

Final Project Report

Team Name - Team Z

Track - Cyber Security

Project Name - Friday

Friday

FridAy by Team Z

Cyber Watch Dashboard

Welcome to Cyber Watch. Type ls to list available options.

> ls

1. Phishing Detection
2. DoS Attack Prevention
3. Malware Threat Analysis

> help

Available commands: ls, phishing, dos, malware, clear

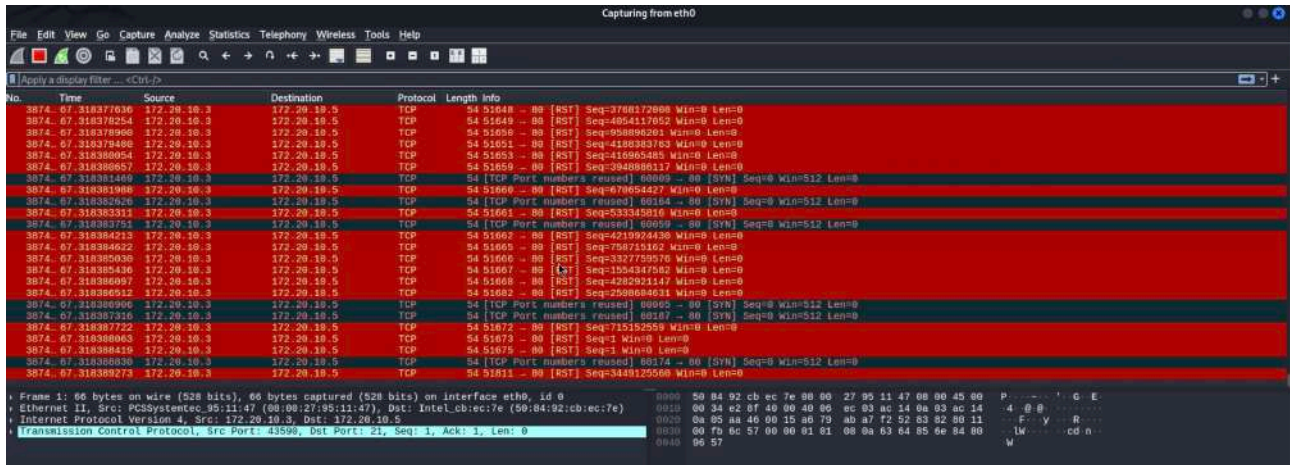
> phishing

Redirecting to Phishing Detection...

>

Our aim was to create a suite of tools to prevent cyber attacks in real time. We have successfully implemented the following.

1. We have successfully created our own datasets by performing cyber attacks in real time and converting these logs into CSV format using TShark tool.



The screenshot shows the Wireshark interface with a packet list table. The table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The packets are captured on interface eth0. The list includes several TCP RST (Reset) packets and one TCP SYN (Synchronize) packet. The 'Info' column provides details for each packet, such as sequence numbers, window sizes, and flags.

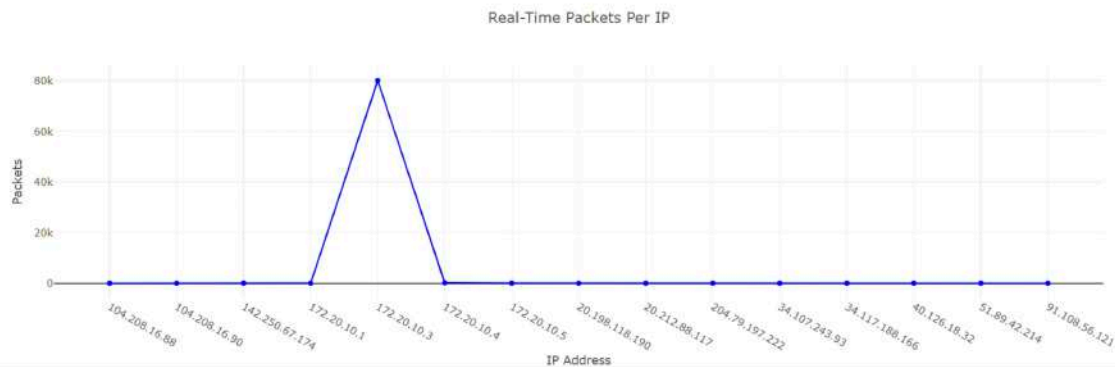
No.	Time	Source	Destination	Protocol	Length	Info
3874	0.7318377036	172.20.10.3	172.20.10.5	TCP	54	51648 → 80 [RST] Seq=3768172000 Win=0 Len=0
3874	0.7318378254	172.20.10.3	172.20.10.5	TCP	54	51649 → 80 [RST] Seq=4054117052 Win=0 Len=0
3874	0.7318379960	172.20.10.3	172.20.10.5	TCP	54	51650 → 80 [RST] Seq=9080804201 Win=0 Len=0
3874	0.7318379486	172.20.10.3	172.20.10.5	TCP	54	51651 → 80 [RST] Seq=4188833763 Win=0 Len=0
3874	0.7318380054	172.20.10.3	172.20.10.5	TCP	54	51653 → 80 [RST] Seq=416865485 Win=0 Len=0
3874	0.7318380857	172.20.10.3	172.20.10.5	TCP	54	51659 → 80 [RST] Seq=3948886317 Win=0 Len=0
3874	0.7318381469	172.20.10.3	172.20.10.5	TCP	54	[TCP Port numbers reused] 60060 → 80 [SYN] Seq=0 Win=512 Len=0
3874	0.7318381988	172.20.10.3	172.20.10.5	TCP	54	51666 → 80 [RST] Seq=670654427 Win=0 Len=0
3874	0.7318382620	172.20.10.3	172.20.10.5	TCP	54	[TCP Port numbers reused] 60164 → 80 [SYN] Seq=0 Win=512 Len=0
3874	0.7318383311	172.20.10.3	172.20.10.5	TCP	54	51661 → 80 [RST] Seq=533345616 Win=0 Len=0
3874	0.7318383751	172.20.10.3	172.20.10.5	TCP	54	[TCP Port numbers reused] 60060 → 80 [SYN] Seq=0 Win=512 Len=0
3874	0.7318384213	172.20.10.3	172.20.10.5	TCP	54	51662 → 80 [RST] Seq=4219924436 Win=0 Len=0
3874	0.7318384622	172.20.10.3	172.20.10.5	TCP	54	51665 → 80 [RST] Seq=758715162 Win=0 Len=0
3874	0.7318385030	172.20.10.3	172.20.10.5	TCP	54	51666 → 80 [RST] Seq=3227729516 Win=0 Len=0
3874	0.7318385436	172.20.10.3	172.20.10.5	TCP	54	51667 → 80 [RST] Seq=1554347582 Win=0 Len=0
3874	0.7318386097	172.20.10.3	172.20.10.5	TCP	54	51668 → 80 [RST] Seq=4282921447 Win=0 Len=0
3874	0.7318386512	172.20.10.3	172.20.10.5	TCP	54	51669 → 80 [RST] Seq=268884631 Win=0 Len=0
3874	0.7318386966	172.20.10.3	172.20.10.5	TCP	54	[TCP Port numbers reused] 60060 → 80 [SYN] Seq=0 Win=512 Len=0
3874	0.7318387336	172.20.10.3	172.20.10.5	TCP	54	[TCP Port numbers reused] 60167 → 80 [SYN] Seq=0 Win=512 Len=0
3874	0.7318387722	172.20.10.3	172.20.10.5	TCP	54	51672 → 80 [RST] Seq=715152558 Win=0 Len=0
3874	0.7318388065	172.20.10.3	172.20.10.5	TCP	54	51673 → 80 [RST] Seq=1 Win=0 Len=0
3874	0.7318388439	172.20.10.3	172.20.10.5	TCP	54	51675 → 80 [RST] Seq=1 Win=0 Len=0
3874	0.7318388830	172.20.10.3	172.20.10.5	TCP	54	[TCP Port numbers reused] 60174 → 80 [SYN] Seq=0 Win=512 Len=0
3874	0.7318389273	172.20.10.3	172.20.10.5	TCP	54	51681 → 80 [RST] Seq=5448125560 Win=0 Len=0

2. We have successfully implemented a Transformer based model using hash mapping to prevent Phishing. Our tool detects malicious links and blocks them, if the links are not malicious the tool allows access to the website.



3. We have successfully implemented an LSTM based model to detect Denial of Service attacks. Our model works by detecting a DoS attack and raising a caution for the IP address, subsequently blocking the IP address.

CyberWatch: Real-Time Network Monitoring & Blocking



Blocked IPs

172.20.10.3

4. We have successfully implemented a malware detection system that utilises Steganography detection techniques to identify if a particular file or software has virus embedded in it or not. If Malware is present it alerts the user and analyse the type of malware

CyberWatch : Malicious File Detected

File Name: music.apk

Flagged by the following vendors:

Lionic (Lionic): Trojan.AndroidOS.Metasploit.C!c
CTX (CTX): apk.trojan.metasploit
CAT-QuickHeal (CAT-QuickHeal): Android.Agent.ACZ
Skyhigh (Skyhigh): Artemis!Trojan
McAfee (McAfee): Artemis!DB24A6693271
K7GW (K7GW): Trojan (005983af1)
Trustlook (Trustlook): Android.Malware.Trojan
VirIT (VirIT): Android.Trj.RemoteCode.KC
SymantecMobileInsight (SymantecMobileInsight): Hacktool:Mesexploit
Symantec (Symantec): Trojan.Gen.MBT
ESET-NOD32 (ESET-NOD32): a variant of
Android/TrojanDownloader.Agent.UN
Avast (Avast): Android:Metasploit-G [PUP]
Cynet (Cynet): Malicious (score: 99)
Kaspersky (Kaspersky): HEUR:Trojan-Downloader.AndroidOS.Agent.jy
Rising (Rising): Downloader.Agent/Android!8.3A1 (KTSE)
F-Secure (F-Secure): Malware.ANDROID/Agent.FJNR.Gen
DrWeb (DrWeb): Android.RemoteCode.6833