राष्ट्रीय प्रौद्योगिकी संस्थान सिक्किम

NATIONAL INSTITUTE OF TECHNOLOGY SIKKIM

REPORT

Ministry: National Technical Research Organisation,(NTRO)

PS Code: SIH1455

Problem Statement Title: Efficient enumeration of URLs of active hidden servers over anonymous channel (TOR)

Team Name: Binary Brains

Theme Name: Blockchain and Cybersecurity

Team Details:-

Team Leader Name: Harshit Vyas

Branch (Btech/Mtech/PhD etc): BTech Stream (ECE, CSE etc): CSE Year (I,II,III,IV): II

Team Member 1 Name: Sarika Gautam

Branch (Btech/Mtech/PhD etc): BTech Stream (ECE, CSE etc): CSE Year (I,II,III,IV): III

Team Member 2 Name: Debanjana Sur

Branch (Btech/Mtech/PhD etc): BTech Stream (ECE, CSE etc): CSE Year (I,II,III,IV): II

Team Member 3 Name: Arindam Das

Branch (Btech/Mtech/PhD etc): BTech Stream (ECE, CSE etc): ECE Year (I,II,III,IV): II

Team Member 4 Name: Anand Pandey

Branch (Btech/Mtech/PhD etc): BTech Stream (ECE, CSE etc): EEE Year (I,II,III,IV): II

Team Member 5 Name: Aditya Sharma

Branch (Btech/Mtech/PhD etc): BTech Stream (ECE, CSE etc): ECE Year (I,II,III,IV): II

Defining Problem Statement: The Tor network is designed to provide anonymity and privacy for users by routing their internet traffic through a series of volunteer-operated nodes, making it challenging to trace the origin of the traffic. While this anonymity is essential for protecting the privacy and security of users, it also creates an environment where hidden services (websites hosted on Tor) can operate with relative impunity, often engaging in illicit activities. The problem at hand is the efficient enumeration of URLs of active hidden servers over the anonymous channel Tor.

Understanding the TOR Network: The Tor network, short for "The Onion Router," is an open-source, volunteer-driven network that allows users to browse the internet anonymously. It achieves this by encrypting and routing internet traffic through a series of relays, making it difficult for anyone to trace the source of the traffic. This anonymity is crucial for protecting users' privacy and enabling free expression, but it also presents challenges for law enforcement agencies and security researchers.

Creation of Bots: To enumerate URLs of active hidden servers over Tor, malicious actors often create bots that continuously scan the Tor network for potential targets. These bots are programmed to exploit vulnerabilities or weaknesses in hidden services to gather information or engage in malicious activities. Detecting and countering these bots requires advanced techniques in network monitoring and cybersecurity.

Bot Monitoring on TOR: Monitoring the Tor network for malicious or suspicious activity is essential to maintain security and prevent illegal activities. Bots, automated programs thatperform various tasks, are frequently used to scan the Tor network for hidden services, gather information, or potentially engage in illicit activities such as distributed denial of service (DDoS) attacks, data theft, or illegal content distribution. Detecting and monitoring these bots is a challenging task due to the inherent anonymity provided by Tor.

Creation of a Pseudo Tor: The Tor network's design principles and architecture have inspired the creation of similar networks that aim to provide anonymity and privacy. These networks often use different technologies and approaches but share the goal of enabling users to browse the internet without revealing their identity or location. Examples include I2P (Invisible Internet Project) and Freenet. These networks present similar challenges for monitoring and security as the Tor network.

Use Cases:-

Security Enhancement: Detects and mitigates potential security threats and malicious activities within the Tor network, monitors for cyberattacks, malware, and unauthorized access attempts originating from or using Tor and provides real-time alerts to network administrators for swift incident response and threat mitigation.

Privacy Protection: Ensures that Tor is not being used for unauthorized or potentially harmful activities that may compromise user privacy, guards against the risk of data exfiltration and communication with malicious Tor nodes and balances the need for network security with user privacy concerns.

Compliance and Report: Generates detailed logs and reports on Tor network activities, aiding in compliance with regulatory requirements, provides a comprehensive record for audits and internal security policy enforcement and demonstrates proactive monitoring and security measures to regulatory authorities.

Research and Threat Intelligence: Gathers valuable data for research on the Tor network's behaviour and evolving threat landscape, contributes to the identification of emerging threats, vulnerabilities, and trends within the Tor network and enhances the organization's overall cybersecurity posture through threat intelligence gathering and analysis.

Conclusion: We performed many test cases that consisted of creating a bot with Postman API, but we couldn't execute that properly because we lacked information about API. We also checked the path of the packet over IP on Surface Web and tested the same for the Onion website, but it didn't work with the dig command.

We visited one of the onion sites and checked its source code. We found one server trace with the name "Infocon.org", We fetched and succeeded in finding the server IP, which was 50.230.231.89.

We tested the server IP with n-map and found the following open port:

```
nmap 50.230.231.89
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-27 13:36 UTC
Nmap scan report for 50-230-231-89-static.hfc.comcastbusiness.net
(50.230.231.89)
Host is up (0.017s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
25/tcp   open   smtp
80/tcp   open   http
110/tcp  open   pop3
143/tcp  open   imap
443/tcp  open   https
465/tcp  closed smtps
993/tcp  open   imaps
995/tcp  open   pop3s
6346/tcp closed gnutella

Nmap done: 1 IP address (1 host up) scanned in 5.36 seconds
```

In summary, the efficient enumeration of URLs of active hidden servers over the anonymous channel Tor presents a multifaceted challenge that encompasses understanding the Tor network, monitoring for malicious bots, countering the creation of such bots, and addressing the emergence of Tor-like networks.

Bro/Zeek VS Our Bot

Bro/Zeek is an open-source network security analysis monitoring tool that can be highly customised to the user’s specific needs, deep contextual understanding of the user's network and systems, and response flexibility. Our bot can adapt quickly to changing situations and respond to incidents in real time.

References:-

- **Bro/Zeek -** open-source network security analysis monitoring tool
- **Research paper from GoogleScholar**
- **Geeksforgeeks**
- **ChatGPT**
- **Github repo**
- **Youtube**