

# Certified Ethical Hacking With Penetration Testing

## CEHWPT

# Gamo@HP:~\$Whoami

## ❶ SPEAKERS INFO



### ■ MR. KHALED GAMO

Khaled Gamo is managing information Security of Almadar Aljadid, Almadar is first mobile operator in Libya. He was Director General of National Information Security & Safety Authority (NISSA). He holds a Bachelor's degree in communication engineering as well as Holding a series of certification in field IT and information security such as CEH, ECSA, CCIE security written exam, CCVP, CCNP, and CCNA. He has over 18 years of experience in the Telecom Sector and information technology he was working in Huawei Libya as Data communication product manager, also he was technology division manager in Libya post Telecommunication Company. Khaled was managing cyber security programs at national level including national cyber security strategy and building Libya-CERT. He was also involved in developing Cyber security legislation initiative in Libya.

<https://www.facebook.com/carthagearena/videos/1701847216530321/>

# SANS Cyber Security Roadmap

## Cyber Security Skills Roadmap

Explore this interactive training roadmap to find the right courses for your immediate cyber security skill development and for your long-term career goals. More than 60 courses deliver critical skills in the cyber defense operations, digital forensics, software development, and management practice areas of cyber security.

### 1. BASELINE SKILLS

**Core Techniques**  
Prevent, Defend, Maintain

2 COURSES

#### Every Security Professional Should Know

Security Essentials

[SEC401](#)

Hacker Techniques

[SEC504](#)

**Security Management**  
Managing Technical Security Operations

2 COURSES

### 2. FOCUS JOB ROLES

#### Monitoring & Detection

*Intrusion Detection, Monitoring Over Time*

2 COURSES

#### Penetration Testing

*Vulnerability Analysis, Ethical Hacking*

2 COURSES

#### Incident Response & Threat Hunting

*Host & Network Forensics*

3 COURSES

### 3. CRUCIAL SKILLS, SPECIALIZED ROLES

#### Cyber Defense Operations

*Harden Specific Defenses*

8 COURSES

#### Specialized Penetration Testing

*Focused Techniques & Areas*

7 COURSES

#### Threat Intel & Forensics

*Specialized Investigative Skills*

5 COURSES

#### Development & Secure Coding

4 COURSES

#### Industrial Control Systems

3 COURSES

CISSP® Training

[MGT414](#)

#### Advanced Management

*Advanced Leadership, Audit, Legal*

4 COURSES

# Eccouncil Cyber Security Roadmap



# Offensive of Security Cyber Security Roadmap

## MOST POPULAR

### FOUNDATIONAL COURSE

#### NETWORKS

Offensive Security Certified Professional  
**OSCP**

#### OFFICIAL CERTIFICATION COURSE

**Penetration Testing with Kali Linux (PwK)**  
*ONLINE TRAINING*

PwK is a foundational pentesting course that covers the latest tools and techniques while also training students to maintain an offensive mindset.

**ENROLL NOW**

### ADVANCED COURSE

#### WEB APPLICATIONS

Offensive Security Certified Web Expert  
**OSWE**

#### OFFICIAL CERTIFICATION COURSE

**Advanced Web Attacks & Exploitation (AWAE)**  
*ONLINE TRAINING*

AWAE is designed to specifically address the unique challenges and vulnerabilities associated with web application security and pentesting.

**ENROLL NOW**

### EXPERT COURSE

#### WINDOWS ENVIRONMENT

Offensive Security Certified Exploitation Expert  
**OSEE**

#### OFFICIAL CERTIFICATION COURSE

**Advanced Windows Exploitation (AWE)**  
*LIVE TRAINING*

AWE is an advanced course that requires experienced exploit developers to execute complex exploits within the modern Windows Environment.

**VIEW COURSE**

# Mile2 Cyber Security Roadmap

Career Area	Fundamental	Foundational	Specialized	Advanced
Security Awareness	<b>C)SA1™</b>	<b>C)SA2™</b>		
IS Management Leadership	<b>C)SP™</b>	<b>C)ISSO™</b>	<b>IS<sup>20</sup> CONTROLS™</b>	<b>C)SLO™</b>
Pen Testing & Hacking	<b>C)VA™</b>	<b>C)PEH™</b>	<b>C)PTE™</b>	<b>C)PTC™</b> <b>C)PSH™</b>
Incident Handling	<b>C)SP™</b>	<b>C)ISSO™</b>	<b>C)IHE™</b>	
Forensics	<b>C)SP™</b>	<b>C)DFE™</b>	<b>C)VFE™</b>	<b>C)NFE™</b>
Disaster Recovery	<b>C)SP™</b>	<b>C)ISSO™</b>	<b>C)DRE™</b>	
Healthcare	<b>C)SP™</b>	<b>C)ISSO™</b>	<b>C)HISSP™</b>	
Auditing	<b>C)SP™</b>	<b>C)ISSO™</b>	<b>C)ISMS-LA™</b> <b>C)ISMS-LI™</b>	<b>C)ISSA™</b>

# Course Modules

Introduction To  
Ethical Hacking

Introduction To  
Linux system

Reconnaissance  
Phase

Enumeration  
Phase

Scanning  
Phase

System Hacking  
Phase

Working With  
Exploit Tools

Social  
Engineering

Hacking Web  
Applications

Hacking Web  
Servers

Complete  
Pentest Report

CTF Challenge

# Course Strategy

Having  
Fun

More & More  
Practice &  
Exercises

CTF  
Scenarios

Explaining  
subject  
Practice it

Exercise Every  
Day as Home  
work

Using  
Cyber ranges

The Truth About Living in a  
Technology Based World

The global cybersecurity market is set to grow from its current market value of more than \$120 billion to over \$300 billion by 2024, according to a new research report by Global Market Insights.

The Estimated Annual Cost of  
Global Cybercrime Is  
\$375 Billion



# Yearly Cyber Crime Victim Count Estimates

Victims Per YEAR:



566 Million

# Yearly Cyber Crime Victim Count Estimates

Victims Per DAY:



1.5 Million

# Yearly Cyber Crime Victim Count Estimates

Victims Per SECOND:



18

# Yearly Cyber Crime Victim Count Estimates

Number of Identities Exposed:



Over 657  
Million





# How Protected Do You Feel?



# CYBERTHREAT REAL-TIME MAP

EN

Download Trial

MAP STATISTICS DATA SOURCES BUZZ WIDGET

Share f t



DEMO OFF



401931 187238 16141 128375 230273 4295 969687 68

OAS ODS MAV WAV IDS VUL KAS BAD

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on [more information](#).

ACCEPT AND CLOSE



LOCAL TIME

2:51:53

ATTACKS TO  
84,8FIREEYE CYBER  
GERMANY  
THREAT MAP

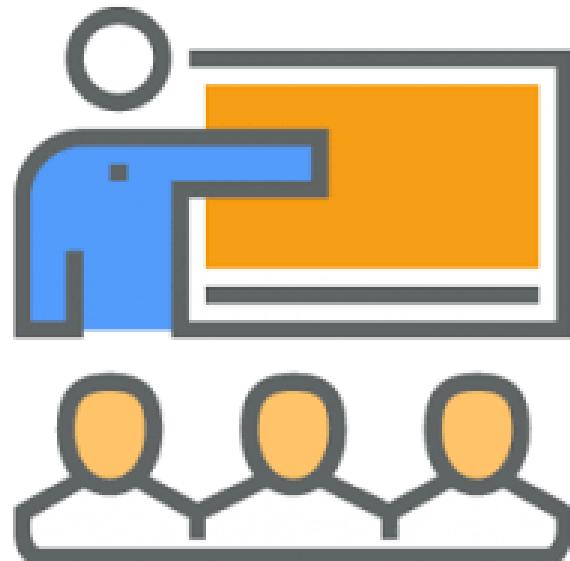
Please resize the browser window

or

[VIEW FULL SCREEN](#)

The "FireEye Cyber Threat Map" is based on a subset of real attack data, which is optimized for better visual presentation. Customer information has been removed for privacy.

# “ Who Should Attend This Course “



- Security Officers
- Auditors
- Security Professionals
- Site Administrators
- Any person that might be worried about the integrity of their network infrastructure

# What's Expected of You

# Code of Ethics

<http://www.eccouncil.org/Support/code-of-ethics>

- ❑ Privacy
- ❑ Intellectual property
- ❑ Disclosure
- ❑ Areas of Expertise
- ❑ Unauthorized Usage
- ❑ Illegal Activities
- ❑ Authorization
- ❑ Disclosure
- ❑ Management
- ❑ Knowledge Sharing
- ❑ Confidence
- ❑ Extreme Care
- ❑ Malicious Activities
- ❑ No Compromise
- ❑ Legal Limits
- ❑ Involvement
- ❑ Underground Communities



Practice builds knowledge, knowledge  
builds confidence

— SuperDale



# Time to Start “Thinking” like a Hacker



- Hacking vs. Ethical Hacking
- Fundamentals of Information Security
- Terminology
- The Technology Triangle

# Hacking vs. Ethical Hacking

“Ethical Hacking”  
really?

Define hacking

Internet crimes

Intellectual  
property

# Fundamentals of Information Security

Authenticity

Integrity

Availability

Confidentiality

Non-repudiation

# Speak like a Hacker



Exploit

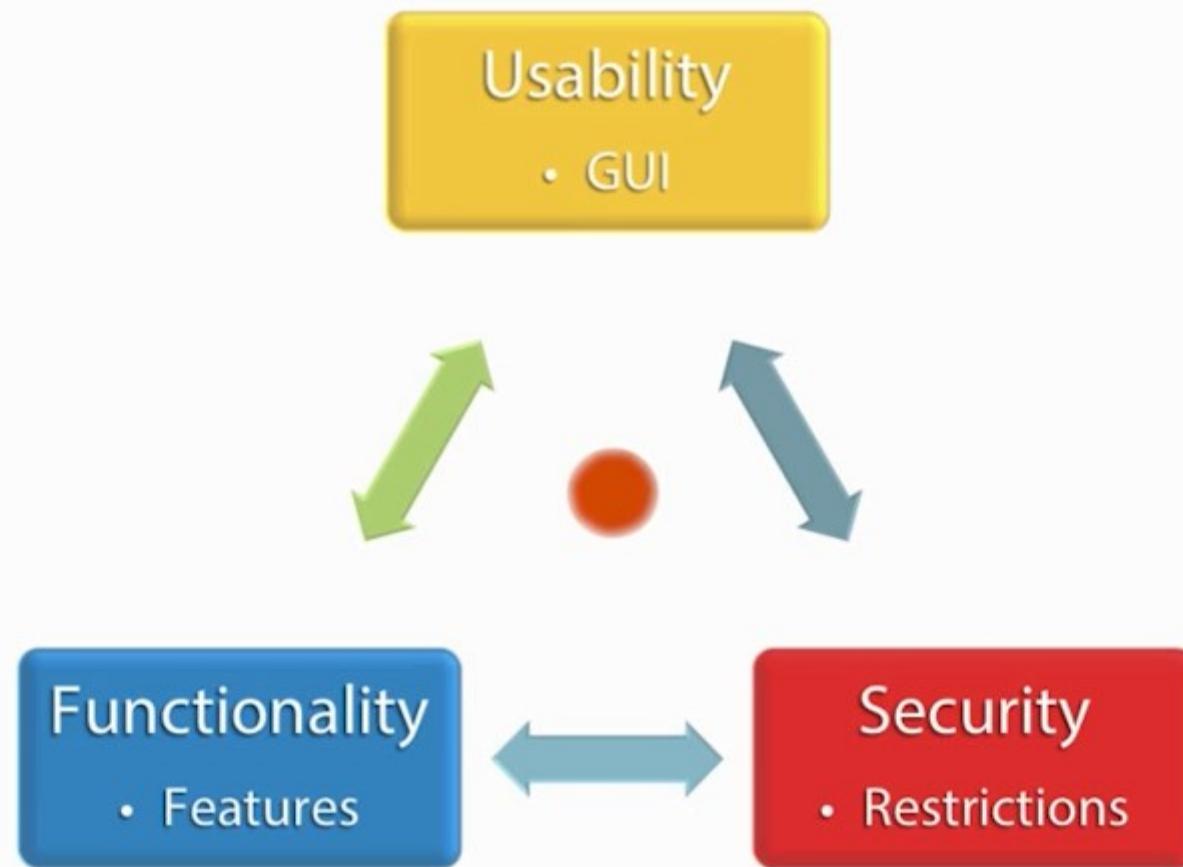
Hack value

Vulnerability

Target of Evaluation

Zero-day Attack

# The Technology Triangle



# Security Threats and Attack Vectors

# Security Threats

**“What Could Possibly Be a Threat in My Network?”**

# Security Threats

Hosts

Natural

Physical

Applications

Human

Network

# Hosts



Footprinting



Physical Security



Passwords



Malware

# Hosts



Denial of Service



Unauthorized  
Access

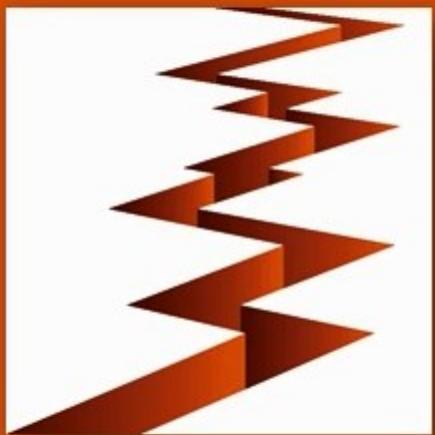


Privilege Escalation



Back Doors

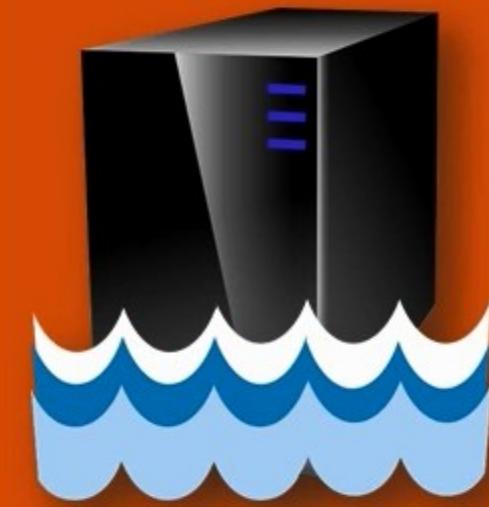
# Natural



Earthquakes



Hurricanes



Floods

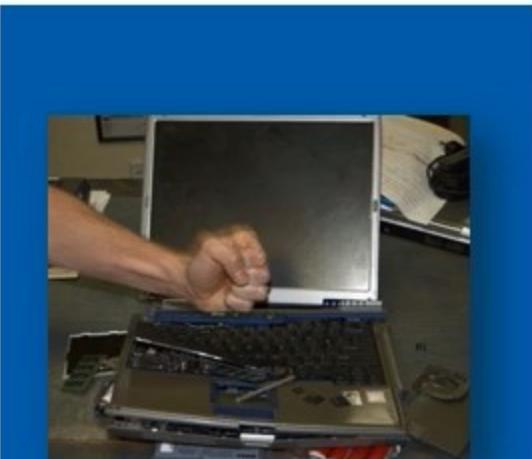


Natural Disasters

# Physical



Theft



Impact



Power



End of Life

# Applications



Configuration



Buffer Overflow



Lazy Coding

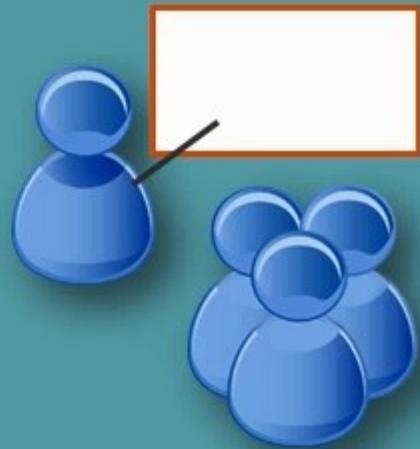


Data/Input  
Validation

# Human



Malicious  
Employees



Lack of Training



Social Networking



Hackers

# Network



Sniffing /  
Eavesdropping



ARP Poisoning



DoS



Spoofing

# Where Do Most Attacks Come From?

External

Foreign Countries

Internal

# How Many Attack Vectors Are You Aware Of?

- VM & Cloud environments
- Unpatched OS/software
- Social networking
- Internal users
- Hackivism
- Malware
- Botnets
- Security staffing
- Lack of security policies
- Compliance with regulations/laws
- Complexity of network infrastructure
- Mobile devices

# How Many Attack Vectors Are You Aware Of?

- Auto configuration
- Incompatibility of logging systems
- Default activation
- Shortcuts
- Bigger headers
- 4to6 translation
- Multiple IP's per device
- Network discovery

# Hacking Concepts



Hacking is exploiting security controls  
either in a technical, physical or a human-  
based element

— **Kevin Mitnick**



# Who? What? Where?



What is hacking?

What's an Ethical Hacker?

Types of hackers?

Why do they hack?

How does hacking influence companies?

# Hacking Defined:

Exploiting a Systems Vulnerabilities  
and Security Controls to Gain Access  
to System Resources and Features,  
Outside the Creator's Original  
Purpose.

# History of Hacking

In the beginning...

- 1970's



# History of Hacking

In the beginning...

- 1970's



# History of Hacking

In the beginning...

- 1970's
- 1980's

**the 10-Megabyte Computer System**



**Only \$5995 COMPLETE**

**New From IMSAI®**

- 10-Megabyte Hard Disk
- 5 1/4" Dual-Density Floppy Disk Back-up
- 8-Bit Microprocessor  
(Optional 16-bit Microprocessor)
- Memory-Mapped Video Display Board
- Disk Controller
- Standard 64K RAM  
(Optional 256K RAM)
- 10-Slot S-100 Motherboard
- 28-Amp Power Supply
- 12" Monitor
- Standard Intelligent 62-Key ASCII Keyboard (Optional Intelligent 86-Key ASCII Extended Keyboard)
- 132-Column Dot-Matrix Printer
- CP/M® Operating System

*You Read It Right ...  
All for \$5995!*

**IMSAI®** ...Thinking ahead for the 80's

**415/635-7615**

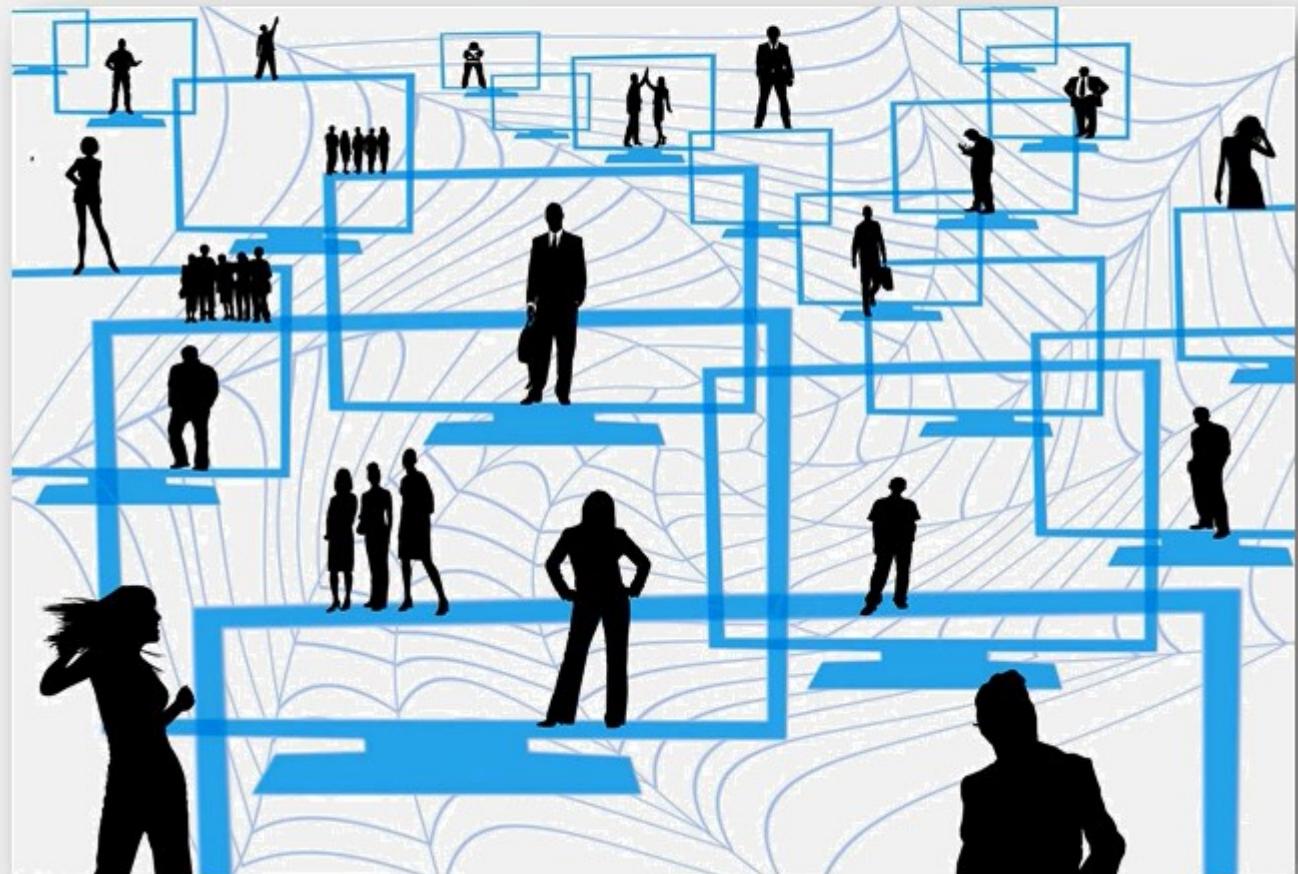
Computer Division of the Fischer-Freitas Corporation  
910 81st Avenue, Bldg. 14 • Oakland, CA 94621

\*CP/M is a trademark of Digital Research. Imsai is a trademark of the Fischer-Freitas Corporation

# History of Hacking

In the beginning...

- 1970's
- 1980's
- 1990's



# History of Hacking

In the beginning...

- 1970's
- 1980's
- 1990's
- 2000's



# History of Hacking

## In the beginning...

- 1970's
- 1980's
- 1990's
- 2000's

## Currently...

- DoS
- Stock Manipulation
- ID Theft / Credit Card Theft
- Piracy
- Theft of Services
- Vandalism

# Ethical Hacking Defined:

Involves the Use of Hacking Methods  
and Tools to Discover Weaknesses for  
System Security

# What Skills Should an Ethical Hacker Have?



Expert with  
Programs and  
Networks



Proficient with  
Vulnerability  
Research

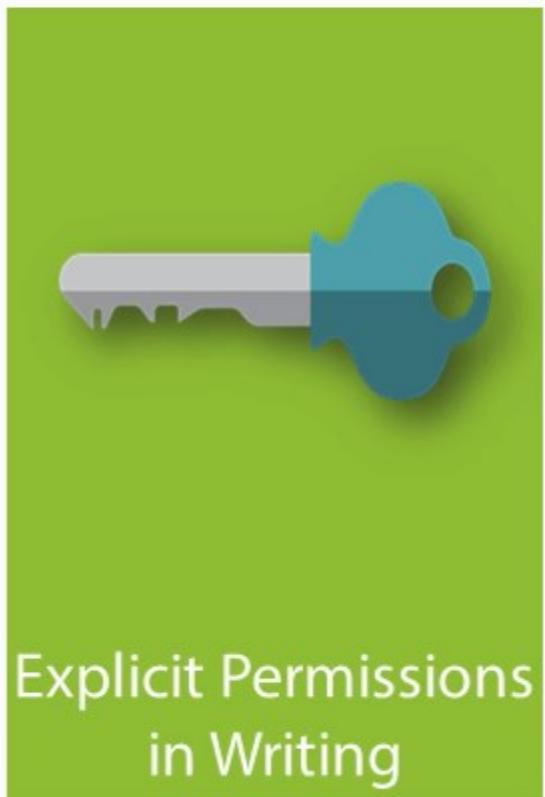


Mastery with  
Diverse Hacking  
Techniques

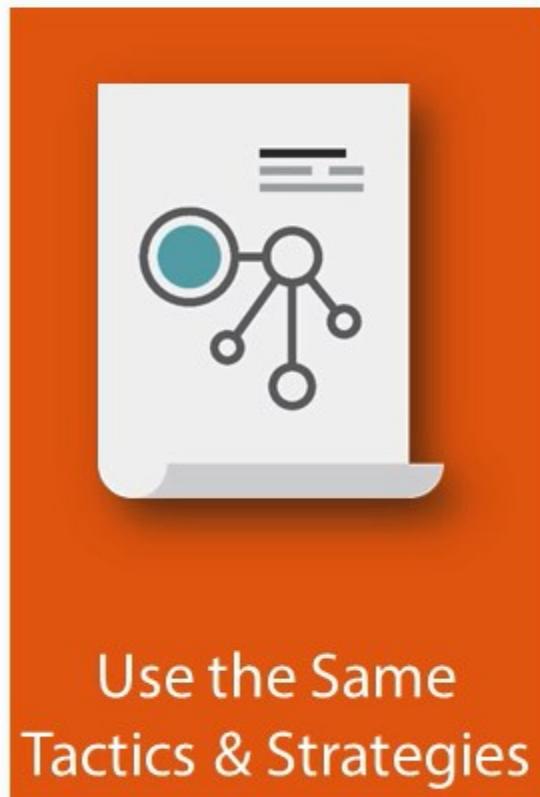


Follow a Strict Code  
of Conduct

# What Skills Should an Ethical Hacker Have?



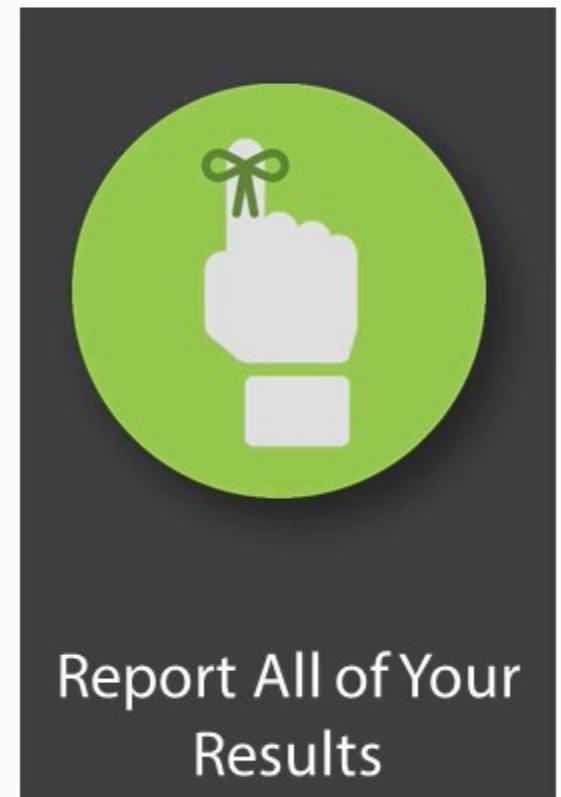
Explicit Permissions  
in Writing



Use the Same  
Tactics & Strategies



"No means NO!"



Report All of Your  
Results

# Types of Pen Tests

Black Box

Gray Box

White Box

# Why a Hacker Hacks



Hobby



Illegal Activities



Malicious Intent



Gain Knowledge

# Types of Hackers

Black Hats

White Hats

Gray Hats

Suicide Hackers

Script Kiddies

Spy Hackers / Cyber  
Terrorists / State  
Sponsored Hackers

# Hacktivism



Drive

Political / Social / Ideology / Vandalism /  
Protest / Humiliate

Political Agenda

Defacing or Disabling Websites

Targets

Government Agencies

Multinational Corps

"Wrong"

# How Does Hacking Influence Companies?



- Customer private information
- Intellectual property
- Down time / slow site
- Loss of revenues
- Financial information
- Reputation
- Loss of business

# Hacking Phases

# Summary



- Reconnaissance
- Scanning
- Gaining access
- Maintaining access
- Clear tracks

What is the MOST secure  
system?

The one that is never built

# You Can't Stop “Them”



Your job is to discourage, misdirect and slow them down

Time is NOT on your side

Attacker only has to find 1 opening  
You have to cover all of them

# The Phases

Reconnaissance

Scanning

Gaining access

Maintaining  
access

Clearing tracks

# Phase 2) Scanning



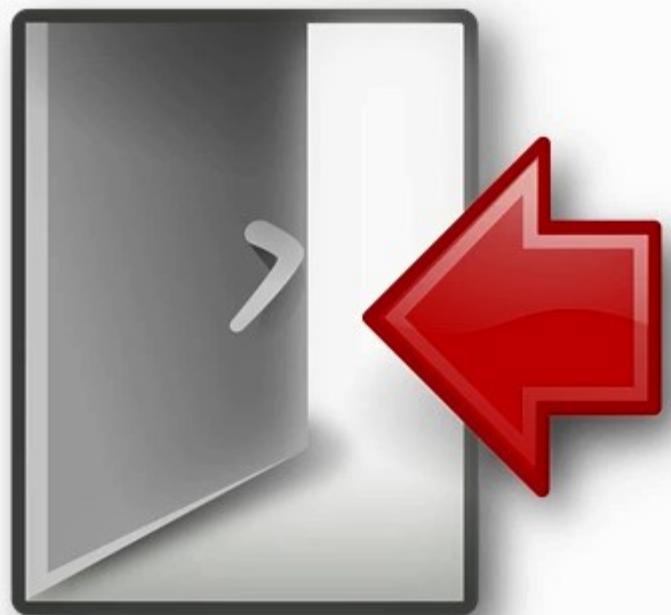
## Gather Info

- ID systems
- Vulnerabilities

## Tools Used

- Port Scanners
- Vulnerability Scanners

# Phase 3) Gaining Access



## Path

- Via network
- Via OS
- Via application
- Our goal?

# Phase 4) Maintaining Access

- ❑ PWNing the system
- ❑ Use system as a launch pad
- ❑ Inject Backdoor/Trojans
  - ❑ Used to revisit
  - ❑ Used to sniff/monitor network
- ❑ Use resources
- ❑ Harden up



# Phase 5) Clearing Tracks



“These are not the drones that you  
were looking for...”

- Destroy proof
- Hide my stuff
- Cyber blind

# Categories of Attacks



- Application attacks
- Misconfiguration attacks
- Shrink-wrap code attacks
- O/S attacks
- Entry Points

# Application Attacks

## Causes

- ❑ Time
- ❑ Features
- ❑ QA
- ❑ Add-on

## Results

- ❑ Buffer overflows
- ❑ Cross-site scripting
- ❑ Active content
- ❑ DoS and SYN
- ❑ SQL Injection

## Other App Attacks

- ❑ Session hijacking
- ❑ Man in the Middle
- ❑ Directory traversal

# Visual of Directory Traversal

The screenshot shows a web browser window titled "Index of /files - Iceweasel". The address bar displays the URL "natas2.natas.labs.overthewire.org/files/". The page content is an Apache directory listing for "/files". The table lists two files: "pixel.png" and "users.txt". The "users.txt" file contains the user list for the natas2 user.

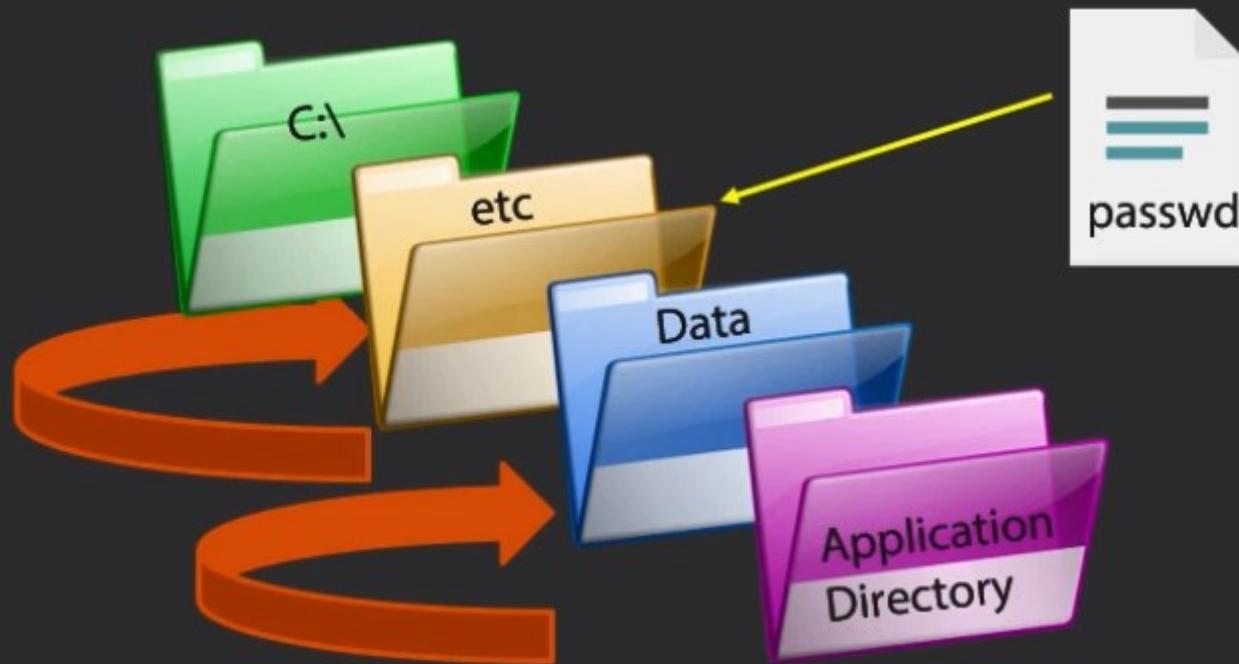
Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
 <a href="#">pixel.png</a>	06-Jun-2013 13:57	303	
 <a href="#">users.txt</a>	12-Jul-2013 13:35	145	

Apache/2.2.22 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80

# Visual of Directory Traversal

http://YourApplication.com

http://YourApplication.com/. . . /etc/passwd



# Misconfiguration Attacks



## Targets

- ❑ Web servers
- ❑ Application platforms
- ❑ Frameworks
- ❑ Databases
- ❑ Hardware

# O/S Attacks

Gaining access via  
vulnerabilities

O/S vulnerabilities via  
defaults

O/S attacks via non-  
updated systems

# Entry Points for an Attack

Remote Network  
Dial-Up Network

Local Network  
Stolen Equipment

Social Engineering  
Physical Entry

# Necessity of Ethical Hacking

# Rapid Growth in Tech = Trouble

## What Ethical Hackers do for companies

- Review systems and infrastructure
- Test current security
- Create solution
- Retest

You HAVE to answer questions like:

- What can be seen?
- What is being monitored?
- What can be done?
- Is there adequate protection?
- Are compliances met?

# What Skills You Must Have

# “I've Got Hacking Skills”

O/S Knowledge

Computer  
professional

Network guru

Security awareness

# “I've Got Hacking Skills”

Software  
knowledge

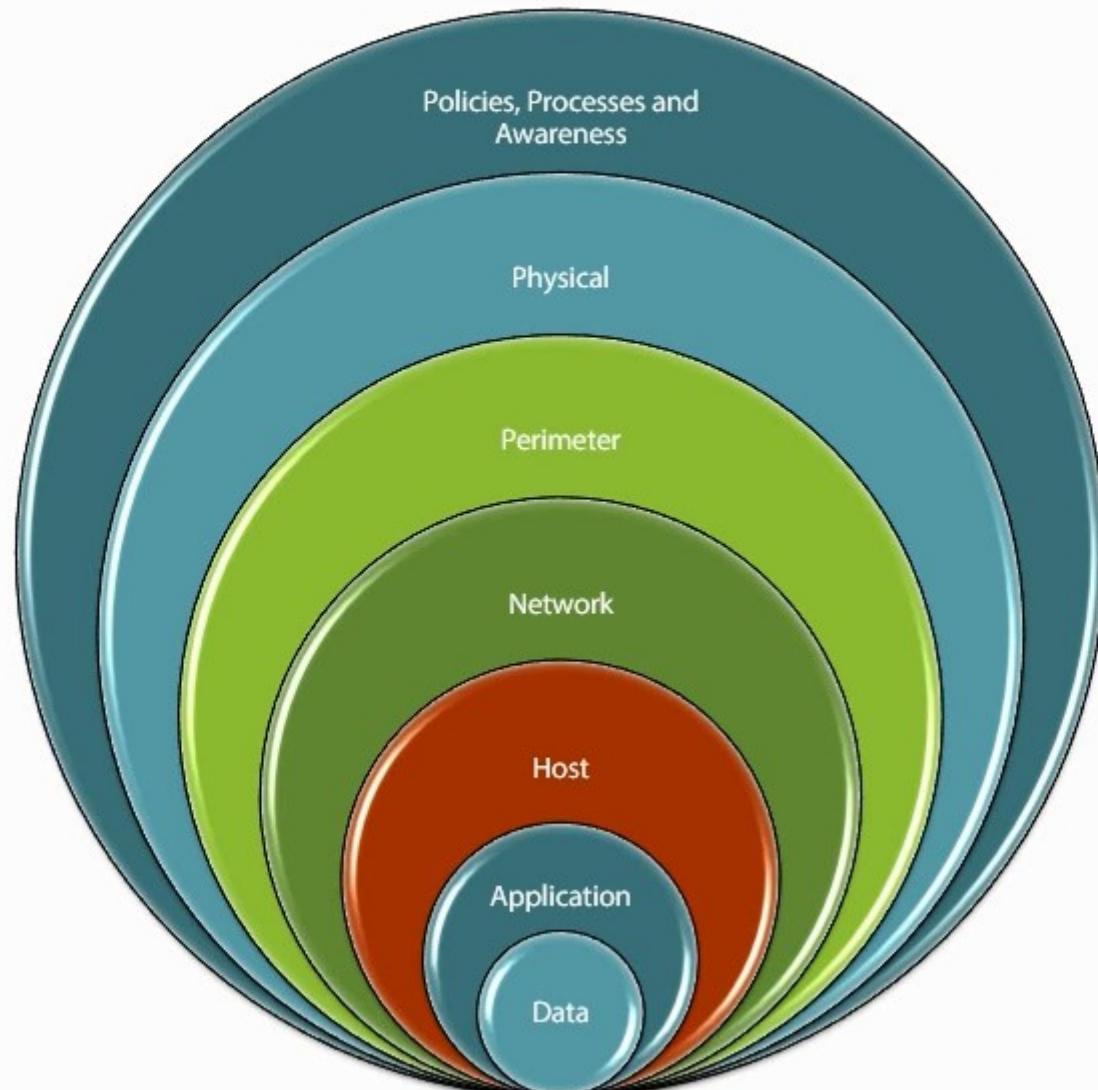
Management skills

Patience

A lot of “Sherlock  
Holmes”

# Multi-layered Defense

# "You've Leveled Up"



# Incident Management

# Think Outside the Box



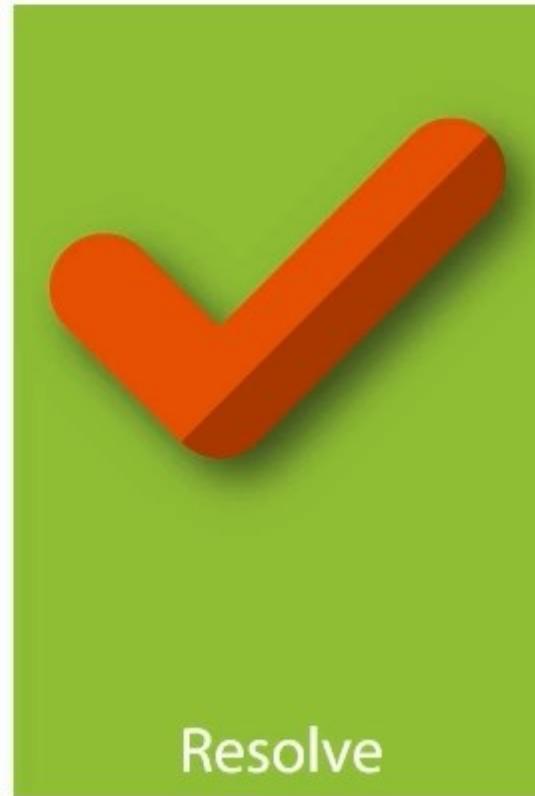
Identify



Analyze



Prioritize



Resolve

# The “Why” of Incident Management

Better service  
quality

Pro-active

Reduces impact

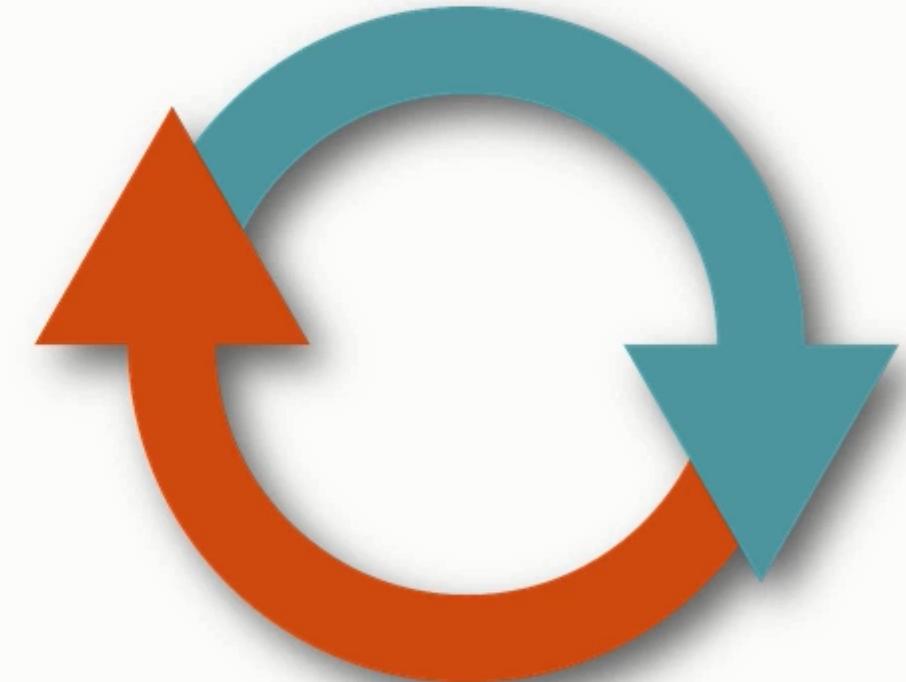
Meets availability

More efficient &  
productive

Customer/user  
satisfaction

# IM Process

- 1 • Prepare for Event Handling and Reaction
- 2 • Detection & Examination
- 3 • Sorting & Ranking
- 4 • Notification
- 5 • Containment
- 6 • Forensic Examination
- 7 • Purge & Recovery
- 8 • Post-incident Actions



# Security Policies

# Security Policies Examples

**Passwords**

**Acceptable-use**

**User account**

**Email security**

**Remote-access**

**Firewall**

**Information  
protection**

**Network  
connection**

**Special access**

# Vulnerability Research

# Knowledge IS Power!

- How often are you checking?
- Where do you check?
- Start thinking like a Hacker
- Collect information about trends in security, attacks, and threats
- Find out how to recover



# Places to Look

- ❑ O/S Vendors
- ❑ Application vendors
- ❑ Hardware vendors
- ❑ Manufacture vendors
- ❑ Component vendors
- ❑ Security related sites/blogs
- ❑ [www.hackerstorm.co.uk](http://www.hackerstorm.co.uk)
- ❑ [www.eccouncil.org](http://www.eccouncil.org)
- ❑ [www.securitymagazine.com](http://www.securitymagazine.com)
- ❑ [www.securityfocus.com](http://www.securityfocus.com)
- ❑ [blogs.windowssecurity.com](http://blogs.windowssecurity.com)
- ❑ [www.hackersjournals.com](http://www.hackersjournals.com)
- ❑ [www.zdnet.com/topic/security](http://www.zdnet.com/topic/security)



<https://www.youtube.com/watch?v=L78r7YD-kNw>

## **Exercise 1 : Analysis of the Cyber Attack on the Ukrainian Power Grid**

**Read the case and answer the following Questions**