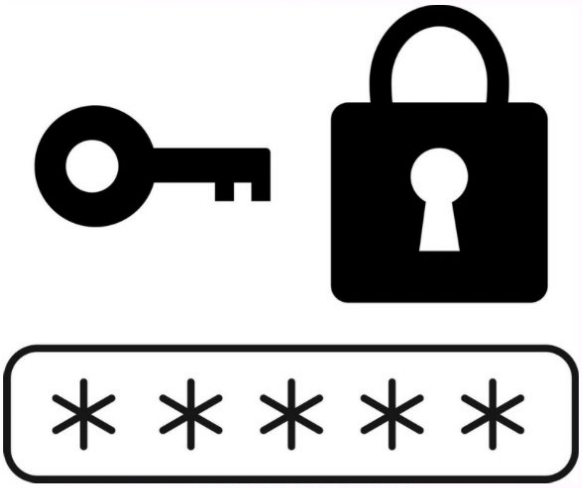
SECURITY TRYBE

COMMON TYPES OF PASSWORD ATTACKS

Brute Force Attack:
Hackers use software to guess various password combinations until they crack the code.

Keylogger:
Malicious software records keystrokes, capturing passwords as users type.

Social Engineering:
Hackers create fake websites resembling legitimate login pages. When users enter their information, it gets recorded.

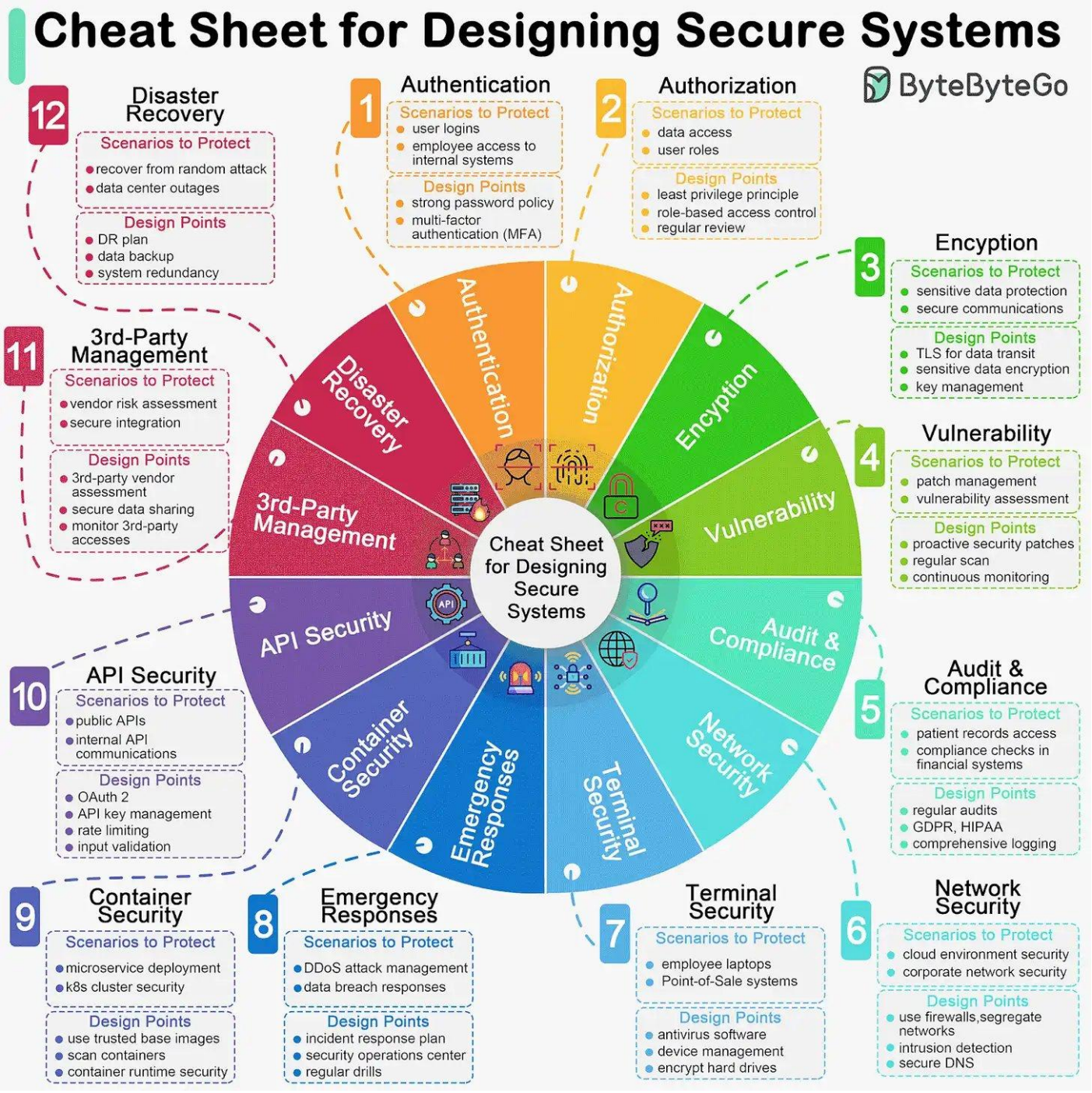


Rainbow Table Attack:
This type of password crack uses pre-computed table of all possible hashes of all possible passwords

Credential Stuffing:
Cybercriminals exploit stolen credentials (such as usernames and passwords) to break into accounts.

Dictionary Attack:
Similar to brute force attacks, dictionary attacks rely on common phrases or dictionary words as passwords.

Designing Secure Systems



Risk Management Framework

Domain 1: Security & Risk Management

CISSP Cheat Sheet Series

CIA Triad

Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Note – Encryption (At transit – TLS) (At rest - AES – 256)
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Availability	Ensuring timely and reliable access to and use of information by authorized users.

***Citation:** https://www.isc2.org/Certifications/CISSP/CISSP-Student-Glossary

Achieving CIA - Best Practices

Separation of Duties	Mandatory Vacations	Job Rotation	Least Privileges	Need to know	Dual Control

Availability Measuring Metrics	RTO/MTD/RPO, MTBF, SLA

D.A.D.

Disclosure	Alteration	Destruction
Opposite of Confidentiality	Opposite of Integrity	Opposite of Availability

IAAAA

Identification	Unique user identification
Authentication	Validation of identification
Authorization	Verification of privileges and permissions for authenticated user
Accountability	Only authorized users are accessing and use the system accordingly
Auditing	Tools, processes, and activities used to achieve and maintain compliance

Plans

Type	Duration	Example
Strategic Plan	up to 5 Years	Risk Assessment
Tactical Plan	Maximum of 1 year	Project budget, staffing etc
Operational Plan	A few months	Patching computers Updating AV signatures Daily network administration

Protection Mechanisms

Layering	Abstractions	Data Hiding	Encryption

Data classification

Entails analyzing the data that the organization retains, determining its importance and value, and then assigning it to a category.

Risk Management

- No risk can be completely avoided .
- Risks can be minimized and controlled to avoid impact of damages.
- Risk management is the process of identifying, examining, measuring, mitigating, or transferring risk

***Citation:** https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/

Solution – Keep risks at a tolerable and acceptable level.
Risk management constraints – Time, budget

Risk Terminology

Asset	Anything of value to the company.
Vulnerability	A weakness; the absence of a safeguard
Threat	Things that could pose a risk to all or part of an asset
Threat Agent	The entity which carries out the attack
Exploit	An instance of compromise
Risk	The probability of a threat materializing

***Citation:** https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/

Risk Management Frameworks

Preventive Ex ISO 27001	Deterrent Ex ISO 27000	Detective	Corrective	Recovery
Security Policies	Security Personnel	Logs	Alarms	Backups
Security Cameras	Guards	Security Cameras	Antivirus Solutions	Server Clustering
Callback	Security Cameras	Intrusion Detection Systems	Intrusion Detection Systems	Fault Tolerant Drive Systems
Security Awareness Training	Separation of Duties	Honey Pots	Business Continuity Plans	Database Shadowing
Job Rotation	Intrusion Alarms	Audit Trails		Antivirus Software
Encryption	Awareness Training	Mandatory Vacations		
Data Classification	Firewalls			
Smart Cards	Encryption			

Risk Framework Types

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Risk Management Life Cycle

Assessment	Analysis	Mitigation / Response
Categorize, Classify & Evaluate Assets	Qualitative vs Quantitative	Reduce, Transfer, Accept
as per NIST 800-30:	Qualitative – Judgments	Reduce / Avoid
System Characterization	Quantitative – Main terms	Transfer
Threat Identification	AV – Asset Value	Accept / Reject
Vulnerability Identification	EF – Exposure Factor	
Control Analysis	ARO – Annual Rate of Occurrence	
Likelihood Determination	Single Loss Expectancy = AV * EF	

Security Governance

The 6 Steps of the Risk Management Framework

Categorize

Select

Malware Types

Malware Types

CYVEER
www.cyveer.com

Malware Type	Function	Impact
Virus	Self-replicates, infects files	Data corruption, system damage
Worm	Self-spreads across networks	Network disruption, resource depletion
Trojan Horse	Disguises as legit software	Data theft, system control
Ransomware	Encrypts files, demands payment	Data loss, financial loss
Spyware	Secretly monitors user activity	Privacy violation, data theft
Adware	Displays unwanted ads	Annoyance, performance degradation
Rootkit	Hides malicious software	Unauthorized access, persistent threats
Keylogger	Records keystrokes	Credential theft, data breach
Fileless Malware	Runs from memory	Difficult to detect, stealthy attacks
Cryptojacker	Mines cryptocurrency	Performance issues, resource hijacking
Botnet	Creates network of infected devices	DDoS attacks, spam distribution
Logic Bomb	Executes code on trigger	Data destruction, system damage
Wiper	Destroys data	Irreversible data loss
Scareware	Falsely claims infection	Financial loss, system compromise
Malvertising	Spreads malware via ads	Wide-spread infection
Backdoor	Bypasses authentication	Unauthorized access

www.cyveer.com

Pentest ????

?????Penetration Test?????? Pen Test
??
??

PentAGI

Advanced AI-Powered Penetration Testing

- PentAGI - Advanced AI-Powered Penetration Testing
- GitHub: https://github.com/vxcontrol/pentagi

Search Engines

#SEARCH ENGINES FOR PENTESTERS

1. shodan.io (Server)
2. google.com (Dorks)
3. wigle.net (WiFi Networks)
4. grep.app (Codes Search)
5. app.binaryedge (Threat Intelligence)
6. onyphe.io (Server)
7. viz.greynoise.io (Threat Intelligence)
8. censys.io (Server)
9. hunter.io (Email Addresses)
10. fofa.info (Threat Intelligence)
11. zoomeye.org (Threat Intelligence)
12. leakix.net (Threat Intelligence)
13. intelx.io (OSINT)
14. app.netlas.io (Attack Surface)
15. searchcode.com (Codes Search)
16. urlscan.io (Threat Intelligence)
17. publicwww.com (Codes Search)
18. fullhunt.io (Attack Surface)
19. socradar.io (Threat Intelligence)
20. binaryedge.io (Attack Surface)
21. ivre.rocks (Server)
22. crt.sh (Certificate Search)
23. vulners.com (Vulnerabilities)
24. pulsedive.com (Threat Intelligence)

Cybersecurity Certificate

Google Cybersecurity Certificates (GCC)

Google ????

- ????????????
- ???????? - Google ????
- Google Cybersecurity Certificate - Grow with Google

Qualify for the following jobs:

- Cybersecurity analyst
- Information security analyst
- Security analyst
- IT security analyst
- SOC analyst
- Cyber defense analyst

You'll learn about:

- Programming for cybersecurity tasks
- Frameworks and controls that inform security operations
- Using security information and event management (SIEM) tools for cybersecurity
- Detecting and responding to incidents using an intrusion detection system
- Performing packet capture and analysis
- Using AI to boost productivity

Cybersecurity Tools

Seach More

- 10 Top Open Source Penetration Testing Tools
- OSV-Scanner
- 5 Tools to Scan a Linux Server for Malware and Rootkits (tecmint.com)
- Hottest cybersecurity open-source tools of the month: May 2025 - Help Net Security

Online Tools

??	????
shodan.io	????????????????
censys.io	?????????????????????
hunter.io	?????????????????????
fullhunt.io	????????????????
onyphe.io	?????????????????????
socradar.io	?????????????????????
binaryedge.io	?????????????????
ivre.rocks	?????????
crt.sh	?????SSL/TLS???????
vulners.com	?????????????????
publicwww.com	???????,?????????????????
pulsedive.com	?????????????????
intelx.io	???????(OSINT)????????
wigle.net	?????????????
viz.greynoise.io	?????????????????????

Vulnerability Scanner

- OpenVAS
- Nessus
- RustScan : The Modern Port Scanner

- Vuls : Agentless Vulnerability Scanner for Linux/FreeBSD
  - GitHub: https://github.com/future-architect/vuls
  - Vuls: A Free, Open Source Vulnerability Scanner for Linux - The New Stack
  - Vuls: Open-source agentless vulnerability scanner - Help Net Security

Tools

-Wazuh

The Open Source Security Platform

- https://wazuh.com/
- YT: this Cybersecurity Platform is FREE
- YT: you need this FREE CyberSecurity tool
- YT: Wazuh Open Source SIEM Tutorial - YouTube
- YT: Wazuh! Powerful, Open Source Endpoint Security Monitoring!

-Web Check

All-in-one OSINT tool for analysing any website

- Web Check (web-check.xyz)
- GitHub: https://github.com/Lissy93/web-check

-OWASP: Nettacker

Automated Penetration Testing Framework (????????)

- OWASP/Nettacker: Automated Penetration Testing Framework

-WAF: Web Application Firewall

- GoTestWAF
- Test and evaluate your WAF before hackers
- SafeLine - A self-hosted WAF(Web Application Firewall)
  - YT: SafeLine: A Feature-Rich WAF with a Catch (or Two)
- waf-checker

-Pi-Alert: WiFi/LAN ??????

- Pi.Alert
- [Video] Pi Alert - Open Source, Self Hosted, Network Device Change Notification and Intrusion Detection

-WatchYourLAN

- GitHub: https://github.com/aceberg/WatchYourLAN

-ntopng

Network traffic monitor

- ntopng – ntop
- YT: NTopNG - A Free, Open Source, Self Hosted, Network Monitoring and Analysis Tool. - YouTube

-ImHex: Hex Editor

A Hex Editor for Reverse Engineers, Programmers and people who value their retinas when working at 3 AM

- GitHub: https://github.com/WerWolv/ImHex/

-OSSIEM

Open Source SIEM Stack, Wazuh + Graylog + Velociraptor + Copilot

- GitHub: https://github.com/socfortress/OSSIEM

-Fishing Test

- pfish - ?????????

-CISO Assistant

CISO Assistant is a one-stop-shop for GRC, covering Risk, AppSec and Audit Management

- GitHub: https://github.com/intuitem/ciso-assistant-community

-MISP

MISP (Malware Information Sharing Platform)

- https://www.misp-project.org/

Cybersecurity Linux Distro.

- TOP VIRTUAL MACHINES FOR CYBERSECURITY PROFESSIONALS | by Flavio Queiroz | CTI Flash Insights | Medium
- Kali Linux
- ParrotOS
- BlackArch Linux ????? Arch Linux ?????????????????????????????????? 2866 ??????????????????????????BlackArch Linux ???? Arch ?????

Honey Pot ????

Introduction

- ????????Honey Pot?? | iThome
- ????????????? ???HoneyPot????Bot?? | iThome

Self-hosted Services

- Awesome-Honeypot - Cowrie Honeypot with Elasticsearch