

## Cyber Security Professionals

Cyber Security courses aims to equip students with the knowledge and skills required to defend the computer operating systems, networks and data from cyber-attacks.

Cyber Security as a profession is evolving over the years, reason being the increasing rate of cyber-crimes. Any industry that transacts online or carries sensitive data is in need of a Cyber Security professional to safeguard its date from such delinquents. Cyberspace being a common platform which is accessed anyone from every corner of the world, the scope of cybersecurity is equally spread across the globe.



**NETWORK RHINOS**

The Network Experts



Other Courses offered by Network Rhinos

CCNA

CCNP

CCIE

Python

Linux

AWS

# Module 1: Security Risk Assessment (Ethical Hacking)

## Introduction to Ethical Hacking

- What is Hacking
- What is Ethical Hacking
- What is Penetration Testing
- What is Vulnerability Auditing

## Footprinting

- What is FootPrinting
- Footprinting Techniques
- Footprinting Website & Tools

## Scanning

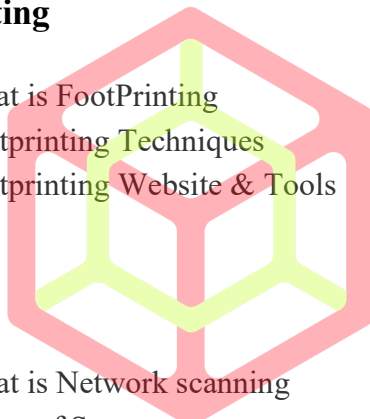
- What is Network scanning
- Types of Scanners
- Vulnerability Scanner Tools

## Proxy

- What is a proxy server
- Types of proxies
- What is a Darkweb
- Why hackers prefer to use Darkweb

## Hacking Web Servers & Web Applications

- What is a web server
- Types of web attacks



**NETWORK RHINOS**

The Network Experts

## **Session Hijacking**

What is session hijacking  
Session hijacking Techniques  
Session hijacking Tools

## **Denial of Service**

What is a DoS and DDoS attack  
DoS attack techniques  
DoS attack Tools

## **System Hacking**

What is System Hacking  
What is Password Cracking  
Password Cracking techniques  
Password Cracking Website & Tools



# NETWORK RHINOS

## **Sniffers**      The Network Experts

What is a sniffer  
Sniffing Techniques  
Sniffing Tools

## **Phishing**

What is Phishing  
Phishing Techniques  
Phishing Tools

## **Malware**

What is malware

Types of malware  
Malware creation Tools  
USB password stealers

## **Wireless Hacking**

Types of wireless networks  
Wireless Hacking Techniques  
Wireless Hacking Tools

## **Kali Linux**

What is Kali Linux  
Kali Linux Tools

# **Module 2 Web Application Penetration Testing**

## **Introduction to Pen testing**

WAPT Methodology  
Phases of Pen Testing  
WAPT Standards

OWASP  
SANS  
WASC

**NETWORK RHINOS**

The Network Experts

## **Introduction to Web Applications**

Working of web applications  
HTT Protocol  
HTTP Request  
HTTP Response  
HTTP Methods  
HTP Status Codes  
Client Server Communication  
HTTP Security (HTTPS)  
Web servers  
Application servers

Data base servers

## **Burp Suite**

Introduction to Burp Suite

Lab Setup

Working of proxy in Burp Suite

Working of Intruder in Burp suite

Working of Repeater in Burp Suite

Different Attack Types(sniper, Battering Ram, Pitch Fork and cluster bomb)

Encoders

Extender

Engagement Tools

## **SQL Injection**

Introduction to SQL

SQL Map

Practical POC

Authentication Bypass

Practical POC

Blind SQL Injection

Practical POC

Time Based SQL Injection

Practical POC

SQL Injection in Burp Suite

Practical POC

Authentication Bypass in Burp Suite

Practical POC

Challenges: Authentication Bypass

## **HTML Injection**

Introduction to HTML

HTML Tags

Working of Iframe

Types of HTML Injections

Stored HTML Injection

Practical POC  
Reflected HTML Injection  
Practical POC  
Iframe injection  
Practical POC  
Click Jacking  
Practical POC

## **Command Injection**

Introduction to Command Injection  
Command injection on DVWA  
Practical POC

## **Broken Authentication and Session Management**

Introduction to Session id's  
Cookies  
Browser Storage Mediums  
Local Storage and Session storage  
HTTP only Flag  
Secure Flag  
Broken Authentication  
Session Hijacking  
Practical POC  
Session Replay  
Practical POC  
Session Fixation  
Practical POC  
Browser cache weakness  
Practical POC  
Testing for Account Lock out policy and strong password policies  
Practical POC

## **XSS Cross Site Scripting**

Introduction to XSS  
Introduction to Java Script  
Types of XSS  
Stored XSS

Practical POC  
Reflected XSS  
Practical POC  
DOM based XSS  
Practical POC  
Payload Writing

## **IDOR – Insecure Direct Object Reference**

Introduction to IDOR Vulnerabilities  
Web root Directories  
Directory Traversal  
Practical POC  
File Upload Vulnerability  
Practical POC  
Introduction to Netcat  
Working of Netcat  
File Inclusions  
Practical POC

## **Security Misconfiguration**

Introduction to Security Misconfiguration  
Directory Listing  
Dirbuster  
Practical POC  
Sensitive Information Disclosure through error messages  
Practical POC  
Unwanted Services running on the server  
Nmap scanning  
Practical POC

## **Sensitive Data Exposure**


Introduction to sensitive data Exposure  
Qualys SSL Labs  
Heart beat request  
Heart bleed Vulnerability  
Poodle attack  
HTTP Arbitrary Methods

Practical POC

## Missing Function Level Access Control

Introduction to Missing function Level Access Control  
Authorization checks  
Practical POC

## CSRF – Cross Site Request Forgery



Introduction to CSRF  
CSRF Vulnerability  
Anti CSRF tokens  
JTokens  
Same Origin Policy  
Practical POC 1  
Practical POC 2

## Using components with known Vulnerabilities

Introduction to using components with known vulnerabilities  
Wappalizer  
Practical POC 1  
Practical POC 2

## Unvalidated Redirects and Forwards

Introduction to Unvalidated Redirects and Forwards  
Host Header Injection  
Practical POC  
Cross Origin Resource sharing Vulnerability  
Practical POC

## Remote File Inclusions

Introduction to Remote File Inclusions  
RFI Attacks  
Practical POC



## XML Injections

Introduction to XML  
XML Injections  
Practical POC

## Security Headers



Strict-Transport-Security  
Content-Security-Policy  
X-Frame-Options  
X-Content-Type-Options  
Referrer-Policy  
Feature-Policy

## Vulnerability Analysis

Introduction to CVSS Scoring  
CVSS Calculation  
Risk Rating  
Severity level analysis  
Color coding

**NETWORK RHINOS**

The Network Experts

## Vulnerability Scanners

Demo: Nessus  
Demo: Burp Suite Professional  
Demo: OWASP ZAP  
Demo: Qualys SSL Scanner  
Demo: SQL Map Tool

## Mitigations

SQL Injection Mitigations  
Stored Procedure  
Parameterized procedure

Input Validation  
Mitigations to HTML Injection  
Mitigations to XSS  
Mitigations to Directory Traversal  
Mitigations to File Upload Vulnerability  
Mitigations to File Inclusion  
Mitigation to security Misconfiguration  
Mitigation to Sensitive Data Exposure  
Mitigations to Host Header Injection  
Mitigations to CROS  
Mitigations to RFI  
Mitigations to XML Injection

## Report Writing

Detailed Reporting of Vulnerabilities with Risk Rating  
Findings  
Mitigations  
Steps to Reproduce  
Support Evidence

# NETWORK RHINOS

The Network Experts