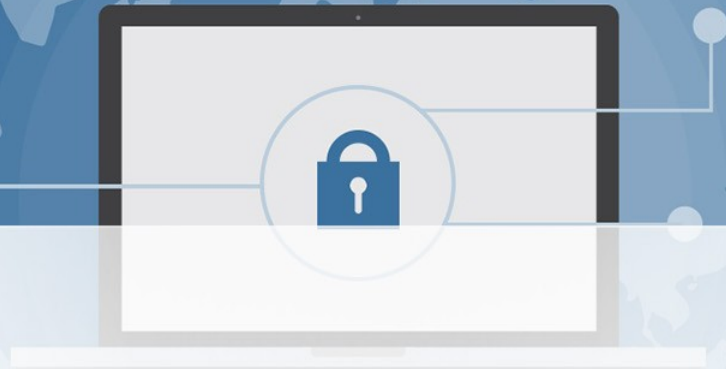# Automated Network Penetrator

Group Members : (1) Muhammad Zeeshan Ahmed
(2) Muhammad Abdul Wahab
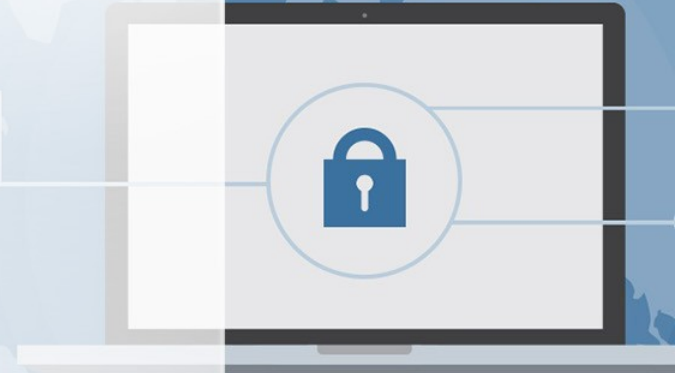
Supervisor: Dr. Saad A. Malik

Outline

- Introduction
- Significance
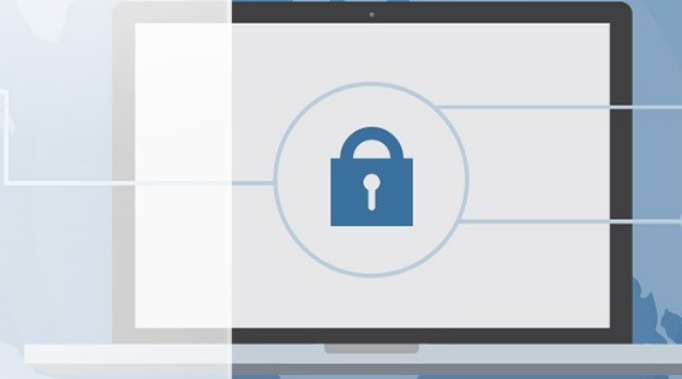- Background
- Progress
- Goals
- Timeline

Introduction

- Penetration (Exploitation of vulnerabilities present in an organization's network.)
- Ethical and Unethical
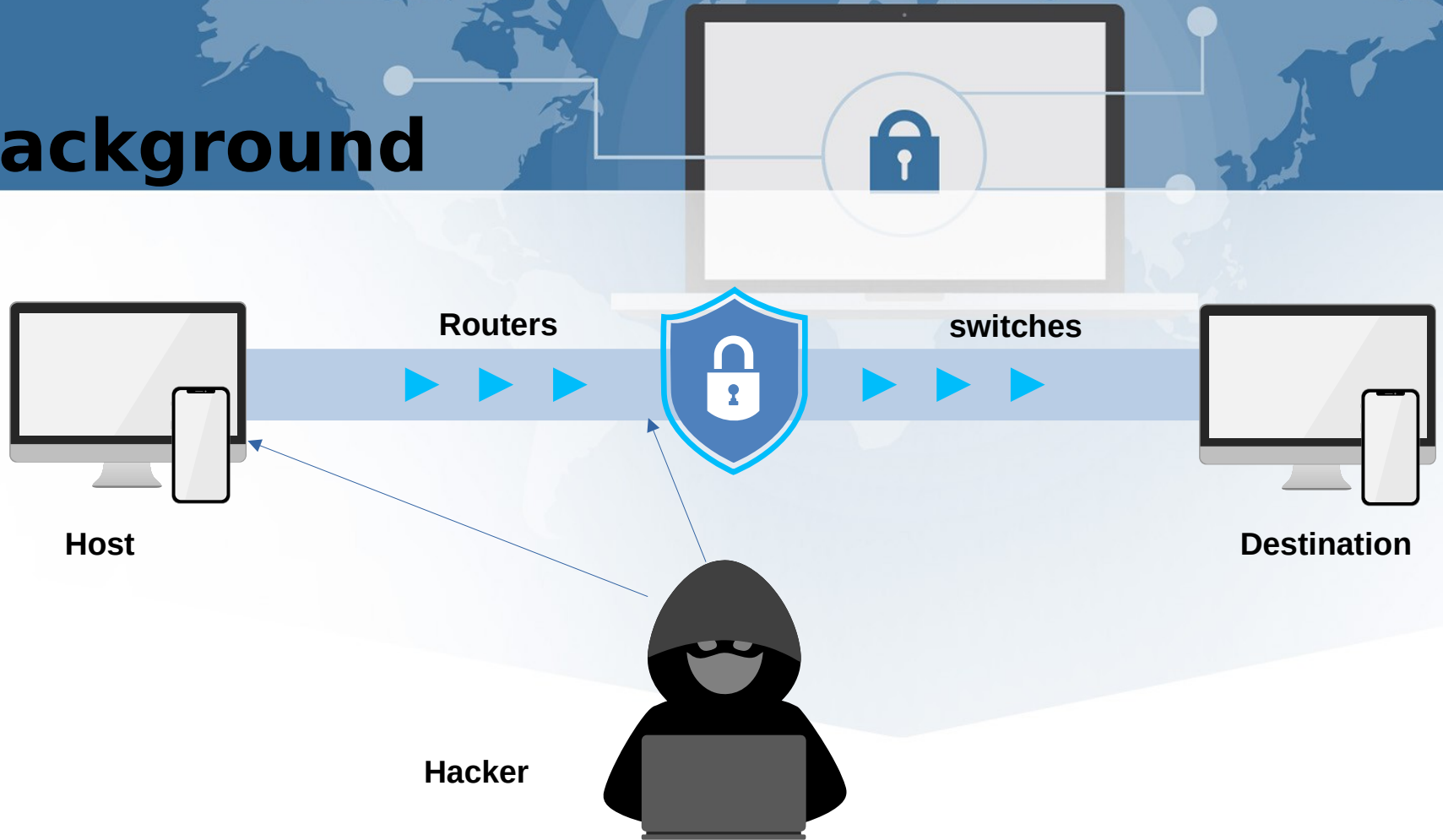- Can be Mobile application penetration or web application penetration
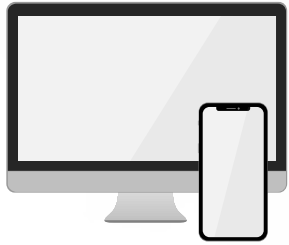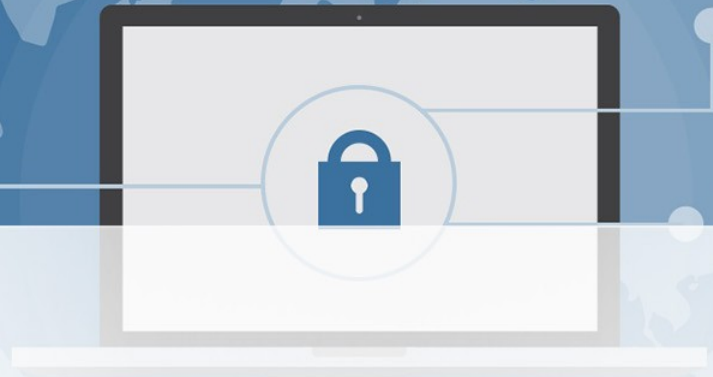
Significance

- Simulates the Hacking
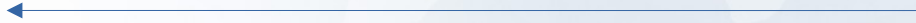- Exploitation tells the degree of vulnerability
- Helps to Secure the system

Background

Scope

Services

Hacker

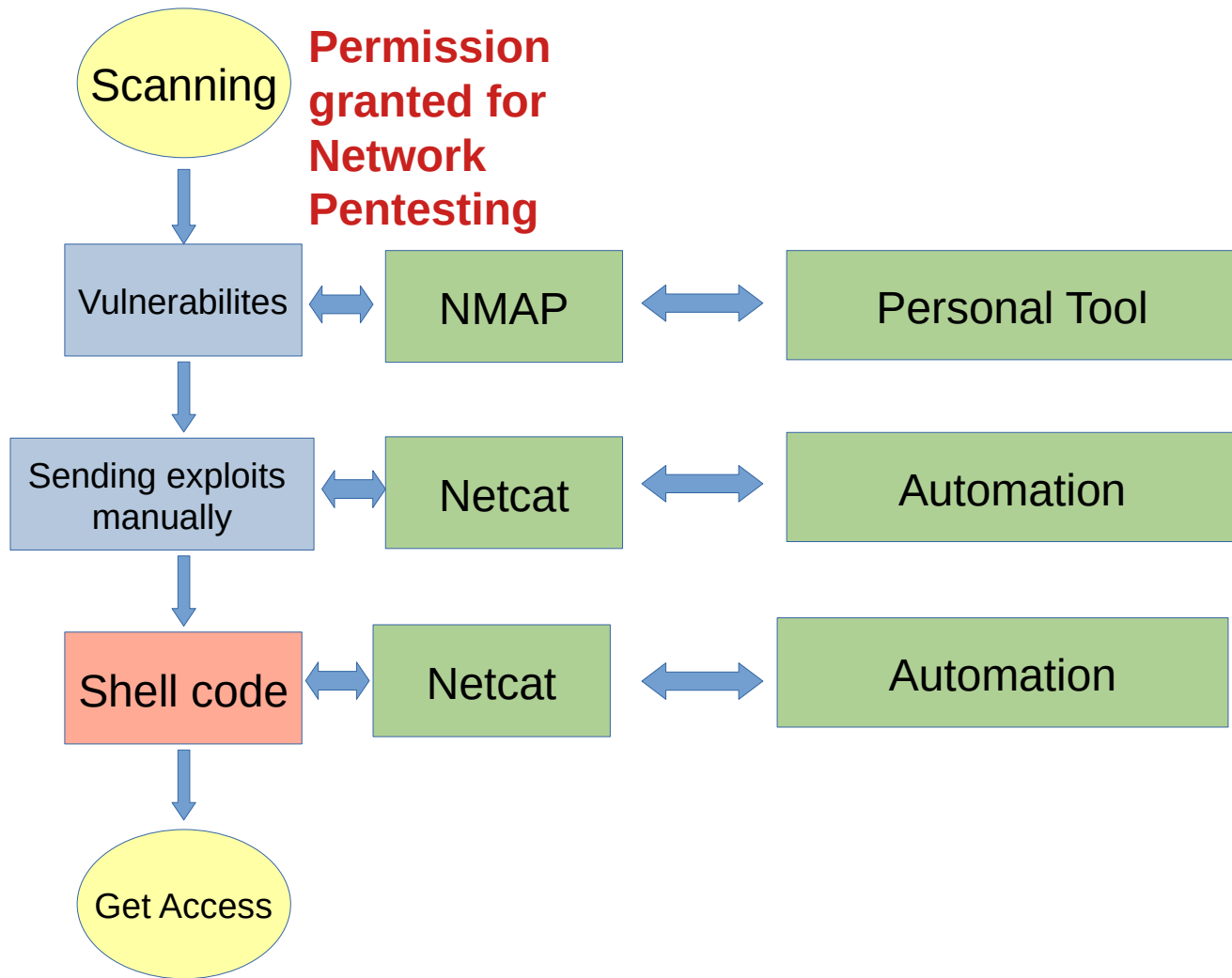# Progress

- Scanner
- Vulnserver
- TRUN
- Buffer++

Scanning

Permission granted for Network Pentesting

Vulnerabilites ⟷ NMAP ⟷ Personal Tool

Sending exploits manually ⟷ Netcat ⟷ Automation

Shell code ⟷ Netcat ⟷ Automation

Get Access

Progress

Spike and Boofuzz

Exploit Script ——— overwritten ———→

overwritten

EIP

ESP

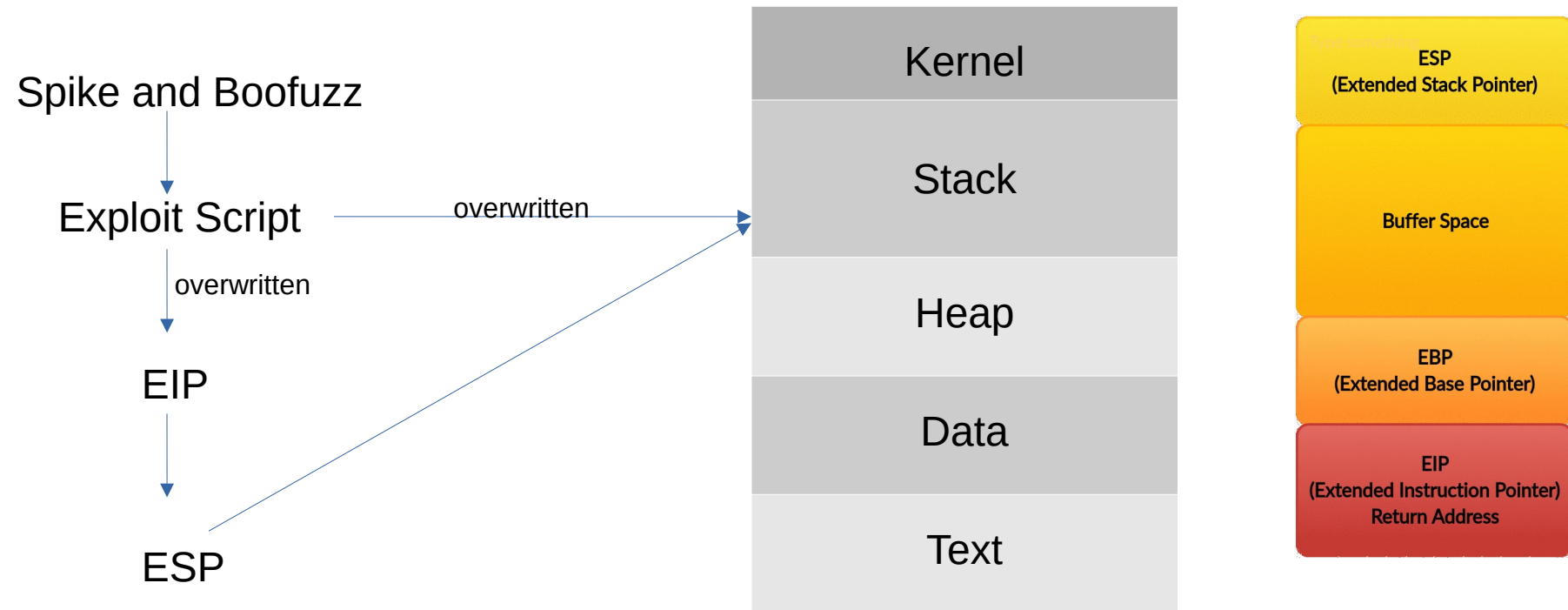| Kernel |
|---|
| Stack |
| Heap |
| Data |
| Text |

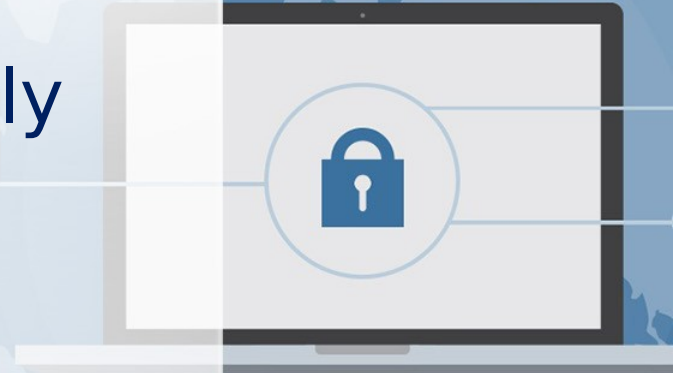| ESP (Extended Stack Pointer) |
|---|
| Buffer Space |
| EBP (Extended Base Pointer) |
| EIP (Extended Instruction Pointer) Return Address |

Goals

- Finding more vulnerablities
- Exploiting them Automatically
- Increasing the scope up to more services

Timeline

Sep 30

Writing parser

FYP Report

Mar 15

DEC 15

June 1

Literature review Lab setup

Vulnerability Report and FYP report