Certified Ethical Hacking With Penetration Testing CEHWPT

Gamo@HP:~$Whoami

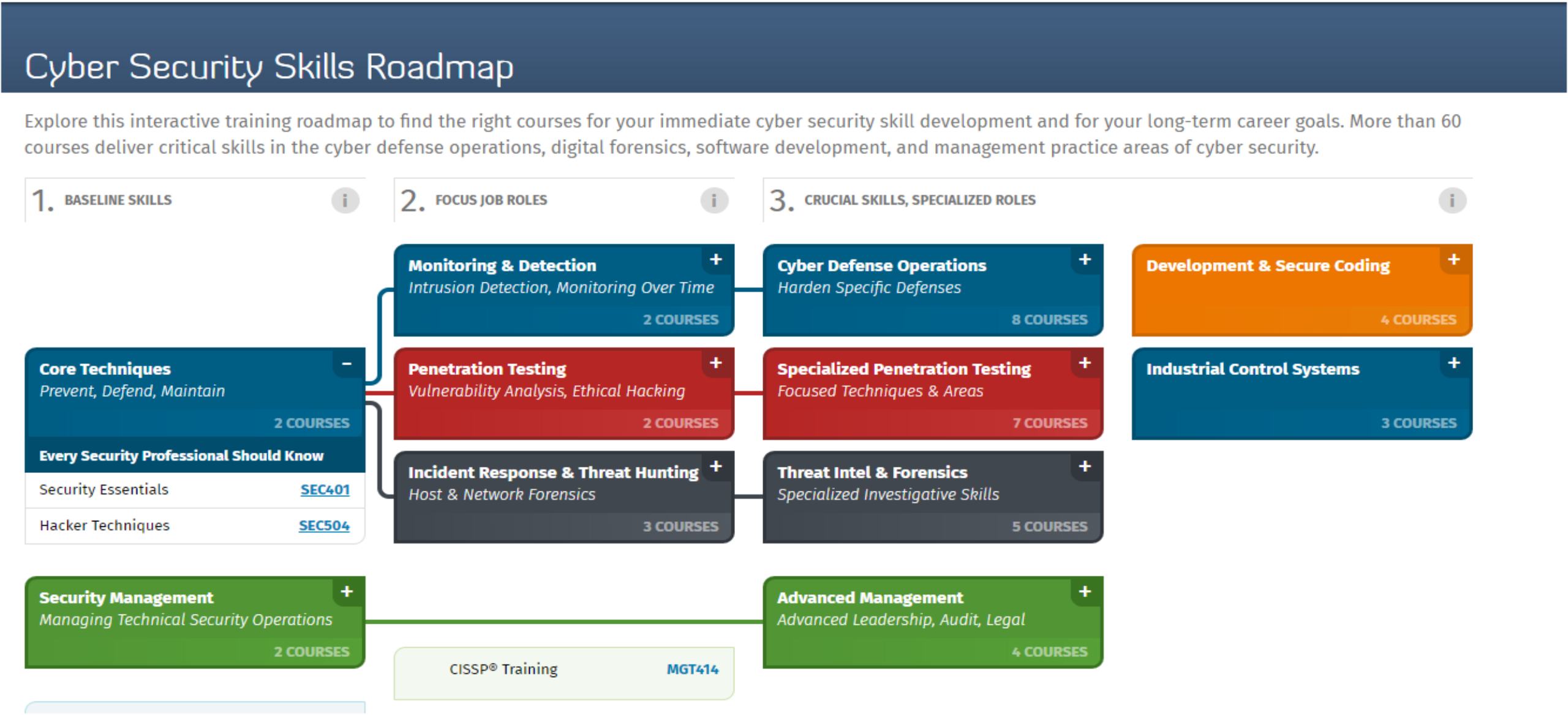
SPEAKERS INFO

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.

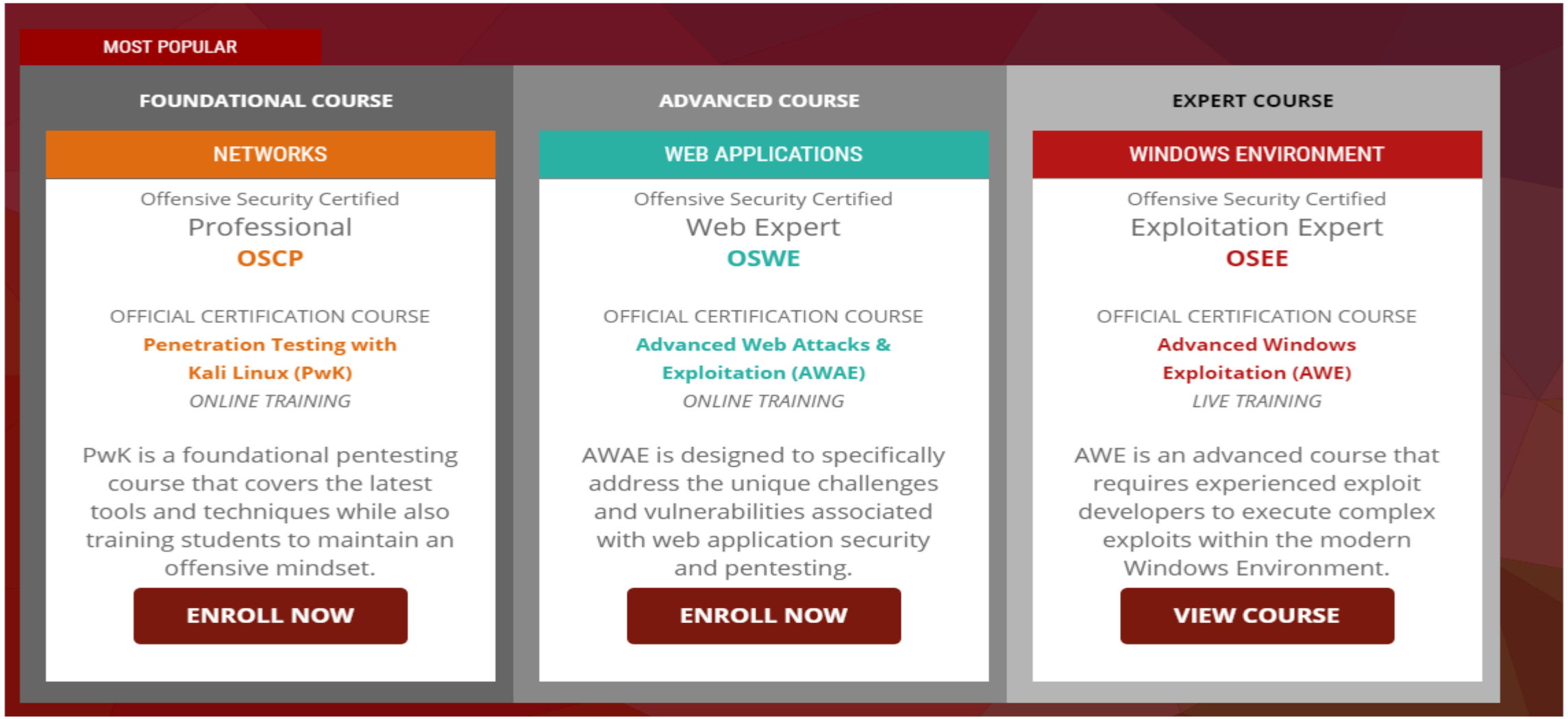
https://www.facebook.com/carthagearena/videos/1701847216530321/

SANS Cyber Security Roadmap



Eccouncil Cyber Security Roadmap

Offensive of Security Cyber Security Roadmap



Mile2 Cyber Security Roadmap

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

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


POLICE


CREDIT CARD
1234 5678 90

How Protected Do You Feel?

https://cybermap.kaspersky.com

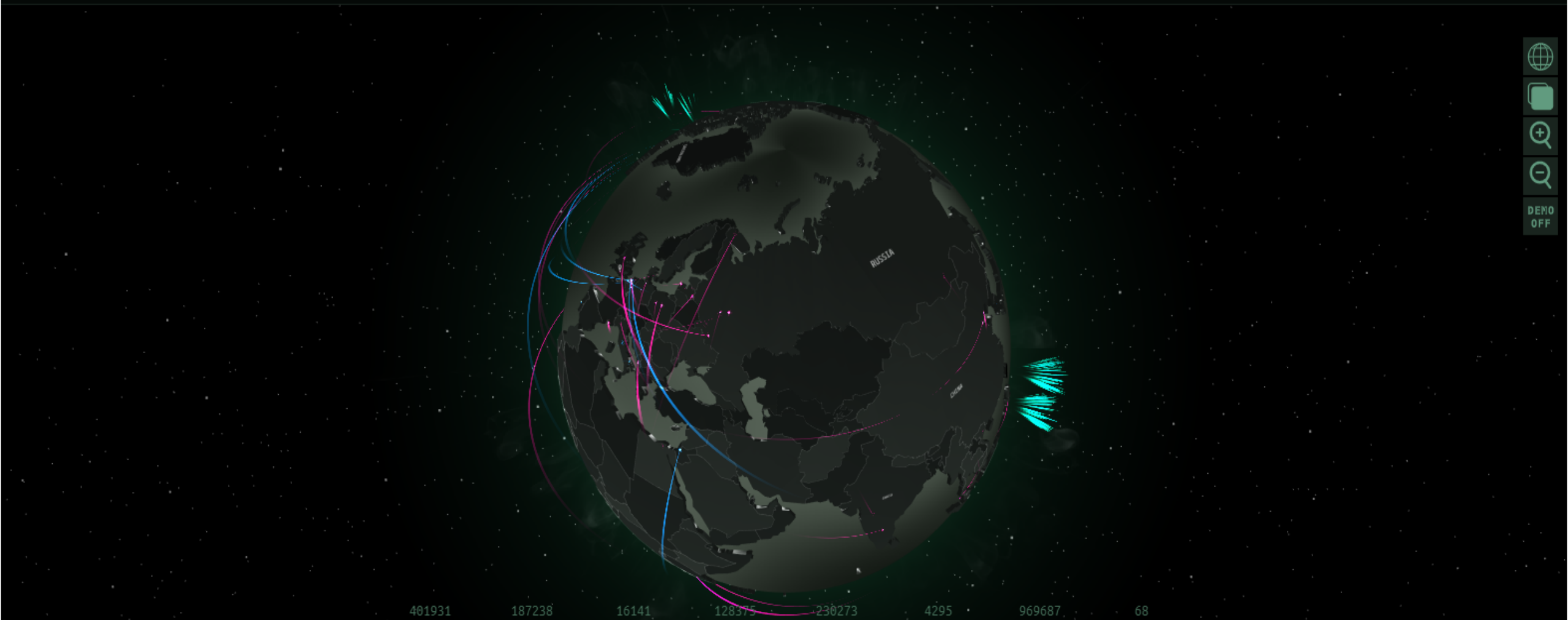
CYBERTHREAT REAL-TIME MAP

EN

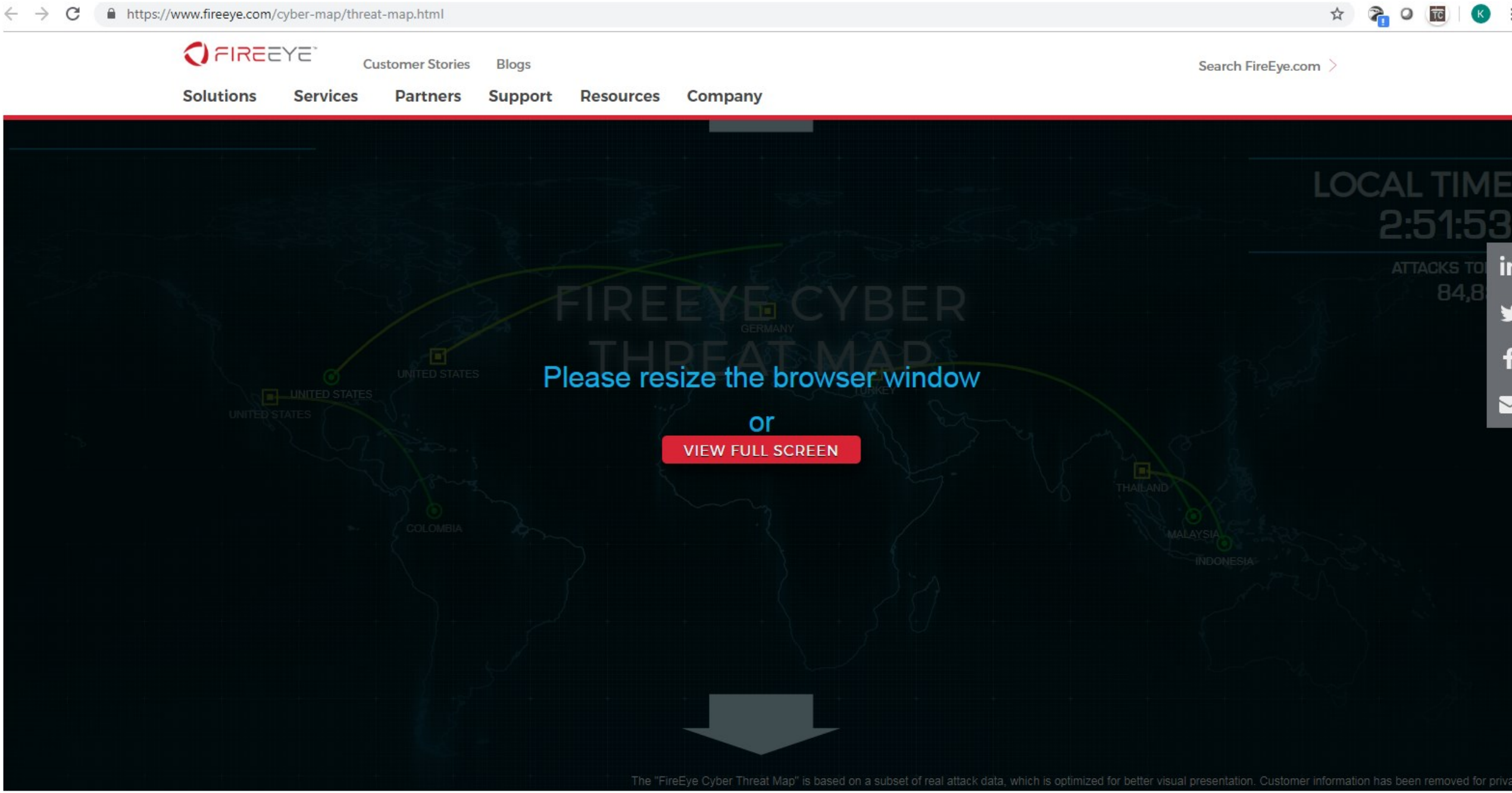
Download Trial

MAP STATISTICS DATA SOURCES BUZZ WIDGET

Share



DEMO OFF


https://www.fireeye.com/cyber-map/threat-map.html
FIREEYE
Customer Stories
Blogs
Search FireEye.com
Solutions
Services
Partners
Support
Resources
Company
LOCAL TIME
2:51:53
ATTACKS TO
84,8
FIREEYE CYBER
THREAT MAP
Please resize the browser window
or
VIEW FULL SCREEN
GERMANY
UNITED STATES
UNITED STATES
UNITED STATES
TURKEY
THAILAND
MALAYSIA
INDONESIA
COLOMBIA
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 priva

“ 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

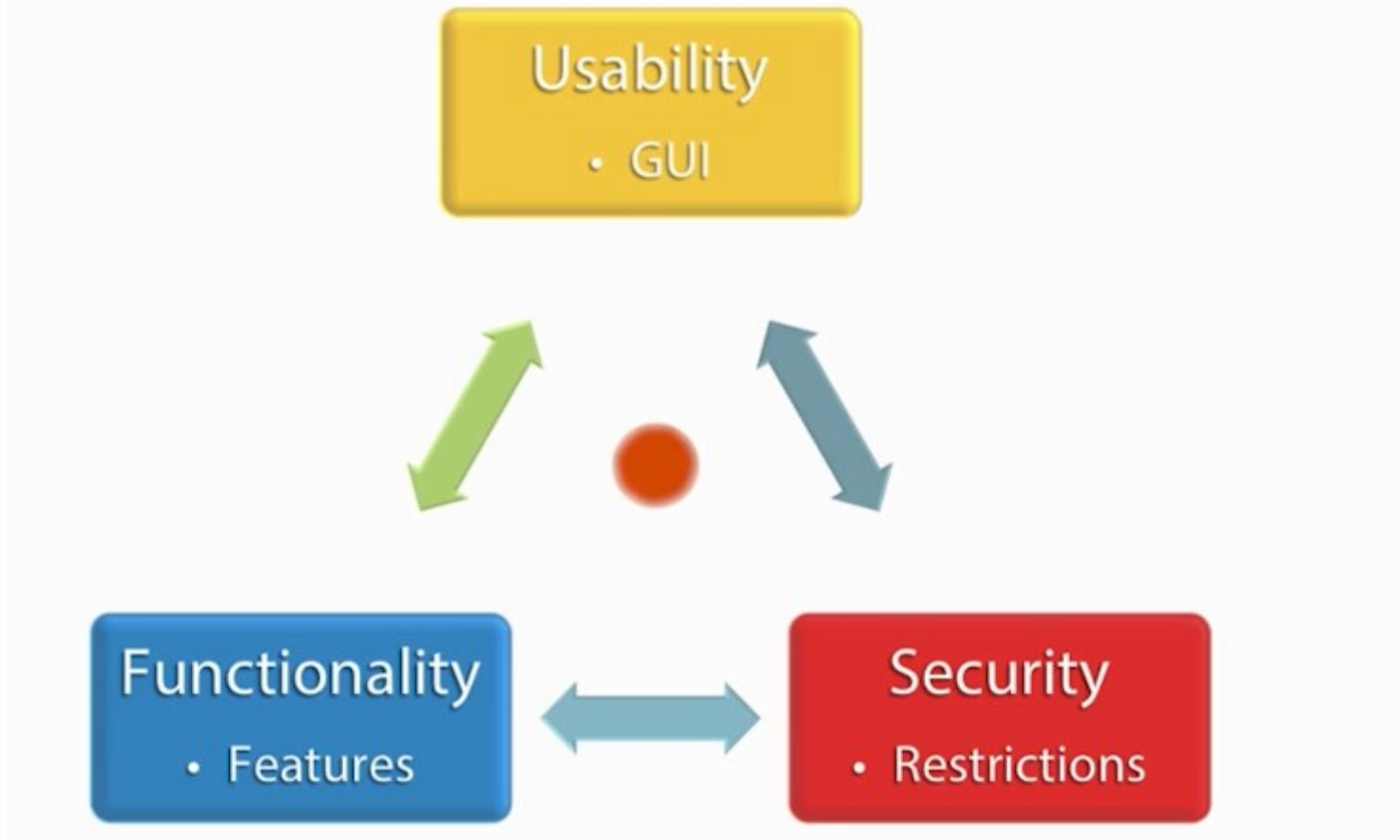
Intellectual property

Fundamentals of Information Security

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?”

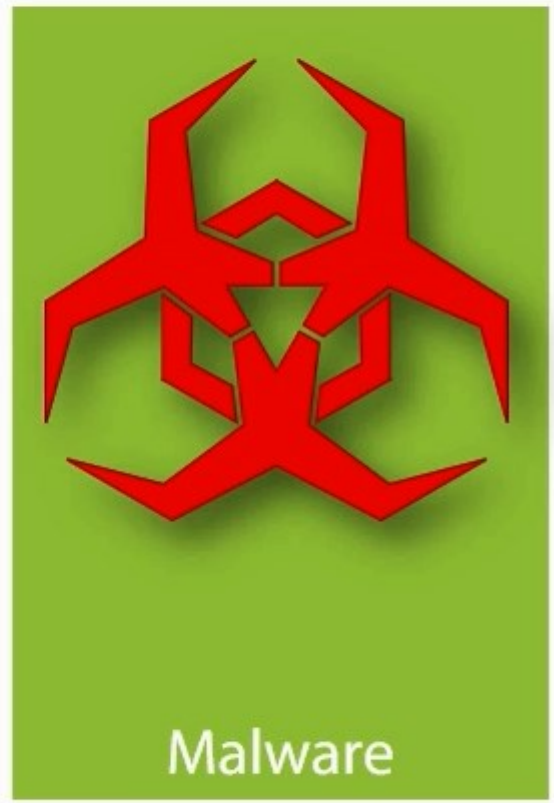
Security Threats

Hosts


Footprinting


Physical Security


windows8user
Locked
Password
Windows 8
Passwords


Malware

Hosts

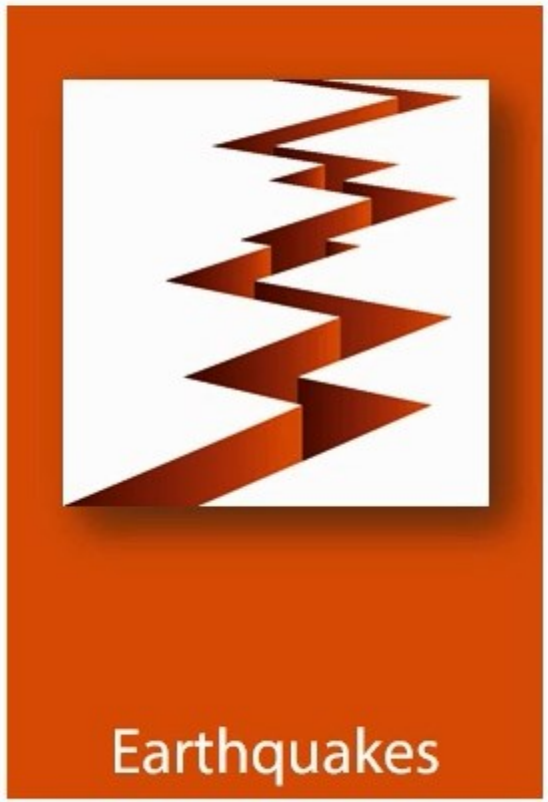
Denial of Service

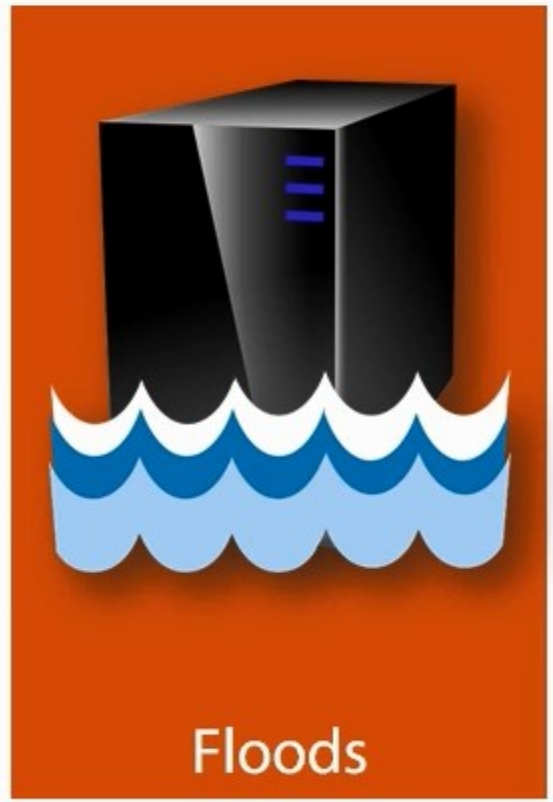
Unauthorized Access

Privilege Escalation

Back Doors

Natural





Physical

Theft

Impact

Power

End of Life

Applications

Configuration

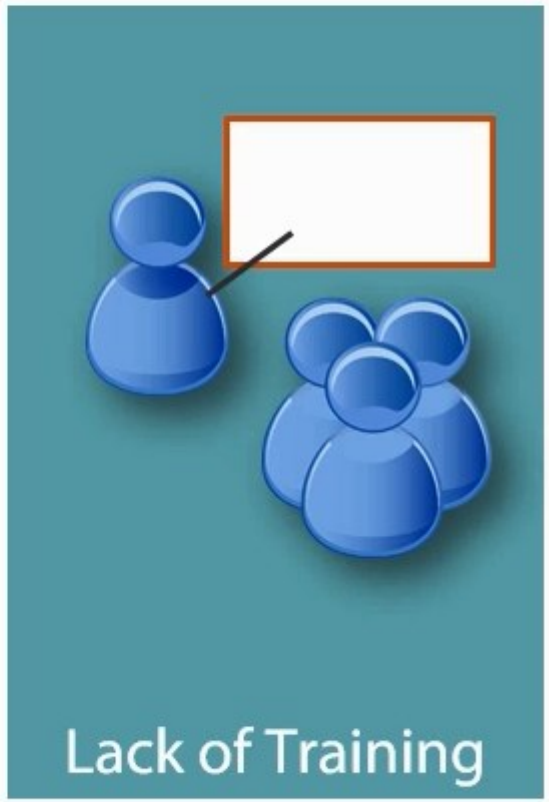
Buffer Overflow

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

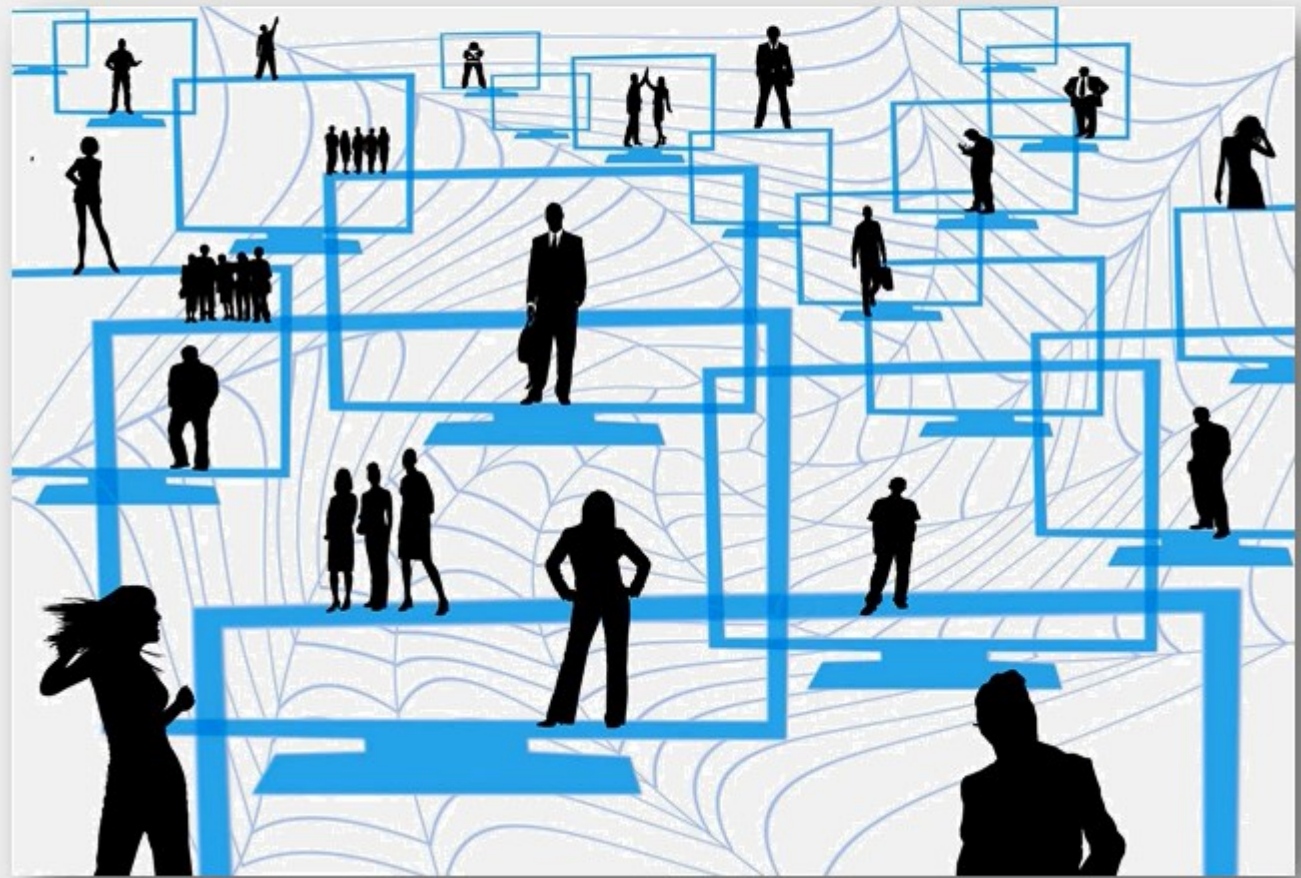
In the beginning…

- 1970's
- 1980's

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

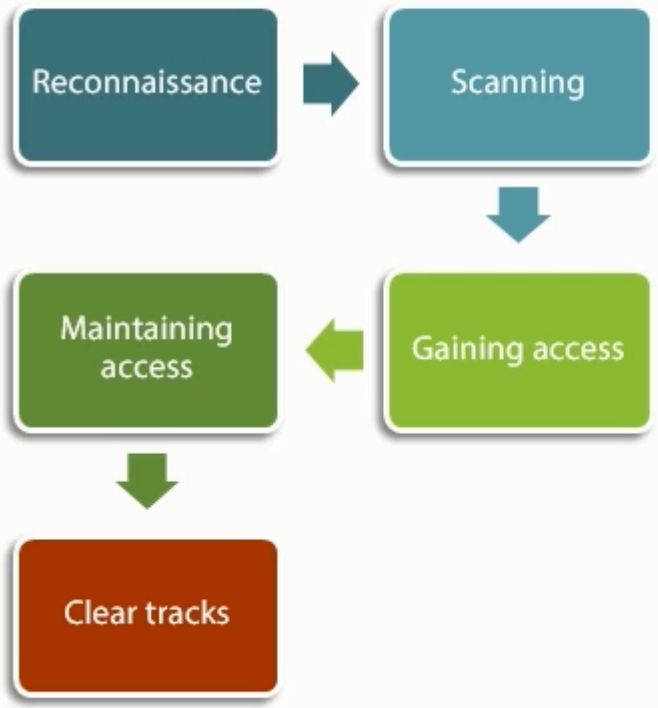
Government Agencies
Multinational Corps
“Wrong”

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

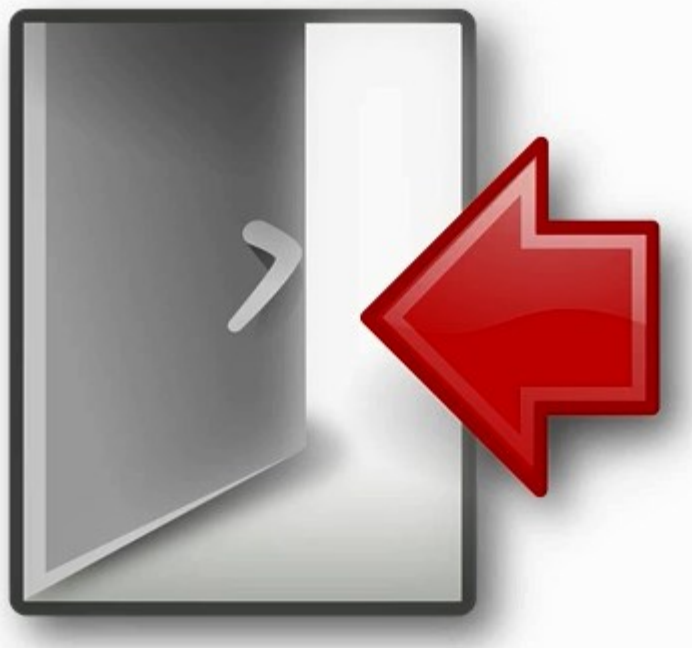
Gather Info

- 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

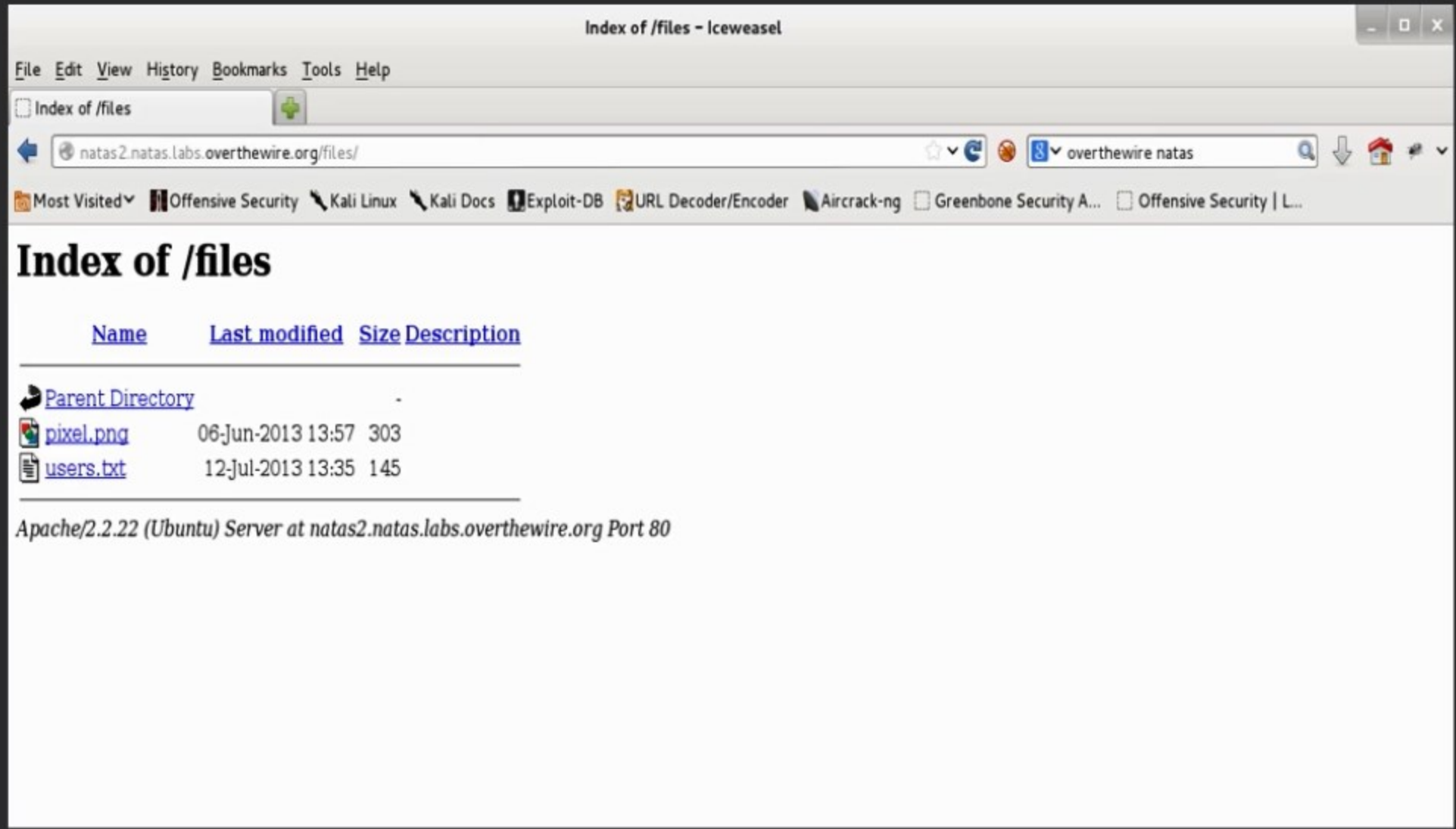
Results

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

Other App Attacks

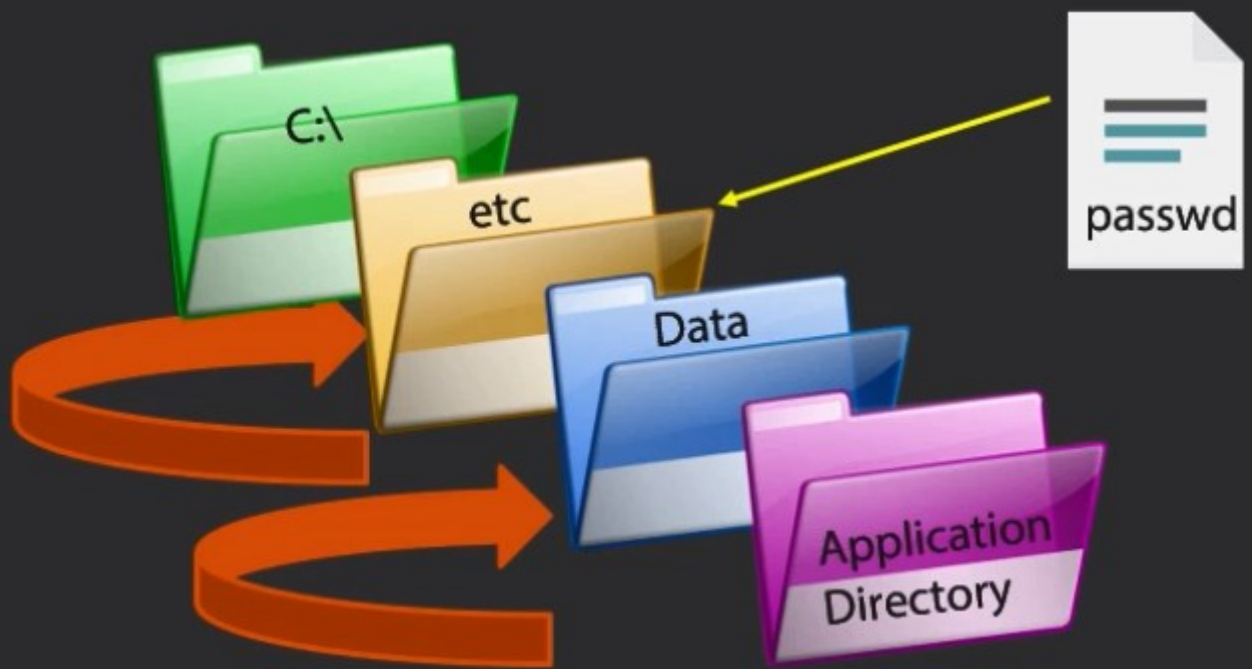
- Session hijacking
- Man in the Middle
- Directory traversal

Visual of Directory Traversal



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	Local Network	Social Engineering
Dial-Up Network	Stolen Equipment	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?

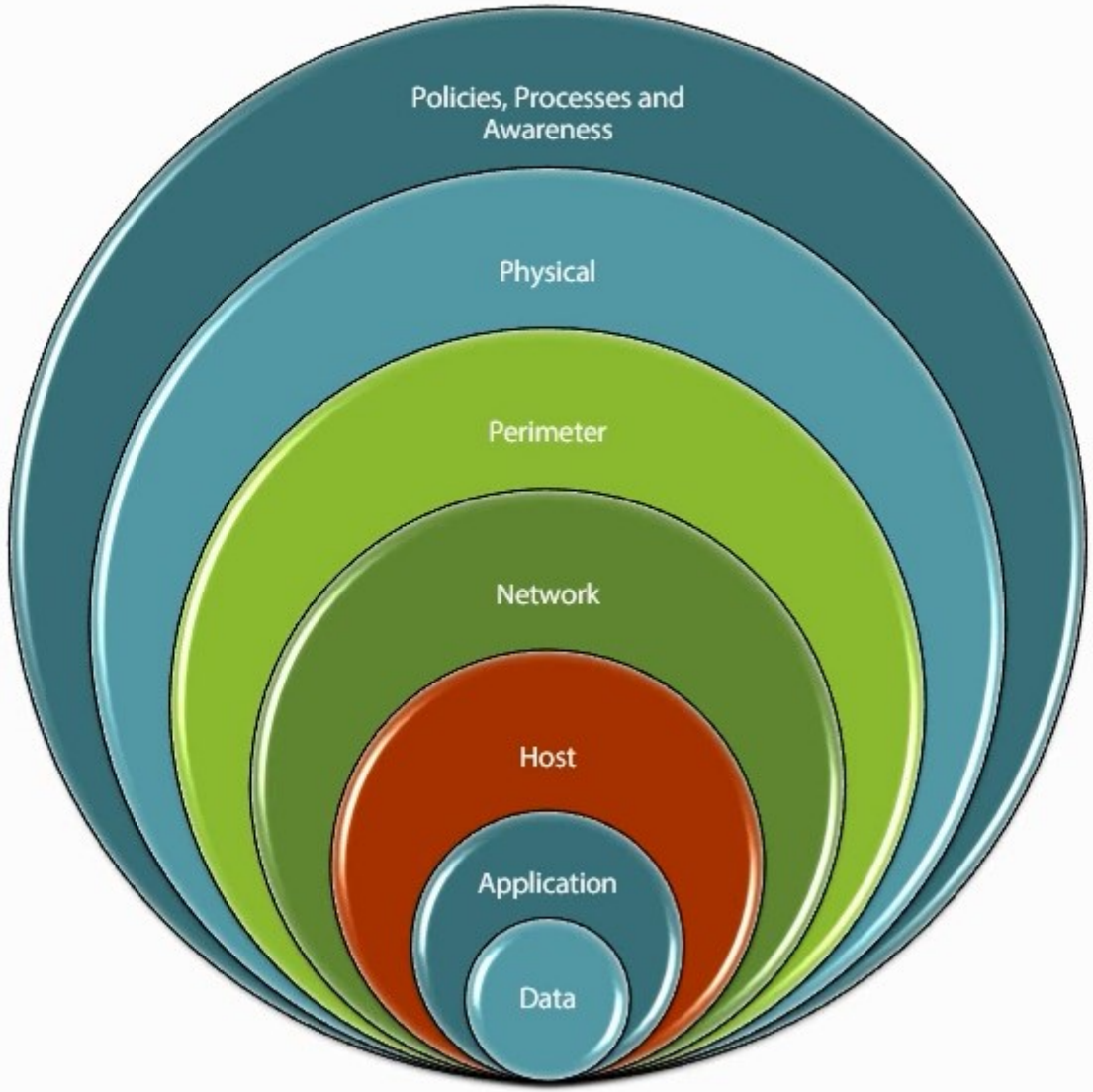
What Skills You Must Have

“I’ve Got Hacking Skills”

“I’ve Got Hacking Skills”

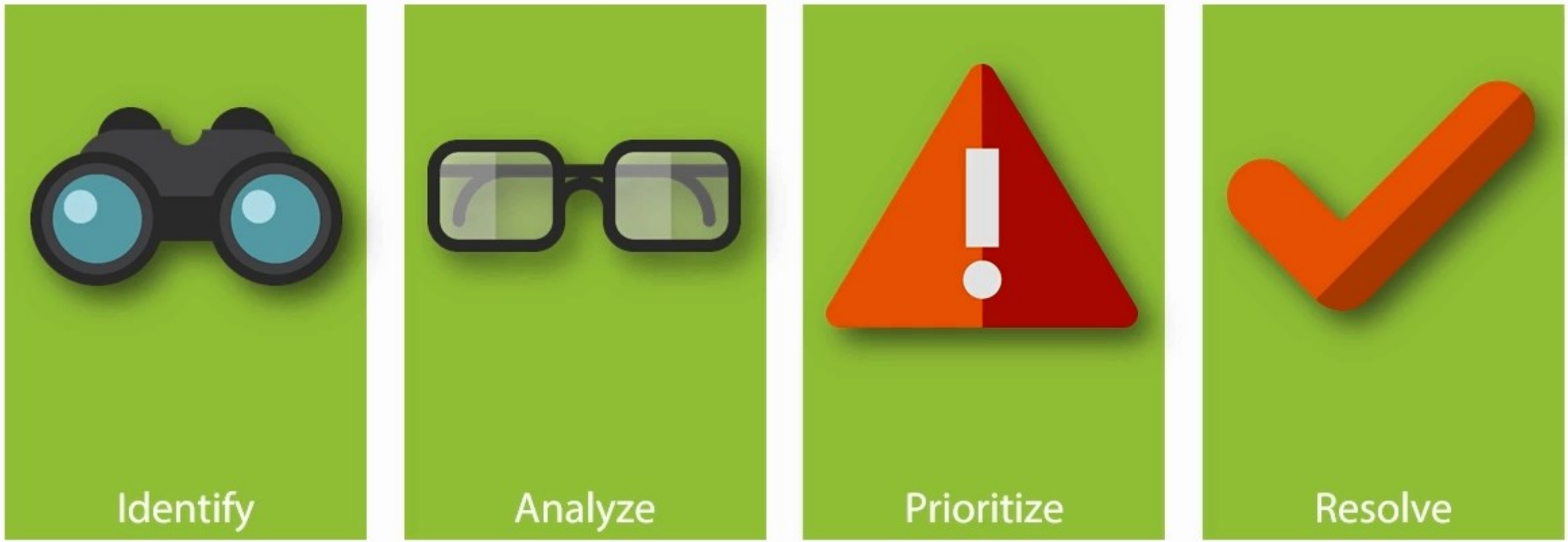
Multi-layered Defense

“You’ve Leveled Up”



Incident Management

Think Outside the Box



The "Why" of Incident Management

Better service quality

Pro-active

Reduces impact

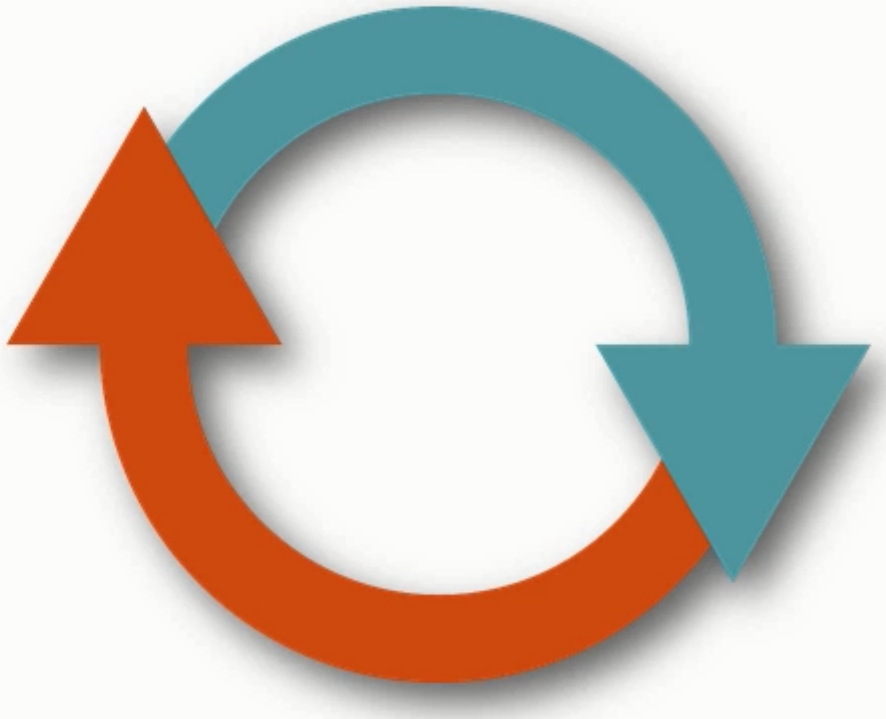
Meets availability

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 Polices Examples

Acceptable-use

Passwords

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
- www.eccouncil.org
- www.securitymagazine.com
- www.securityfocus.com
- blogs.windowssecurity.com
- www.hackersjournals.com
- 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