OCTOBER 16, 2021

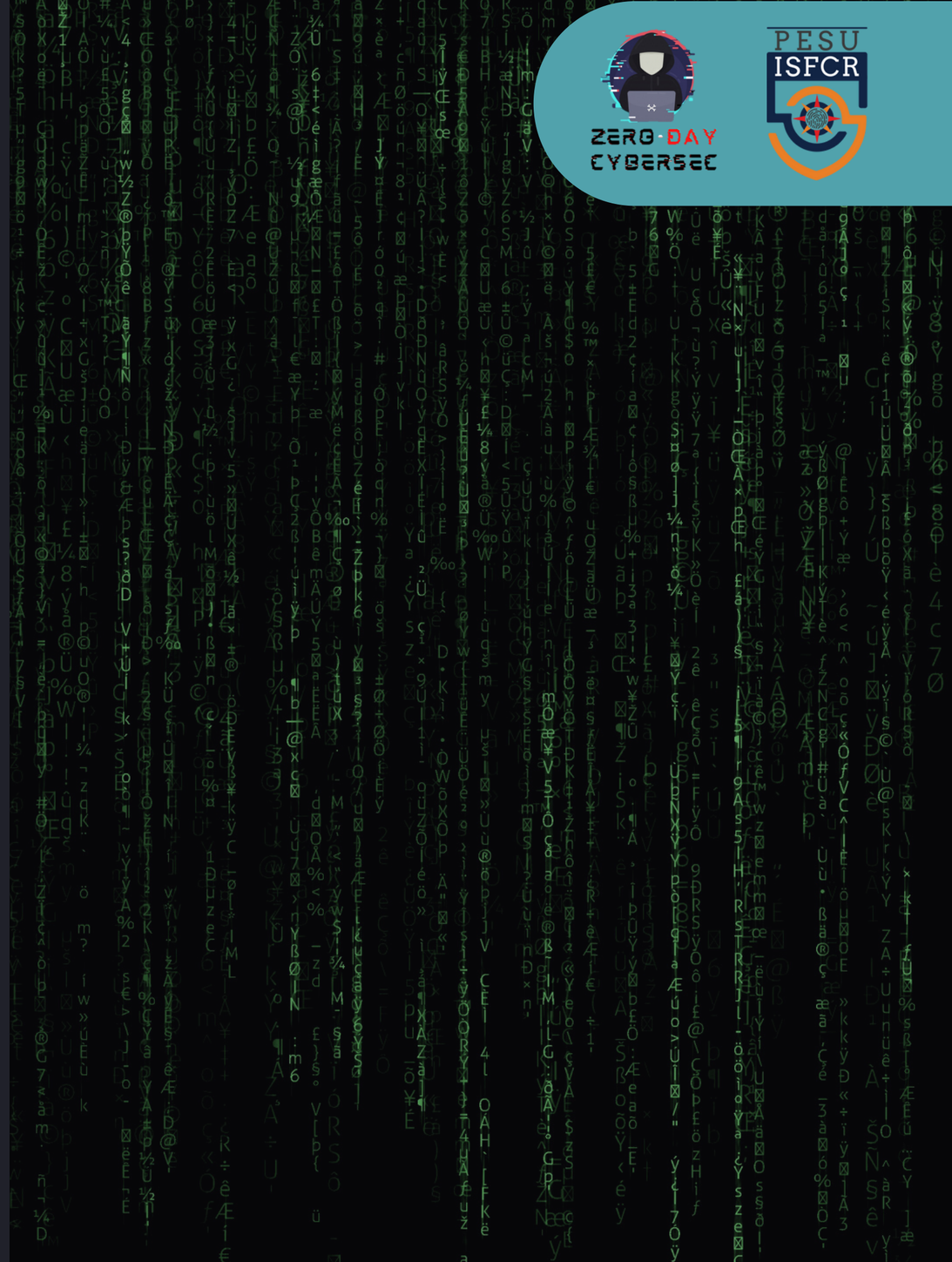
INTRODUCTION TO PENTESTING

Break your limits

Workshop Overview

Points of Discussion

- Definitions
- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks



Introduction

Setting Up Kali Linux / Parrot

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security.

Kali contains several hundred tools which are geared towards various information security tasks

What is Pentesting?

and why do it?

A penetration test is an authorized simulated cyberattack on a computer system/network,

Performed to evaluate the security of the system.

Happens on the mutual consent of the customer and the penetration testing provider

PENTESTING

Phases

- RECONNAISSANCE
- SCANNING
- GAINING ACCESS
- MAINTAIN ACCESS
- COVERING TRACKS

Recon

DEFINITION

Identifying which attacks can be launched and how likely the organization’s systems fall vulnerable to those attacks.

HOW

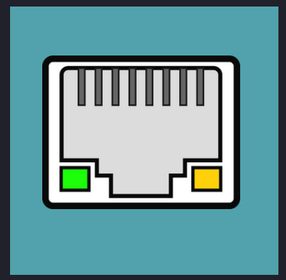
TCP and UDP services
Vulnerabilities
Through specific IP addresses
Host of a network

Scanning

Attackers try to find different ways to gain the target's information.

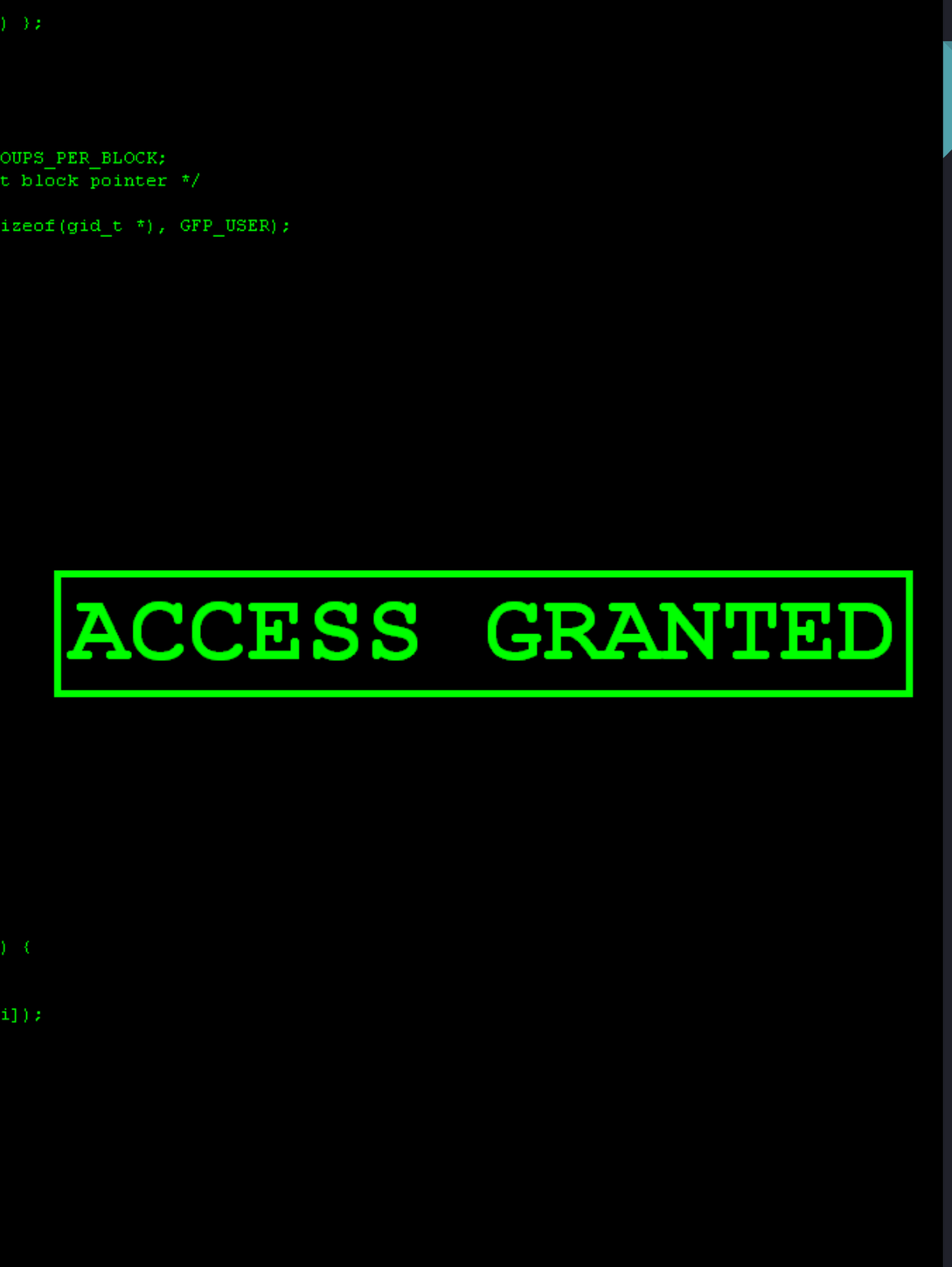
This phase is more tool-oriented rather than performed manually.

Vulnerability Scanning:
Nikto, Nmap



Port Scanning:
Nmap, Nnessus

Network Scanning:
Bettercap,**netdiscover**



Gaining Access

??

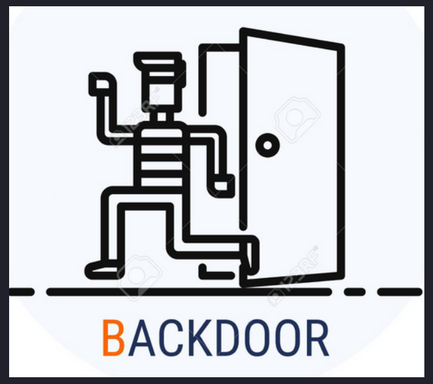
DEFINITION

Establish a connection with the target and exploit the vulnerabilities found in the previous phase

HOW

Exploiting Vulnerabilities and uploading reverse shells or getting command execution on Victim

Maintaining Access



PRIVILEGE ESCALATION

Get higher-level permissions on that machine to access as much data as possbile

POST EXPLOITATION

Extract meaningful information (Database Extraction) and further attacks (**DDoS** attacks, **Pivoting**)

PERSISTENCE

Maintain access for as long as possible (even after shutdown, etc) using **backdoors** and **trojans**

COVERING TRACKS

ENSURES THAT THE ATTACKERS LEAVE NO CLUES OR EVIDENCE BEHIND THAT COULD BE TRACED BACK.

EDITING, CORRUPTING, OR DELETING DATA

Access Logs and Bash History can be deleted with right permissions

REVERSE HTTP SHELLS

Reverse Shells are created from a remote machine instead of the attacker's.

TUNNELLING (VPN,ICMP)

Malicious data passing through the tunnel is hidden within normal-looking ICMP echo requests and echo responses.

Demo and Q&A

Any doubts / queries ?

THANK YOU!

VISIT US SOON.