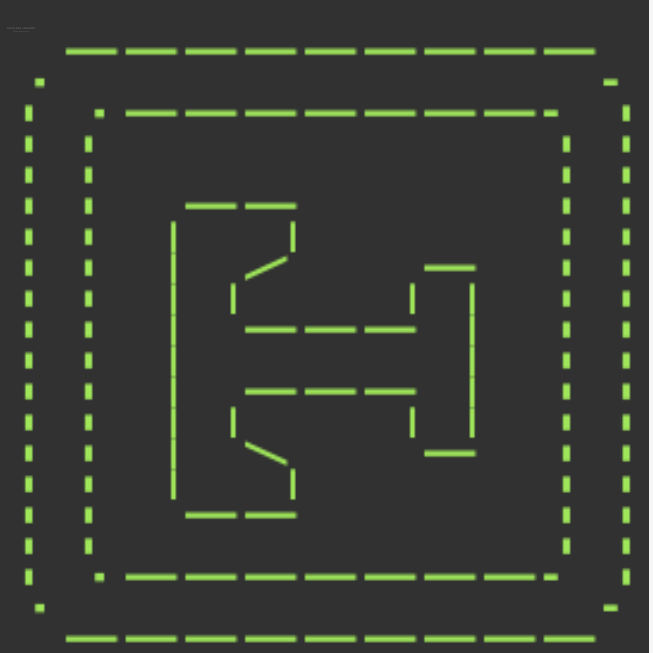


BRISKINFOSEC PENTEST TOOLKIT

WHITEPAPER

PREPARED BY

Mr.Venkatesh
Security Engineer
@briskinfosec Bint lab

PRESENTED BY

NCDRC
(National Cyber Defence Research Centre)
in collabration with
BINT Lab
www.ncdrc.res.in.

1.OVERVIEW

Briskinfosec Pentest Toolkit (BPT) is a powerful and automated security assessment toolkit. BPT is pioneering techniques that helps penetration testers to automate the attack surfaces. Unlike other Pentest Frameworks, BPT focuses on major domains and tool flexibility. This toolkit allows penetration testers to select specific modules (in real-time) for each attack.

2.INSTALLATION

The following installation instructions are suitable for Linux. In theory, BPT should work on any operating system which can run bash scripts and python.

2.1 SOURCE

Cloning the Git repository from GitHub:

$ git clone https://github.com/briskinfosec/BPT

2.2 PREREQUISITES

BPT requires certain things in order to run error free. They are:

- NMAP
- METASPLOIT
- XTERM
- INTERNET CONNECTION
- ROOT USER

2.3 QUICK INSTALLATION

You can install all the prerequisites, the required tools and scripts, using the installation script.

$ chmod +x install.sh

$ ./install.sh

2.4 TO START BPT

To start BTP, simply run

$ chmod +x BPT.sh

$ ./BPT.sh

2.5 TO UPDATE

To update BTP, simply run

$ git pull

3. INTERFACE

When user starts the BPT, an interface will be prompted. BPT checks for all the required tools and if not installed, installs automatically.

Once its boots up, main interface comes up.

The main interface contains options for sub categories:

1. INTEL GATHERING
2. NETWORK SCANNING
3. METASPLOIT TECHNIQUES
4. SSL INFORMATION
5. CREDITS

BPT is user friendly where the user can easily navigate into the options using respective numbers. It also provides navigation panel when user is in the current module.

4. MODULES

BPT offers different modules such as:

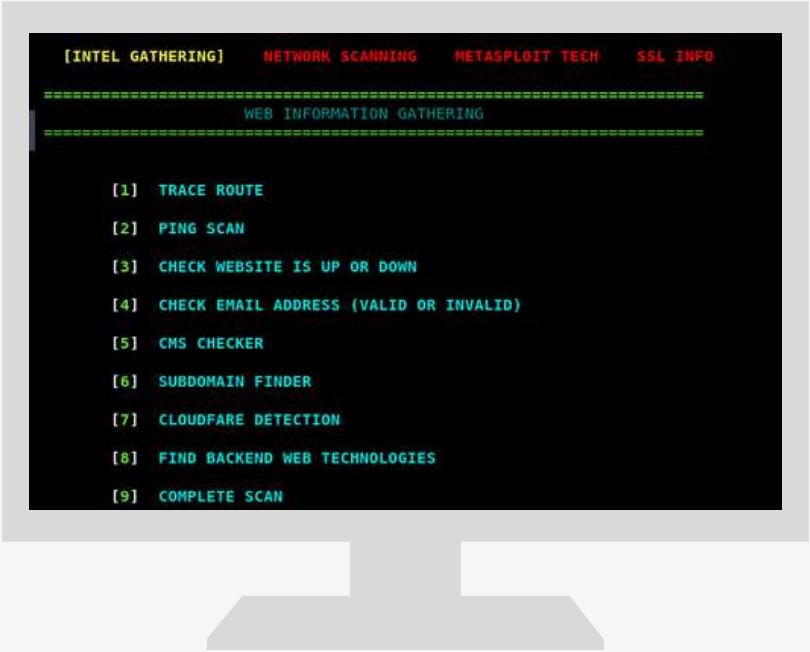
1. INTEL GATHERING
2. NETWORK SCANNING
3. METASPLOIT TECHNIQUES
4. SSL INFORMATION
5. CREDITS

4.1 INTEL GATHERING

This module offers user to gather intelligence information for passive information gathering techniques. Also ,user can gather information based on web and network.

4.1.1 WEB INFORMATION GATHERING

In this module, user can retrieve web based information. This module contains various categories that are listed below:



TRACE ROUTE

- User can gather route information about the target.

PING SCAN

- User can determine live hosts.

CHECK WEBSITE IS UP OR DOWN

- User can find whether the website is live or not.

CHECK EMAIL ADDRESS

- User can check whether the email address is valid or not.

CMS CHECKER

- User can check what type of CMS is used.

SUBDOMAIN FINDER

- User can enumerate the subdomains of the given target.

CLOUDFARE DETECTION

- User can identify whether cloudflare is used or not.

FIND BACKEND WEB TECHNOLOGIES

- User can find the kind of web technologies that are used

COMPLETE SCAN

- User can perform the above scan in one go.

4.1.2 NETWORK INFORMATION GATHERING

DNS LOOKUP

- User can determine the DNS information about the target.

REVERSE DNS

- User can able to reverse lookup their target domain.

HOST RECORD GATHERING

- User can gather the targets host records.

SHARED DNS SERVER

- This module offers user to gather the shared DNS information.

ZONE TRANSFER

- This module offers user to check, if the DNS leaks any zone records.

WHOIS LOOKUP

- This module offers user to find registrant information of the targeted domain.

DNS LEAK TEST

- User can test whether the DNS leaks any information to the attacker.

SERVER INFO

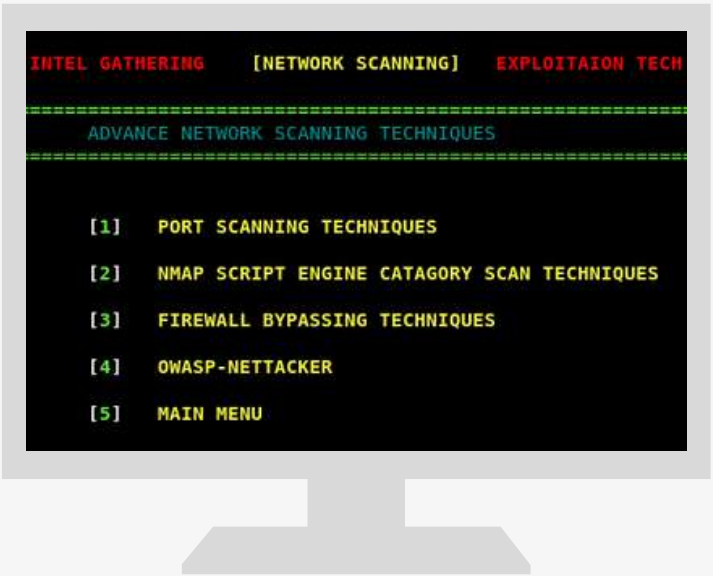
- This module offers the user to gather information about the targeted server.

COMPLETE SCAN

- User can perform the above scans in just one click.

4.2 NETWORK SCANNING

In this category, user can perform network based advanced information gathering. This module contains some advanced and logical scripts that are required to gather information about the given target.



CATEGORIES:

1. PORT SCANNING TECHNIQUES
2. NSE CATEGORY SCAN TECHNIQUES
3. FIREWALL BYPASS TECHNIQUES
4. OWASP-NETTACKER
5. MAIN MENU

4.2.1 PORT SCANNING TECHNIQUES

Port Scanning module contains some advanced scanning concepts which are applicable to scan any kind of network devices. This module offers some serious port scanning techniques.

PING SCAN

- This is not just a normal ping scan. It can bypass blocked ICMP and is customisable.

FULL PORT SCAN (TCP)

- This scan provides a full scan on TCP protocols (all 65535 ports).

AGGRESSIVE SCAN

- This scan provides information such as OS information, vulnerability details, sensitive information, etc.

FULL PORT SCAN (UDP)

- This scan provides a full scan on UDP protocols (all 65535 ports).

DEFAULT SCRIPT SCAN

- This scan uses some backend scripts to gather some detailed information about the given target.

VERSION DETECTION

- This scan provides version information of the running services.

COMPREHENSIVE SCAN

- This is a complete scan which provides complete information. But, this scan is a bit slower.

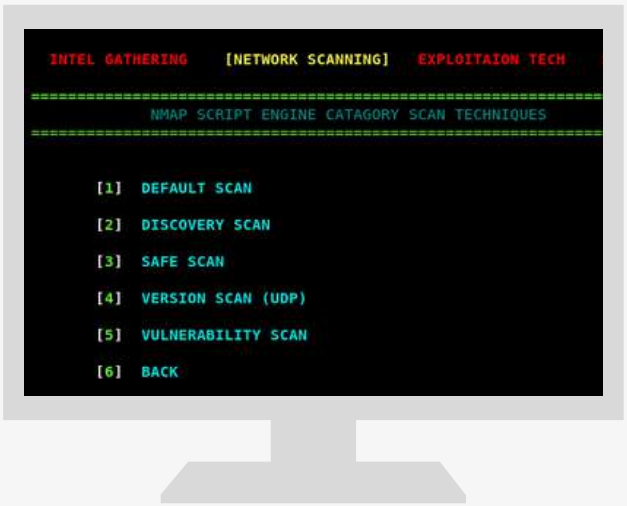
(Note: Don't use this scan in production environment, it may crash the server)

CUSTOM SCAN

- This scan offers user to customize their scan using NSE scripts. It is highly customisable.

4.2.2 NSE CATEGORY SCAN

In this category, user can perform network based advanced information gathering. This module contains some advanced and logical scripts that are required to gather information about the given target.



DEFAULT SCAN

- This scan uses some default NSE scripts for scanning services to gather information.

DISCOVERY SCAN

- This scan uses scripts related to discovery based information (ports, services, versions).

SAFE SCAN

- This scan uses safest scripts in order to get information.

VERSION SCAN (UDP)

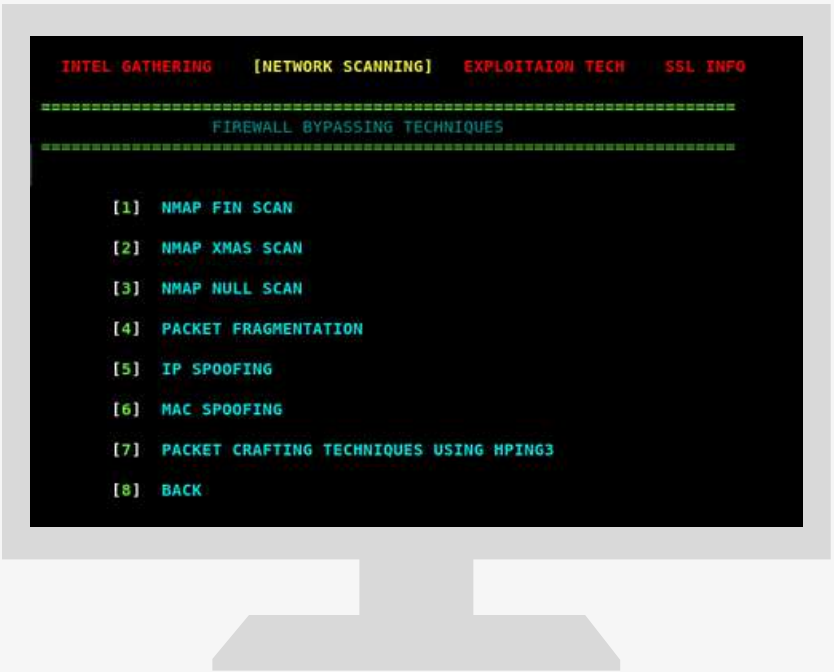
- This scan uses versions related NSE scripts to find version information.

VULNERBILITY SCAN

- This scans user vulnerability based scripts to find vulnerabilities in the target.

4.2.3 FIREWALL BYPASSING TECHNIQUES

This category contains advanced firewall bypassing technique modules. User can use these modules in certain situations.



NMAP FIN SCAN

- This module sends finish packets to trick the firewall.

NMAP XMAS SCAN

- This module uses FIN PSH packets to bypass the firewall.

NMAP NULL SCAN

- This module sends null packets to target for bypassing firewall

PACKET FRAGMENTATION

- This module will fragment the packets to identify the information.

IP SPOOFING

- In this module, user can spoof the source IP in order to bypass the firewall rules.

MAC SPOOFING

- In this module, user can spoof the mac address in order to bypass firewall rule sets.

PACKET CRAFTING USING HPING3

- In this module, packets are sent with different flags. When user gets a reply, it means those flags have bypassed.

4.2.4 OWASP-NETTACKER

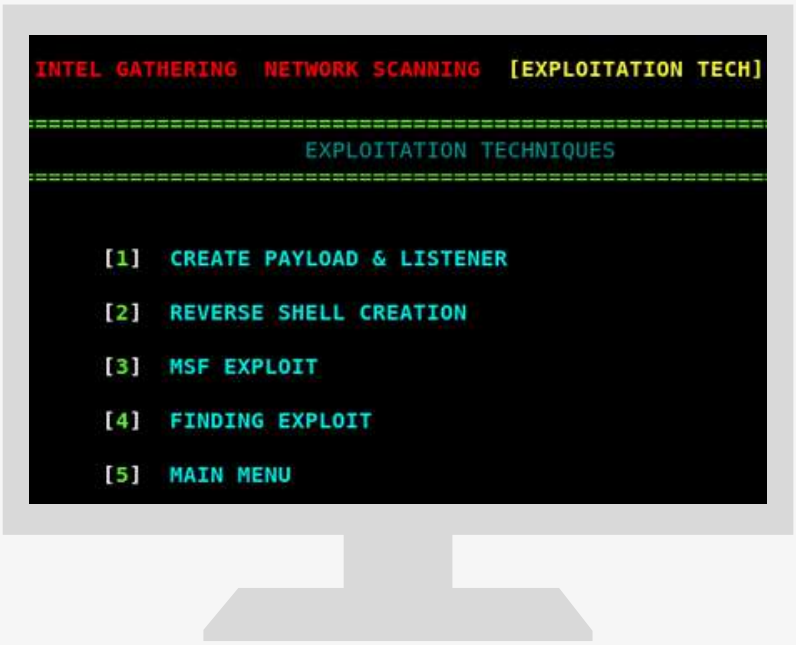
OWASP NETTACKER is an open source software in Python language which lets you to perform **Automated Penetration Testing** and **Automated Information Gathering**. This software can be made to run on Windows/Linux/OSX, under python.

NETTACKER project was created for performing automated information gathering, vulnerability scanning and eventually generating a report for networks that includes services, bugs, vulnerabilities, misconfigurations, and information.
This software uses SYN, ACK, TCP, ICMP and many other protocols to detect and bypass the Firewalls/IDS/IPS and other devices. By using a unique solution in NETTACKER to find protected services such as SCADA, we can make it as one of the best scanners.

4.3 EXPLOITATION TECHNIQUES

This category focuses on payload creation and exploitation of certain vulnerabilities.
There are some modules used in this BPT. They are:

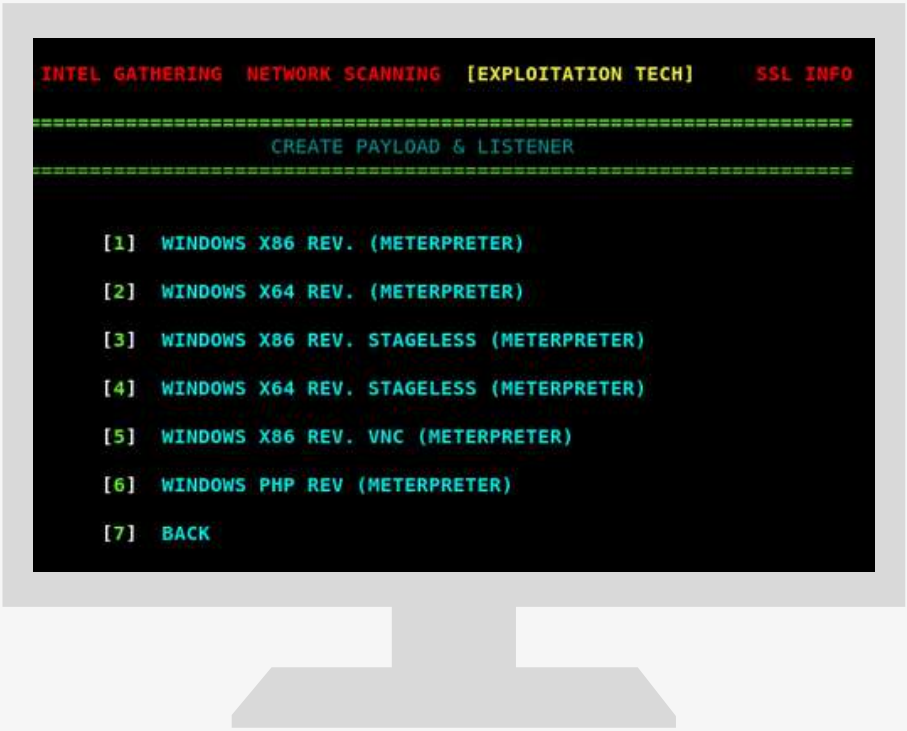
1. CREATE PAYLOAD & LISTENER
2. REVERSE SHELL CREATION
3. EXPLOITATION
4. FINDING EXPLOIT



4.3.1 CREATE PAYLOAD & LISTENER

- In this module, user can create payloads for both, stageless and staged environments.

(Note: stageless payloads are used to bypass firewall)



WINDOWS X86 REVERSE (METERPRETER)

- This module is used to create 32 bit Meterpreter reverse payload.

WINDOWS X86 REVERSE STAGELESS (METERPRETER)

- This module is used to create 32 bit stageless payload. This can also be used to bypass firewall.

WINDOWS X64 REVERSE STAGELESS (METERPRETER)

- This module is used to create 64 bit stageless payload. This can also be used to bypass firewall.ds null packets to target for bypassing firewall

WINDOWS X86 REVERSE VNC (METERPRETER)

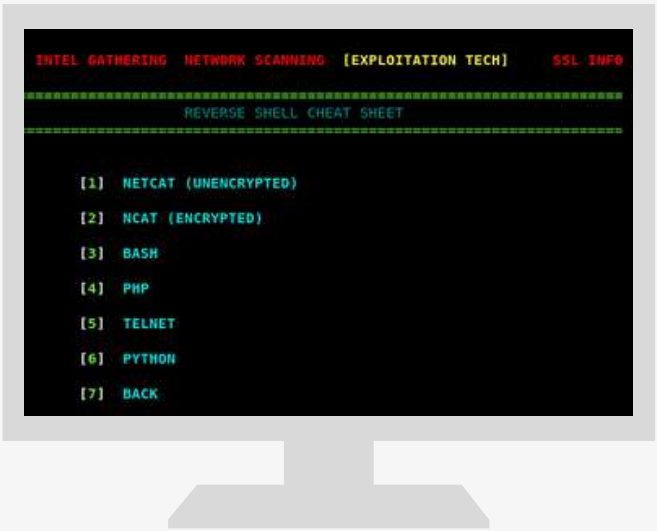
- This module is used to create 32 bit VNC Meterpreter payload.

WINDOWS PHP REVERSE (METERPRETER)

- This module is used to create PHP Meterpreter reverse payload.

4.3.2 REVERSE SHELL CHEAT SHEET

This category contains reverse shell on different languages. User can use this shell to get connections from servers. In this module, user can create reverse shell using different categories and BPT will automatically start the listener using netcat.



NETCAT (UNENCRYPTED)

- This module is used to create a reverse shell script for netcat. This uses unencrypted channel.

NCAT (ENCRYPTED)

- This module is used to create a reverse shell based on ncat. It uses encrypted channel.

BASH

- This module is used to create reverse shell based on bash.

PHP

- This module creates reverse shell code on PHP language.

TELNET

- This module uses telnet to create reverse shell. (Note: to use telnet reverse shell, user needs to use 2 listeners).

PYTHON

- This module uses python to create reverse shell.

4.3.3 MSF EXPLOIT

This module contains exploitation techniques for known vulnerabilities for windows operating system.
In future, we will be adding more modules to the list. These modules are fully automated where user just needs to provide the target information.

MS17-010 ETERNALBLUE DETECTION

- In this Module, user can detect whether MS17-010 patch is installed or not.

(Note: This patch is very critical as attackers can perform RCE attack)

MS17-010 ETERNALBLUE EXPLOITATION

- In this module, user can perform RCE execution on unpatched systems (MS17-010 update). For this, user needs to provide the target IP address, in order to perform RCE.

(Note: This attack can be performed only on 64bit systems)

MS17_010_PSEXEC

- In this module, user can perform RCE using target username and password hashes. So before performing this attack, the user needs to gather username and password of the target.

PASS THE HASH ATTACK

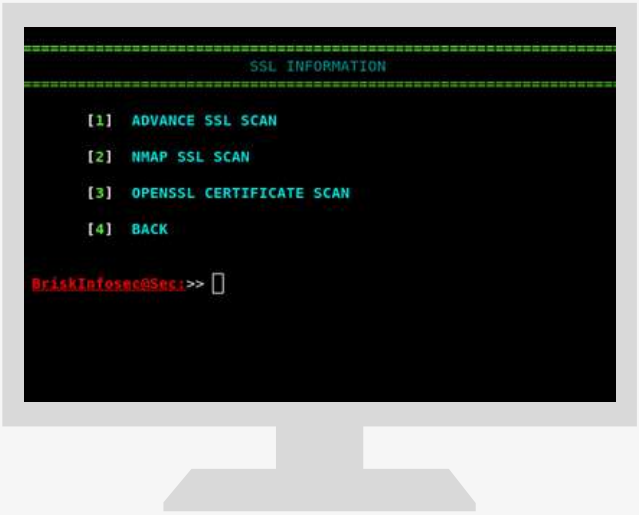
- In this module, user could be able to login the system without the target knowledge. To perform this attack, user needs to have the admin's username and password hashes.

4.3.4 FINDING EXPLOIT

In this module, user can search exploit for the given keywords.

SSL INFORMATION

This module provides information about the SSL certificates and its weakness. User can also gather information about the target SSL information such as weak algorithms, weak ciphers, supported protocols and much more.



ADVANCE SSL SCAN

- In this module, user can reduce the gathered advanced information about the SSL certificates.

NMAP SSL SCAN

- In this module, user can gather SSL information using NMAP tool.

OPENSSL CERTIFICATE SCAN

- In this module, user can identify whether the weak SSL protocols are enabled by downloading SSL certificates.

7.ABOUT US

AUTHOR

VENKATESH - Security Engineer, supported by BRISKINFOSEC BINT LAB.

BINT LAB

BINT LAB (Brisk Intelligence Laboratory) is the indigenous CoE (Center of Excellence) cybersecurity research lab of Briskinfosec.

Here, research and development is focused on making today's systems more secure, simultaneously planning for the security of tomorrow's technology.

Our unique set of capabilities motivates us to focus on our cybersecurity research in various innovative technologies.

BINT LAB is empowered with in-house experts, volunteers, external security researchers and most talented cybersecurity professionals whom possess cult knowledge in the sector of information security.

We have conglomerated a vast library of resources containing blogs, whitepapers, and security assessment tools to help in managing and creating smart cybersecurity solutions.

BRISKINFOSEC'S BINT LAB ACHIEVEMENTS

[✔] Briskinfosec's BINT LAB won the INDIA BOOK OF RECORDS for Cybersecurity initiatives.

[✔] Created ANSE (Advanced Nmap Scripting Engine) scanner for network security assessment.

[✔] Created and published the NCDRC MAST (National Cyber Defence Research Centre Mobile App Security Test) framework.

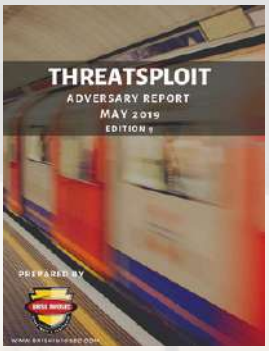
[✔] Researchers are actively participating in Bug Bounty and Hall of Fame events.

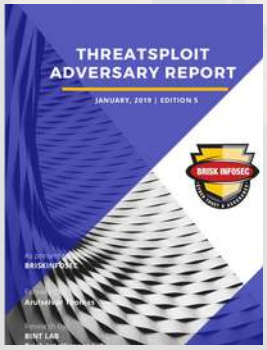
INVITING RESEARCH COLLABORATION:

If you are an individual, university, or an organization looking forward to build and collaborate on cybersecurity research process, you can send your proposal to contact@briskinfosec.com.

YOU MAY BE INTERESTED ON OUR PREVIOUS WHITEPAPER

YOU MAY BE INTERESTED ON OUR PREVIOUS WORKS





REFERENCES ABOUT BRISKINFOSEC

CASE STUDIES

SOLUTIONS

SERVICES

RESEARCH

COMPLIANCES

BLOGS

This White Paper is proudly presented by

BRISKINFOSEC TECHNOLOGY AND CONSULTING PVT LTD

Feel free to reach us for all your cybersecurity needs
contact@briskinfosec.com | www.briskinfosec.com
|USA|INDIA|UK