National University of Computer and Emerging Sciences
Islamabad Campus

Project Phase-1
Proposal

Network & Cyber Security - I

(Cyber Security-T)

20i-1797 Muhammad Usman Shahid
20i-0941 Muhammad Ismail Ramzan
20i-1794 Musaab Imran

Submitted to: **Dr. Zanaib Abaid**

Project Proposal

Group members:

- **20i-1797 Muhammad Usman Shahid**
- **20i-1794 Musaab Imran**
- **20i-0941 Muhammad Ismail Ramzan**

Task – 1

Provide a 1-page proposal of your selected project, explaining the overall aims and achievable targets. You should concisely explain the motivation for your project (i.e. why it is a suitable project), and describe the real world problem you are trying to solve or the security scenario you are trying to demonstrate using the skills acquired in this course. You need to outline all the main features of your project (e.g. if it is a secure encrypted chat application, describe what menus and options it will provide to the user and what authentication and encryption algorithms you will cover). The scope of your project should be clearly understandable from the description.

Project Title:

Network Sniffer

Proposal:

- **Introduction**

we are making a network sniffer that is going to sniff the traffic of network. It will be detecting the following protocols:

- http
- https
- TLS
- TCP
- UDP
- DNS
- DHC
- ICMP
- SSL

It will be a command line application showing all features on a terminal. It will be application which will include the feature for attacker, cyber security analyst and a random user.

- **Features:**

This application will contain the following features mainly:

1. **Analyzes traffic:**

Will analyze traffic and will be able to differentiate the all above mentioned protocols. such that a terminal will be showing that a packet have the following protocols.

2. **Apply filters:**

This will allow user to apply the filters that in command line what he/she wants to see the packet. For example a user enters TCP then he will see only tcp packets similarly If he enters TCP and ICMP then only these two will be shown.

3. **Block websites**

Our sniffer will also allow to block some websites. for example if a user Don't want to go to YouTube.com he can block this specific website. so he will not be visiting there any more.

4. **Redirection to other websites:**

Sniffer will also have ability to redirect to some other website when a specified website is encountered. such that if a user sets that that redirect from YouTube to Twitter each time then when ever YouTube request will be encountered then redirection will be done to Twitter.

5. **Credential highlighter:**

Sniffer will also highlight the sensitive information packets. such that will highlight the password and usernames.

6. **Payload Detector:**

Will detect a java script code in the packets. And will be highlighted by the higlighter. Can be used by security analyst.

- **Aims and achievable targets**:

The main aim is to built an application that is much simpler to analyze the traffic and usable by all attackers, cyber security analyst, researchers, for people maintaining self security and for any user.

Will try to achieve all above targets mentioned, the filter , analyzer, blocker, redirector and highlighter.

- **Motivation:**

The main motivation was to learn the concepts of networks & protocols. To check how the protocols are working. To understand the TCP/IP model.

- **Implementation overview:**

We are gathered on to use the python for this. further more, we know about protocols mentioned above as discussed in class. Now we will think how to implement these and that is our main goal.

Task – 2

Provide group member details along with task distribution, i.e. consider your group as a team undertaking this project for timely delivery to a client. You should clearly allocate primary roles to each group member.

Group Member Name	Role / Tasks Allocated
Muhammad Ismail Ramzan	Analyze traffic, Block Website
Musaab Imran	Apply Filters, Redirect
Muhammad Usman Shahid	Credential highlighter, Payload Detector

Task – 3

In this section, you need to elaborate your project idea by mapping the below mentioned concepts to your project. You do not need to cover all of them. Please describe briefly how a particular concept will be applied in your project. This mapping may change in the next few weeks as you build and expand your project, but at this stage it should be elaborate enough to quantitatively monitor your project progress on weekly basis.

Topic	**Application in your project**
Different kinds of cyberattackers and attacks	MITM, eavesdropping
Malware infection, propagation, and payload	Payload detector
Cryptography	-
Web application basics, HTTP and session management	-
Web attacks (Authentication attacks, session hijacking, command injection)	Credential harvestor
Network basics: TCP, SSL/TLS, HSTS, DNS, ICMP, DHCP	yes
Network security (DoS/DDoS, DNS Poisoning, MITM attacks)	eavesdropping
Other topics not directly covered in the course	Sniffing, packet analysis