Shifu's Squad

NetSpect

KVH-015: Mesh Network Detection

Enabling Cyber Intelligence through SaaS

Ghanashyam Bhat

Karan Bhat Sumbly

Prajwal Bhat

Vijit Kumar

Niveditha Kundapuram

Adarsh Kumar

Problem

Illicit Usage of Mesh Networks

Where there's GOOD, there's BAD

No connectivity with cellular networks

No requirement to connect to the Internet

Similar frequency range as Wi-Fi and Bluetooth

Makes distinguishing mesh network packets is diffcult

Dynamic status of nodes

Nodes leave and join the network dynamically; difficult to track

Exisiting Scenario

DRUG TRAFFICKING

communicate and coordinate drug trafficking activities without being traced or intercepted

TERRORIST ACTIVITIES

communicate and plan attacks without being detected

INDUSTRIAL ESPIONAGE

Illicit gathering and sharingof business information

CYBERCRIMINAL ACTIVITIES

to conduct cyber-attacks, distribute malware, launch phishing scams, to share copyrighted material without permission, etc.

Utopia

Creation of private mesh network

- configured network interfaces to Ad-hoc mode
- Nodes configured to the same cell number

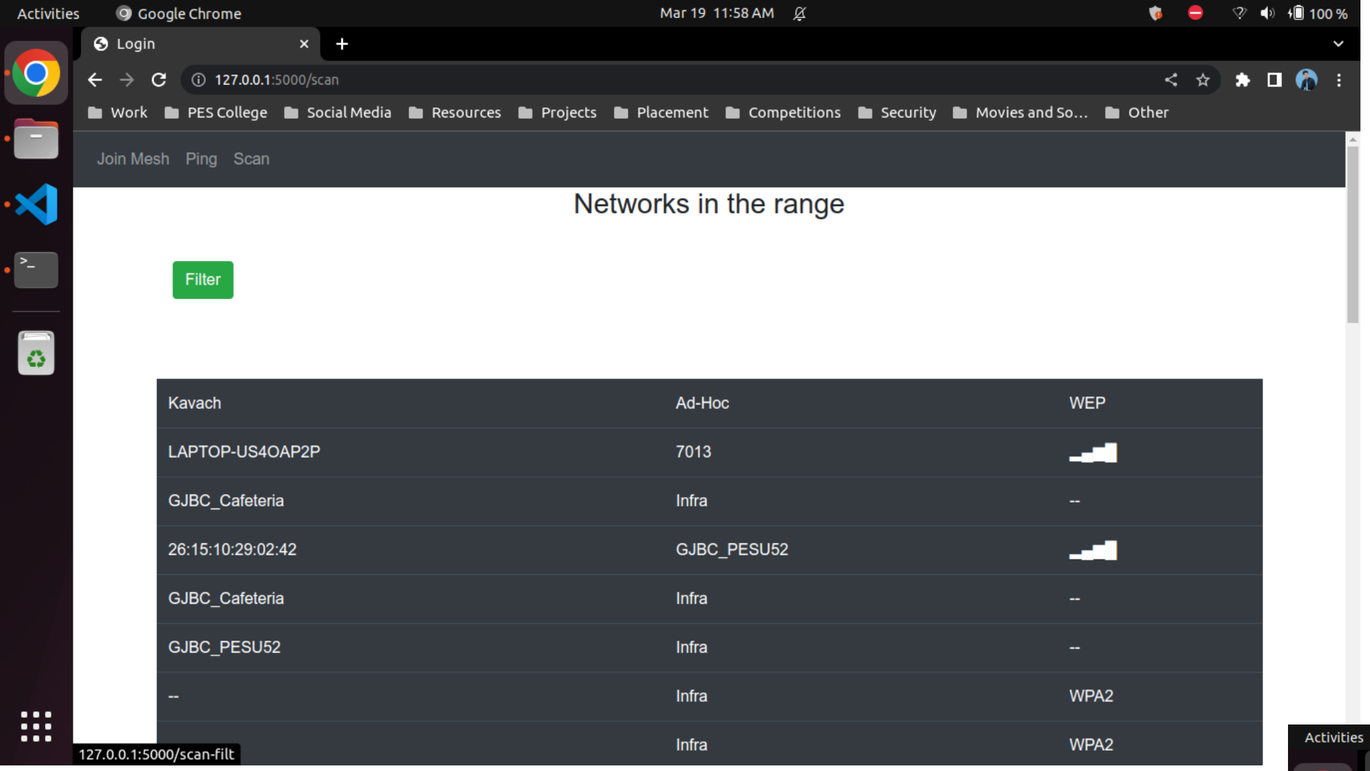
Wi-Fi vs Mesh Ad-hoc Packet Analysis

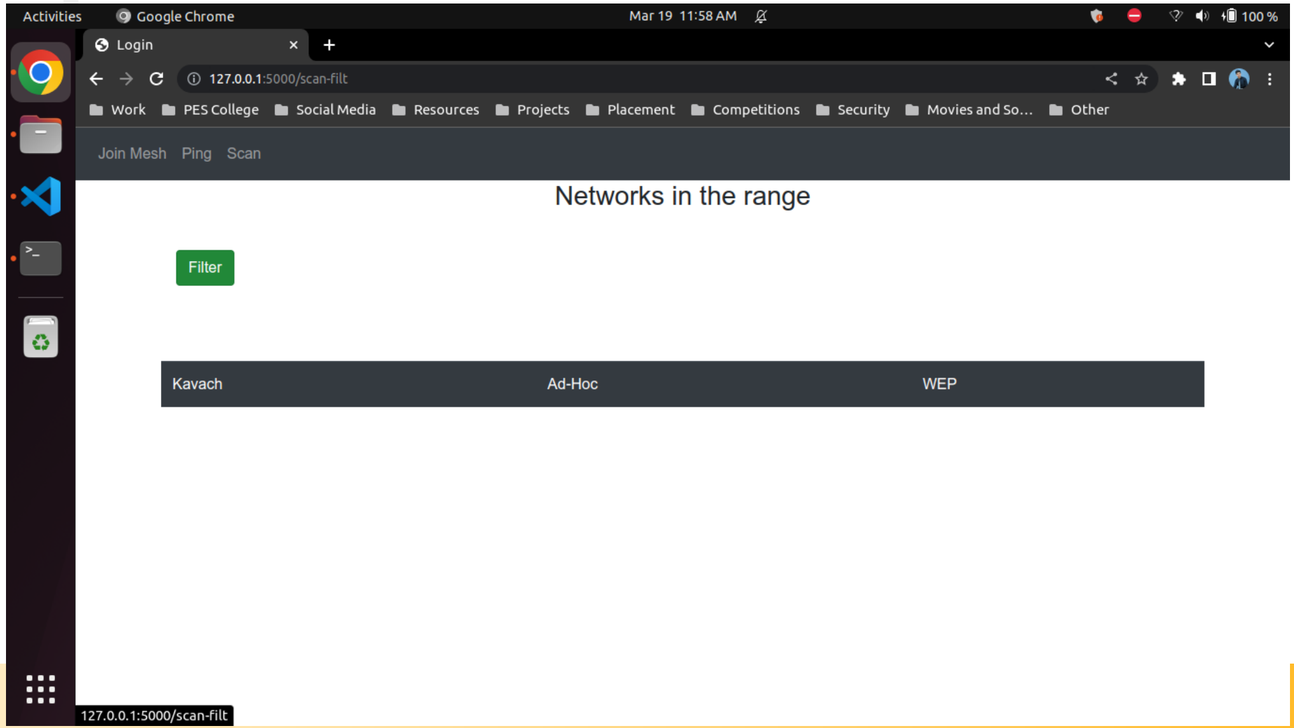
- Additional MDNS layer (active)
- Broadcast Properties: identify properties to differentiate

Statistical Network Analysis

- Traffic pattern and network usage
- Deduce potential threats
- Disrupt network

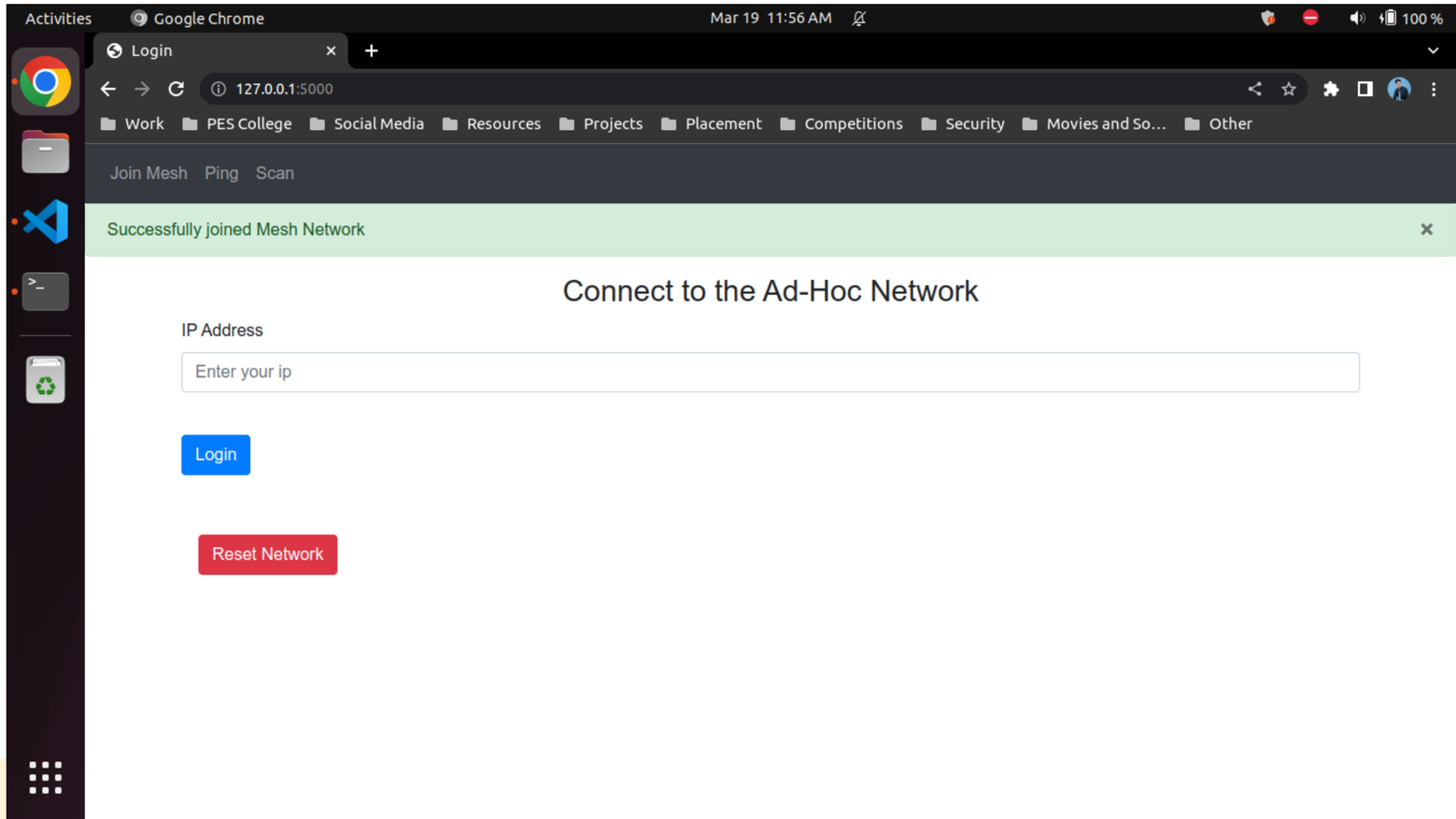
Demonstration



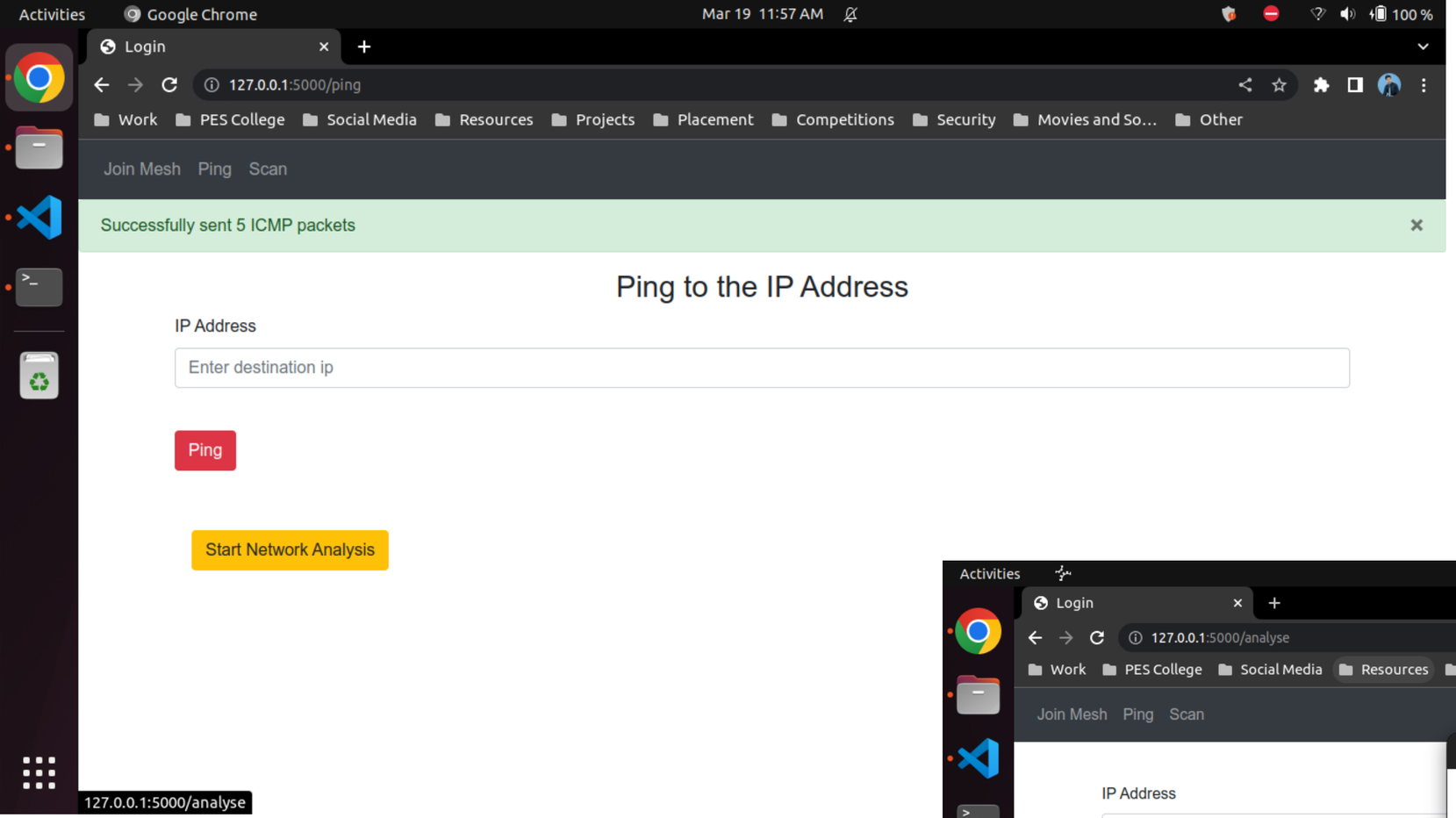


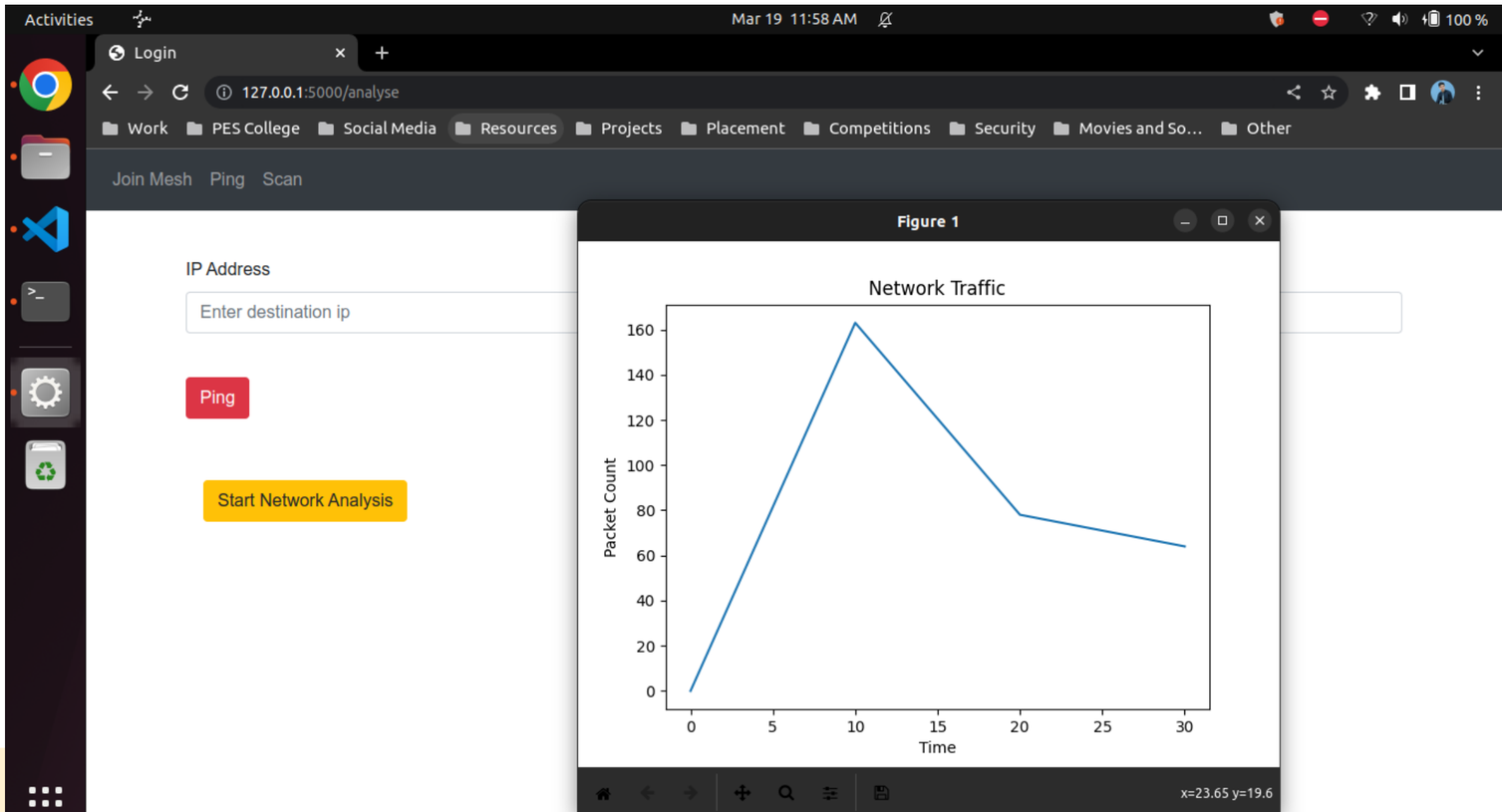
```
                                [00:00:00] Tested 127062 keys (got 10451 IVs)

KB    depth   byte(vote)
 0    1/ 23   12(15104) E0(14848) 2D(14336) 23(14080) B1(13824) 39(13568) 69(13568) 7C(13568) B9(13568) 09(13312) 43(13312)
 1    0/  2   34(17408) A8(14848) 1C(14592) 85(14592) F1(14592) BB(14336) F3(14336) 86(14080) B1(14080) 2C(13824) 7E(13824)
 2    6/ 25   56(14080) 01(14080) 42(13824) 5F(13824) 0A(13824) 26(13824) 38(13568) AD(13568) DA(13568) 75(13312) BF(13312)
 3   10/ 12   C8(13312) 14(13056) 3C(13056) 69(13056) 6A(13056) 8A(13056) 1A(12800) 2B(12800) 64(12800) 68(12800) 83(12800)
 4    0/ 10   90(16128) 12(15360) D4(15104) B8(14848) 20(14592) C3(14592) CE(14336) AC(14080) 2F(13824) C0(13824) 36(13568)

                     KEY FOUND! [ 12:34:56:78:90 ]
     Decrypted correctly: 100%
```

Demonstration



Demonstration





Target Market

Armed Forces & Law Enforcement Agencies

- Police

- Border Security Force (BSF)

- Anti-Naxalite Forces (ANF), Special Task Forces (STF) and Commando Battalion for Resolute Action (CoBRA)

Institutions & Business Organisations

- Offices, universities, etc

Revenue

The State and Central Governments

Half-annual and annual based subscriptions - region specific

Institutions & Business Organisations

SaaS based payments

Future Roadmap

STEP 1

Develop more robust algorithms for packet classification

STEP 2

Use GPU for brute force password cracking

STEP 3

Implement GIS to get precise location of nodes

STEP 4

Prototype conversion to portable devices

Technical Details

Application

locally deployed

Front-end

- HTML/CSS
- Jinja

Password Decryption

- Aircrack-ng
- Monitor Mode Adapter

Back-end

- Flask
- Shell Scripting
- Python
- Networking Frameworks

The Team