

## Experiment 1

### Title

**“Cyber-kill chain: Reconnaissance and Information Gathering : OSINT, Breached credentials, Subdomain brute forcing, Directory scanning.”**

### Objective:

To understand and perform various techniques used in the reconnaissance phase of the cyber-kill chain, including OSINT, analyzing breached credentials, subdomain brute forcing, and directory scanning.

### Requirements:

Kali Linux/Ubuntu, Internet access, snort, theHarvester, Sherlock, Hunter.io, Have I Been Pwned API, Sublist3r, Gobuster, Dirb.

### OSINT (Open-Source Intelligence)

**Ojective:** This involves gathering data from publicly available sources about a target.

**Tools:** theHarvester, Sherlock, Hunter.io

### 1. Using “theHarvester”

- Open a terminal in linux os
- Run the command `>> theHarvester -d https://bmsit.ac.in/ -l 500 -b a`
- Analyze the output for useful information.

```
File Actions Edit View Help
[*] ASNS found: 2
AS14001
AS10500

[*] Interesting URLs found: 6
http://bms.bmsit.ac.in
http://cg.bmsit.ac.in/
http://modle.bmsit.ac.in/
https://bmsit.ac.in/
https://bmsit.ac.in/7
https://ipc.bmsit.ac.in/

[*] LinkedIn links found: 0

[*] IPs found: 38
53.127.171.233
53.127.244.147
53.232.62.252
53.232.253.106
53.232.62.217
53.232.76.102
53.232.253.81
53.197.207.178
53.197.214.0
53.197.235.123
53.68.235.80
54.97.166.101
54.250.217.115
54.230.217.83
54.251.53.83
54.227.11.29
54.105.56.191
54.217.44.243
54.217.3.211
54.72.19.87
54.72.37.151
54.199.189.153
54.199.110.153
54.199.111.153
54.7.99.56
54.168.247.115
54.83.23.240
54.185.199.199
54.199.181.187
54.18.215.94
54.66.122.218
54.151.57.158
54.254.192.172
54.76.21.61
54.76.21.98

[*] No emails found.

[*] Hosts found: 51
admission.bmsit.ac.in
admission.bmsit.ac.in:53.232.62.217
alumni.bmsit.ac.in
alumni.bmsit.ac.in:183.187.238.11
alumni.bmsit.ac.in:ec2-54-254-193-172.ap-southeast-1.compute.amazonaws.com
alumni.bmsit.ac.in:hs.vaave.co
alumni.bmsit.ac.in:hs.vaave.co
bmsit.bmsit.ac.in
bmsit.bmsit.ac.in
bmsit.bmsit.ac.in:53.127.244.147
cdn.bmsit.ac.in
```

## 2. Using "Sherlock"

- Clone the Sherlock repository from Git hub
- >>sudo git clone https://github.com/sherlock-project/sherlock.git
- >>cd sherlock
- >>sudo python3 -m pip install -r requirements.txt
- >>sudo python3 sherlock username

```
(kali@kali)-[~]
$ sherlock bmsit
/home/kali/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (2.0.7) or chardet (5.2.0)/charset_normalizer (2.0.12) doesn't match a supported version
warnings.warn("urllib3 ({}), or chardet ({}), or charset_normalizer ({}), doesn't match a supported version".format(urllib3.__version__, chardet.__version__, charset_normalizer.__version__), RequestsDependencyWarning)
[*] Checking username bmsit on:


[+] Academia.edu: https://independent.academia.edu/bmsit
[+] AllMyLinks: https://allmylinks.com/bmsit
[+] Amino: https://aminoapps.com/u/bmsit
[+] Archive.org: https://archive.org/details/@bmsit
[+] ArtStation: https://www.artstation.com/bmsit
[+] AskFM: https://ask.fm/bmsit
[+] AudioJungle: https://audiojungle.net/user/bmsit
[+] BitBucket: https://bitbucket.org/bmsit/
[+] Blogger: https://bmsit.blogspot.com
[+] Disqus: https://disqus.com/bmsit
[+] Docker Hub: https://hub.docker.com/u/bmsit/
[+] Dribbble: https://dribbble.com/bmsit
[+] Freelancer: https://www.freelancer.com/u/bmsit
[+] GitHub: https://www.github.com/bmsit
[+] GitLab: https://gitlab.com/bmsit
[+] HackTheBox: https://forum.hackthebox.eu/profile/bmsit
[+] HackenProof (Hackers): https://hackenproof.com/hackers/bmsit
[+] HackerOne: https://hackerone.com/bmsit
[+] HudsonRock: https://cavalier.hudsonrock.com/api/json/v2/osint-tools/search-by-username?username=bmsit
[+] Issuu: https://issuu.com/bmsit
[+] Kick: https://kick.com/bmsit
[+] LeetCode: https://leetcode.com/bmsit
[+] LibraryThing: https://www.librarything.com/profile/bmsit
[+] Lichess: https://lichess.org/@/bmsit
[+] Naver: https://blog.naver.com/bmsit
[+] ProductHunt: https://www.producthunt.com/@bmsit
[+] Roblox: https://www.roblox.com/user.aspx?username=bmsit
[+] Scribd: https://www.scribd.com/bmsit
[+] Slack: https://bmsit.slack.com
[+] SlideShare: https://slideshare.net/bmsit
[+] Smule: https://www.smule.com/bmsit
[+] TLDR Legal: https://tldrlegal.com/users/bmsit/
[+] ThemeForest: https://themeforest.net/user/bmsit
[+] VSCO: https://vSCO.co/bmsit
[+] Venmo: https://account.venmo.com/u/bmsit
[+] Vero: https://vero.co/bmsit
[+] WordPress: https://bmsit.wordpress.com/
[+] Xbox Gamertag: https://xboxgamertag.com/search/bmsit
[+] Last.fm: https://last.fm/user/bmsit
[+] Mastodon.cloud: https://mastodon.cloud/@bmsit

[*] Search completed with 40 results

(kali@kali)-[~]
$
```

### 3.Using “Hunter.io”

- Sign up for an API key on hunter.io
- Curl“https://api.hunter.io/v2/domain.search?domain=example.com&api\_key=YOUR\_API\_KEY”
- Analyze the output for useful email address.



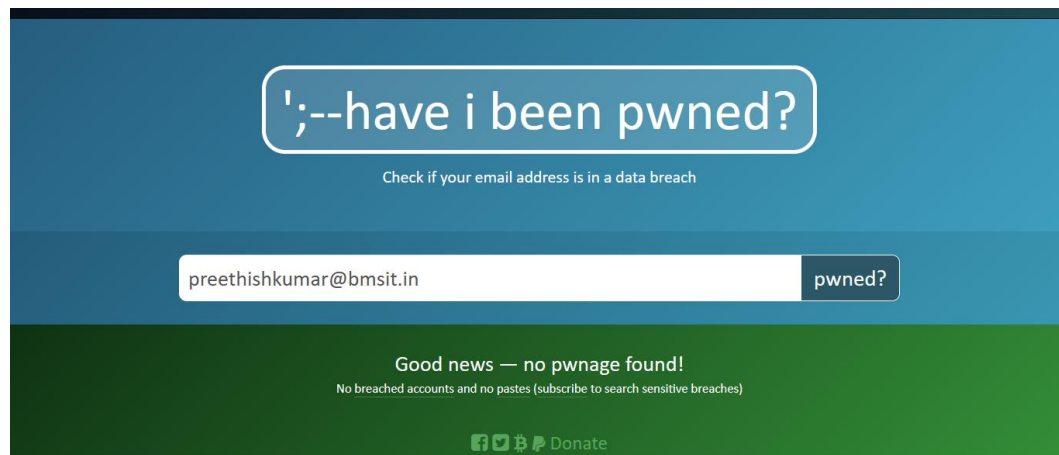
```
kali@kali: ~/Desktop
$ curl "https://api.hunter.io/v2/domain.search?domain=amazon.in&api_key=86ff..." 30cb"
{
  "data": {
    "domain": "amazon.in",
    "disposable": false,
    "webmail": false,
    "accept_all": true,
    "pattern": "{first}",
    "organization": "Amazon",
    "description": "Amazon is an e-commerce giant that offers a wide range of products and services through its online platform.",
    "industry": "Software Development",
    "twitter": "https://twitter.com/amazonminity",
    "facebook": "https://facebook.com/amazonminity",
    "linkedin": "https://linkedin.com/company/amazon",
    "instagram": "https://instagram.com/amazonminity",
    "youtube": null,
    "technologies": [],
    "country": "US",
    "state": "WA",
    "city": "Seattle",
    "postal_code": null,
    "street": null,
    "headcount": "10001+",
    "company_type": "public company",
    "emails": [
      {
        "value": "amit@amazon.in",
        "type": "personal",
        "confidence": 94,
        "sources": [
          {
            "domain": "technofino.in",
            "uri": "http://technofino.in/community/threads/amazon-laptop-damage-scam.24276",
            "extracted_on": "2024-04-13",
            "last_seen_on": "2024-09-22",
            "still_on_page": true
          },
          {
            "domain": "domaininfofree.com",
            "uri": "http://domaininfofree.com/domain-traffic/amazon.in",
            "extracted_on": "2023-05-14",
            "last_seen_on": "2023-12-20",
            "still_on_page": true
          },
          {
            "domain": "domaininfofree.com",
            "uri": "http://domaininfofree.com/email-by-domain",
            "extracted_on": "2023-03-17",
            "last_seen_on": "2023-04-18",
            "still_on_page": false
          },
          {
            "domain": "domaininfofree.com",
            "uri": "http://domaininfofree.com",
            "extracted_on": "2023-03-15",
            "last_seen_on": "2023-03-15",
            "still_on_page": false
          }
        ]
      },
      {
        "first_name": "Ami",
        "last_name": "Traore",
        "position": "fulfillment associate",
        "seniority": null,
        "department": null,
        "linkedin": "https://www.linkedin.com/in/ami-traore-a474bb124",
        "twitter": null,
        "phone_number": null,
        "verification": {
          "date": "2024-09-16",
          "status": "accept_all"
        }
      }
    ],
    "value": "payments-investigate@amazon.in",
    "type": "personal",
    "confidence": 93,
    "sources": [
      {
        "domain": "bbs.ichuanglan.com",
        "uri": "http://bbs.ichuanglan.com/thread-310636-1-1.html",
        "extracted_on": "2024-09-21",
        "last_seen_on": "2024-09-24",
        "still_on_page": true
      },
      {
        "domain": "m.mjzj.com",
        "uri": "http://m.mjzj.com/article/48432",
        "extracted_on": "2024-09-24",
        "last_seen_on": "2024-09-24",
        "still_on_page": true
      },
      {
        "domain": "pinkeman.com",
        "uri": "http://pinkeman.com/news/rules/2194.html",
        "extracted_on": "2024-09-22",
        "last_seen_on": "2024-09-24",
        "still_on_page": true
      },
      {
        "domain": "yimisoftware.com",
        "uri": "http://yimisoftware.com/article/detail/2328",
        "extracted_on": "2024-09-22",
        "last_seen_on": "2024-09-22",
        "still_on_page": true
      }
    ]
  }
}
```

## Analyzing Breached Credentials

**Objective:** To find and analyze breached credentials using online databases and APIs.

**Tools:** Have I Been Pwned

- Access <https://haveibeenpwned.com/>
- Enter the email address
- Analyse the results



## Subdomain Brute Forcing

**Objective:** To discover subdomains of the target domain using brute-forcing techniques.

**Tools:** Sublist3r

- Open a terminal in linux
- `sublist3r -d bmsit.ac.in -o subdomains.txt`

```
File Actions Edit View Help
sublist3r

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 792
  Download size: 620 kB
  Space needed: 1,944 kB / 62.9 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 sublist3r all 1.1-4 [620 kB]
  fetched 620 kB in 1s (605 kB/s)
Selecting previously unselected package sublist3r.
(Reading database ... 392084 files and directories currently installed.)
Preparing to unpack .../sublist3r_1.1-4_all.deb ...
Unpacking sublist3r (1.1-4) ...
Setting up sublist3r (1.1-4) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.1-1) ...

(kali@kali) ~ - [Desktop]
$ sublist3r -d bmsit.ac.in -o subdomains.txt
/home/kali/.local/lib/python3.11/site-packages/requests/_init_.py:102: RequestsDependencyWarning: urllib3 (1.26.18) or chardet (5.2.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported version".format(urllib3.__version__,
Sublist3r
# Coded By Ahmed Aboul-El* @aboul3la

[+] Enumerating subdomains now for bmsit.ac.in
[+] Searching now in Baidu..
[+] Searching now in Yahoo..
[+] Searching now in Google..
[+] Searching now in Bing..
[+] Searching now in Ask..
[+] Searching now in Netcraft..
[+] Searching now in DNSDumpster..
[+] Searching now in VirusTotal..
[+] Searching now in ThreatCrowd..
[+] Searching now in SSL Certificates..
[+] Searching now in PassiveDNS..
[+] Error: RequestsException: now is blocking our requests
[+] Saving results to file: subdomains.txt
[+] Total Unique Subdomains Found: 22
admission.bmsit.ac.in
alumni.bmsit.ac.in
biceps.bmsit.ac.in
bims.bmsit.ac.in
cds.bmsit.ac.in
cg.bmsit.ac.in
clerk.bmsit.ac.in
dis.bmsit.ac.in
feedback360.bmsit.ac.in
fms.bmsit.ac.in
grievance.bmsit.ac.in
innovation.bmsit.ac.in
library.bmsit.ac.in
moodle.bmsit.ac.in
motorheads.bmsit.ac.in
nrcit2018.bmsit.ac.in
pbas.bmsit.ac.in
projects.bmsit.ac.in
register.bmsit.ac.in
sanskrit.bmsit.ac.in
stisba.bmsit.ac.in
wins.bmsit.ac.in
```



## Directory Scanning

**Objective:** To identify directories and files on a web server using scanning tools.

**Tools :** Gobuster, Dirb

### Using Gobuster

- Open a terminal in Linux
- gobuster dir -u <https://bmsit.ac.in/> -w /usr/share/wordlists/dirb/common.txt
- Analyze the output for discovered directories.

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)~[~/Desktop]
$ gobuster dir -u https://bmsit.ac.in -w /usr/share/wordlists/dirb/common.txt -s '200,204,301,403' -b ''

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: https://bmsit.ac.in
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,403
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./.history (Status: 403) [Size: 178]
./.config (Status: 403) [Size: 178]
./.cvs (Status: 403) [Size: 178]
./.cvsignore (Status: 403) [Size: 178]
./.hta (Status: 403) [Size: 178]
./.forward (Status: 403) [Size: 178]
./.git/HEAD (Status: 403) [Size: 178]
./.bash_history (Status: 403) [Size: 178]
./.cache (Status: 403) [Size: 178]
./.bashrc (Status: 403) [Size: 178]
./.htaccess (Status: 403) [Size: 178]
./.htpasswd (Status: 403) [Size: 178]
./.listing (Status: 403) [Size: 178]
./.mysql_history (Status: 403) [Size: 178]
./.listings (Status: 403) [Size: 178]
./.passwd (Status: 403) [Size: 178]
./.perf (Status: 403) [Size: 178]
./.profile (Status: 403) [Size: 178]
./.rhosts (Status: 403) [Size: 178]
./.sh_history (Status: 403) [Size: 178]
./.ssh (Status: 403) [Size: 178]
./.subversion (Status: 403) [Size: 178]
./.svn (Status: 403) [Size: 178]
./.svn/entries (Status: 403) [Size: 178]
./.swf (Status: 403) [Size: 178]
./.web (Status: 403) [Size: 178]
/about (Status: 200) [Size: 140120]
/academics (Status: 200) [Size: 152004]
/administration (Status: 200) [Size: 226231]
/admissions (Status: 200) [Size: 191114]
/alumni (Status: 200) [Size: 206999]
/app (Status: 301) [Size: 194] [→ https://bmsit.ac.in/app/]
/careers (Status: 200) [Size: 153144]
/cert (Status: 301) [Size: 194] [→ https://bmsit.ac.in/cert/]
/config (Status: 301) [Size: 194] [→ https://bmsit.ac.in/config/]
/contact (Status: 200) [Size: 141174]
/database (Status: 301) [Size: 194] [→ https://bmsit.ac.in/database/]
/favicon.ico (Status: 200) [Size: 0]
/feedback (Status: 200) [Size: 140366]
/gallery (Status: 200) [Size: 154614]
/index.php (Status: 200) [Size: 216938]
/library (Status: 200) [Size: 151925]
/media (Status: 200) [Size: 174736]
/newsletters (Status: 200) [Size: 146397]
/policies (Status: 200) [Size: 152501]
/public (Status: 301) [Size: 194] [→ https://bmsit.ac.in/public/]
/resources (Status: 301) [Size: 194] [→ https://bmsit.ac.in/resources/]
/research (Status: 200) [Size: 204845]
/robots.txt (Status: 200) [Size: 24]
/routes (Status: 301) [Size: 194] [→ https://bmsit.ac.in/routes/]
/sports (Status: 200) [Size: 351439]
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,403
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./.history (Status: 403) [Size: 178]
./.config (Status: 403) [Size: 178]
./.cvsignore (Status: 403) [Size: 178]
./.hta (Status: 403) [Size: 178]
./.forward (Status: 403) [Size: 178]
./.git/HEAD (Status: 403) [Size: 178]
./.bash_history (Status: 403) [Size: 178]
./.cache (Status: 403) [Size: 178]
./.bashrc (Status: 403) [Size: 178]
./.htaccess (Status: 403) [Size: 178]
./.htpasswd (Status: 403) [Size: 178]
./.listing (Status: 403) [Size: 178]
./.mysql_history (Status: 403) [Size: 178]
./.listings (Status: 403) [Size: 178]
./.passwd (Status: 403) [Size: 178]
./.perf (Status: 403) [Size: 178]
./.profile (Status: 403) [Size: 178]
./.rhosts (Status: 403) [Size: 178]
./.sh_history (Status: 403) [Size: 178]
./.ssh (Status: 403) [Size: 178]
./.subversion (Status: 403) [Size: 178]
./.svn (Status: 403) [Size: 178]
./.svn/entries (Status: 403) [Size: 178]
./.swf (Status: 403) [Size: 178]
./.web (Status: 403) [Size: 178]
/about (Status: 200) [Size: 140120]
/academics (Status: 200) [Size: 152004]
/administration (Status: 200) [Size: 226231]
/admissions (Status: 200) [Size: 191114]
/alumni (Status: 200) [Size: 206999]
/app (Status: 301) [Size: 194] [→ https://bmsit.ac.in/app/]
/careers (Status: 200) [Size: 153144]
/cert (Status: 301) [Size: 194] [→ https://bmsit.ac.in/cert/]
/config (Status: 301) [Size: 194] [→ https://bmsit.ac.in/config/]
/contact (Status: 200) [Size: 141174]
/database (Status: 301) [Size: 194] [→ https://bmsit.ac.in/database/]
/favicon.ico (Status: 200) [Size: 0]
/feedback (Status: 200) [Size: 140366]
/gallery (Status: 200) [Size: 154614]
/index.php (Status: 200) [Size: 216938]
/library (Status: 200) [Size: 151925]
/media (Status: 200) [Size: 174736]
/newsletters (Status: 200) [Size: 146397]
/policies (Status: 200) [Size: 152501]
/public (Status: 301) [Size: 194] [→ https://bmsit.ac.in/public/]
/resources (Status: 301) [Size: 194] [→ https://bmsit.ac.in/resources/]
/research (Status: 200) [Size: 204845]
/robots.txt (Status: 200) [Size: 24]
/routes (Status: 301) [Size: 194] [→ https://bmsit.ac.in/routes/]
/sports (Status: 200) [Size: 351439]
/storage (Status: 301) [Size: 194] [→ https://bmsit.ac.in/storage/]
/t (Status: 200) [Size: 213160]
/tests (Status: 301) [Size: 194] [→ https://bmsit.ac.in/tests/]
/vendor (Status: 301) [Size: 194] [→ https://bmsit.ac.in/vendor/]
/web.config (Status: 200) [Size: 1194]
Progress: 4614 / 4615 (99.98%)

Finished

(kali@kali)-[~/Desktop]
$
```

## Using Dirb

- Open a terminal in Linux
- `>>dirb https://bmsit.ac.in/`
- Analyze the output for discovered directories

```
kali@kali: ~/Desktop
File Actions Edit View Help
/tests (Status: 301) [Size: 194] [→ https://bmsit.ac.in/tests/]
/vendor (Status: 301) [Size: 194] [→ https://bmsit.ac.in/vendor/]
/web.config (Status: 200) [Size: 1194]
Progress: 4614 / 4615 (99.98%)

Finished

You might want to simulate key-depressing in order to find...

(kali@kali) - [~/Desktop]
$ dirb https://bmsit.ac.in/

DIRB v2.22
By The Dark Raver

START_TIME: Mon Sep 23 09:32:35 2024
URL_BASE: https://bmsit.ac.in/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: https://bmsit.ac.in/ ---
+ https://bmsit.ac.in/about (CODE:200|SIZE:140120)
+ https://bmsit.ac.in/academics (CODE:200|SIZE:152004)
+ https://bmsit.ac.in/administration (CODE:200|SIZE:226231)
+ https://bmsit.ac.in/admissions (CODE:200|SIZE:191114)
+ https://bmsit.ac.in/alumni (CODE:200|SIZE:206999)
=> DIRECTORY: https://bmsit.ac.in/app/
+ https://bmsit.ac.in/careers (CODE:200|SIZE:153144)
=> DIRECTORY: https://bmsit.ac.in/cert/
=> DIRECTORY: https://bmsit.ac.in/config/
+ https://bmsit.ac.in/contact (CODE:200|SIZE:141174)
=> DIRECTORY: https://bmsit.ac.in/database/
+ https://bmsit.ac.in/favicon.ico (CODE:200|SIZE:0)
+ https://bmsit.ac.in/feedback (CODE:200|SIZE:140366)
+ https://bmsit.ac.in/gallery (CODE:200|SIZE:154614)
+ https://bmsit.ac.in/home (CODE:302|SIZE:346)
+ https://bmsit.ac.in/index.php (CODE:200|SIZE:216938)
+ https://bmsit.ac.in/library (CODE:200|SIZE:151925)
+ https://bmsit.ac.in/login (CODE:500|SIZE:6615)
+ https://bmsit.ac.in/logout (CODE:405|SIZE:825)
+ https://bmsit.ac.in/media (CODE:200|SIZE:174736)
+ https://bmsit.ac.in/newsletters (CODE:200|SIZE:146397)
+ https://bmsit.ac.in/policies (CODE:200|SIZE:152501)
=> DIRECTORY: https://bmsit.ac.in/public/
+ https://bmsit.ac.in/register (CODE:500|SIZE:6615)
+ https://bmsit.ac.in/research (CODE:200|SIZE:204845)
=> DIRECTORY: https://bmsit.ac.in/resources/
+ https://bmsit.ac.in/robots.txt (CODE:200|SIZE:24)
=> DIRECTORY: https://bmsit.ac.in/routes/
+ https://bmsit.ac.in/sports (CODE:200|SIZE:351439)
=> DIRECTORY: https://bmsit.ac.in/storage/
+ https://bmsit.ac.in/t (CODE:200|SIZE:213160)
=> DIRECTORY: https://bmsit.ac.in/tests/
=> DIRECTORY: https://bmsit.ac.in/vendor/
+ https://bmsit.ac.in/web.config (CODE:200|SIZE:1194)

--- Entering directory: https://bmsit.ac.in/app/ ---

--- Entering directory: https://bmsit.ac.in/cert/ ---
=> DIRECTORY: https://bmsit.ac.in/cert/app/
=> DIRECTORY: https://bmsit.ac.in/cert/config/
=> DIRECTORY: https://bmsit.ac.in/cert/database/
+ https://bmsit.ac.in/cert/favicon.ico (CODE:200|SIZE:0)
+ https://bmsit.ac.in/cert/index.php (CODE:200|SIZE:17386)
=> DIRECTORY: https://bmsit.ac.in/cert/public/
=> DIRECTORY: https://bmsit.ac.in/cert/resources/
```



## Monitoring and Logging with snort

**Objective :** To monitor network traffic and log reconnaissance activities using snort.

**Tools :** snort

- Configuring Snort
- >> sudo apt-get install snort
- >> sudo snort -A console -i eth0 -c /etc/snort/snort.conf -l /var/log/snort

```
vboxuser@Ubuntu:~$ sudo snort -A console -i enp0s3 -c /etc/snort/snort.conf -l /var/log/snort
Running in IDS mode

--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-Ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 70
00:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060
9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5060 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8
899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
  Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsfc_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
```

- Files Available in snort

```
vboxuser@Ubuntu:/etc/snort$ cd
vboxuser@Ubuntu:~$ cd /etc/snort
vboxuser@Ubuntu:/etc/snort$ ls
attribute_table.dtd      community-sid-msg.map  gen-msg.map           rules                  snort.conf.save       threshold.conf
classification.config    file_magic.conf        reference.config       snort.conf            snort.debian.conf     unicode.map
vboxuser@Ubuntu:/etc/snort$
```

- Modification in snort.conf and local.rules

>> Sudo nano snort.conf

>>sudo nano local.rules

```
GNU nano 6.2 snort.conf
#-----
# VRT Rule Packages Snort.conf
#
# For more information visit us at:
#   http://www.snort.org           Snort Website
#   http://vrt-blog.snort.org/     Sourcefire VRT Blog
#
# Mailing list Contact:   snort-users@lists.snort.org
# False Positive reports: fp@sourcefire.com
# Snort bugs:            bugs@snort.org
#
# Compatible with Snort Versions:
# VERSIONS : 2.9.15.1
#
# Snort build options:
# OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --enable-active-
#
# Additional information:
# This configuration file enables active response, to run snort in
# test mode -T you are required to supply an interface -i <interface>
# or test mode will fail to fully validate the configuration and
# exit with a FATAL error
#-----
#####
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
# 1) Set the network variables.
```

```
vboxuser@Ubuntu:/etc/snort  x  vboxuser@Ubuntu: ~  x
GNU nano 6.2 local.rules
```



- Validation of Configuration

>> Sudo snort -T -c /etc/snort/snort.conf

```
vboxuser@Ubuntu:/etc/snort$ sudo snort -T -c /etc/snort/snort.conf
Running in Test mode

==== Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 70
00:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060
9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8
899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
```

- Perform alert capturing

>> Sudo snort -A console -c /etc/snort/snort.conf

```
vboxuser@Ubuntu:/etc/snort$ sudo snort -T -c /etc/snort/snort.conf
Running in Test mode

==== Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 70
00:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060
9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8
899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
```

- Run Snort in Sniffer Mode (Verbos)

>> snort -v -i enp0s3

```
vboxuser@Ubuntu:/etc/snort$ sudo snort -v -i enp0s3
Running in packet dump mode

==== Initializing Snort ===
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet

==== Initialization Complete ===

o'-'~
'''~
-*)> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Commencing packet processing (pid=4290)
```

- **Run Snort in Packet Logger Mode**

```
>>sudo snort -dev -l /var/log/snort -i enp0s3
```

```
vboxuser@Ubuntu:~$ sudo snort -dev -l /var/log/snort -i enp0s3
Running in packet logging mode

--== Initializing Snort ==--
Initializing Output Plugins!
Log directory = /var/log/snort
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet

--== Initialization Complete ==--

o"')~  -*> Snort! <*-
' ' '  Version 2.9.15.1 GRE (Build 15125)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.10.1 (with TPACKET_V3)
      Using PCRE version: 8.39 2016-06-14
      Using ZLIB version: 1.2.11
```

- **Run Snort in NIDS Mode with a Configuration**

```
>> sudo snort -c /etc/snort/snort.conf -l enp0s3 -A console
```

```
vboxuser@Ubuntu:~$ sudo snort -c /etc/snort/snort.conf -i enp0s3 -A console
Running in IDS mode

--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 70
00:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060
9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8
899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsfe_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort/snort_dynamicrules.
Finished Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules
```

- **Read Packets from a PCAP**

```
>> snort -r /path/to/file.pcap -c /etc/snort/snort.conf
```

```
vboxuser@Ubuntu:~$ sudo snort -r /path/to/file.pcap -c /etc/snort/snort.conf
Running in IDS mode

--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 70
00:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060
9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8
899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
```