



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Assessing Vulnerabilities



*Advanced Cybersecurity
(ACCB6000)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



Previous sessions...

- *Understanding Information Security, Risks involved, assessing, managing and monitoring Risks, Cyber risk resilience*
- *Purpose and role of Hackers, Penetration Testing, Various Laws and Standards*
- *Understanding Footprinting and Reconnaissance Concepts, Methodology.*
- *Using various Tools, Taking Countermeasures*

So far, we discussed about Information security, the threats and attack vectors. In continuation to that, I hope you all have understood the hacking concepts and the reasons to stay ethical. Add more insight, we also discussed various security laws and standards. To conclude, we covered various “Risk” concepts like risk factors, cyber risk resilience in the process of enhancing security.

In continuation, we discussed Footprinting concepts focusing on different methodologies like Search Engines, Google Hacking Techniques etc. giving a walkthrough on Website Footprinting, Email Footprinting, Competitive Intelligence, Network Footprinting etc.

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*



Previous sessions...

Scanning and Enumeration

- *Network Scanning, Tools and Techniques*
- *Banner Grabbing*
- *Scanning – PenTesting*

Enumeration

- *Concepts, Techniques*
- *Countermeasures*

Lab/ Tutorials

- *Activity 1: Download and Setup your Lab.*
- *Coursework Description.*
- *Activity 2 Information Gathering*

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

Continuing the earlier lectures, we discussed on Network Scanning, different tools and methodologies used like Banner Grabbing and mitigation methods etc. following that enumeration concepts, its different tools and techniques were discussed.

During the tutorials, under isolated lab environment you might have practiced different Footprinting, scanning and enumerating methods using various tools.



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Understanding and Assessing Vulnerabilities

- ***What is Vulnerability? How is it classified?***
- ***Assessing Vulnerabilities.***
- ***Managing Vulnerabilities***

Lab/ Tutorials

- ***Activity 3 – Vulnerability Assessment.***

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

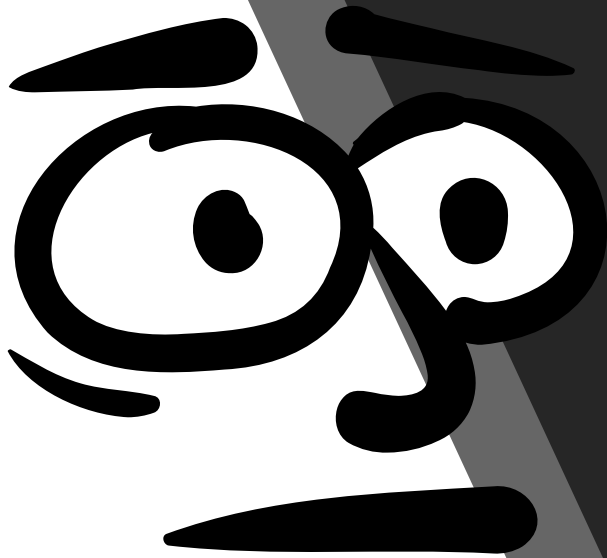
www.uwtsd.ac.uk

During this week, with applied knowledge and understanding on Footprinting, Network Scanning, and Enumeration, we shall move forward focusing on assessing vulnerabilities within a network (either it is our target to attack or defend), different tools used to assess and techniques

During the tutorials, under isolated lab environment you will be using different tools to assess, manage and report vulnerabilities.



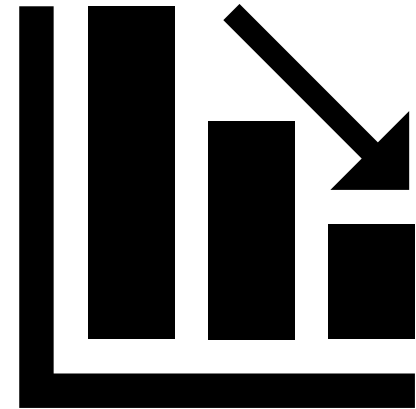
Vulnerability



- So far, we discussed different tools and techniques to look for information (**Reconnaissance & Footprinting**).
- With the available information we tried to scan the target and identify potential attack vectors & vulnerabilities.
- To identify attack vectors and vulnerabilities, we need to first know what is in the target's network. So, we started identifying hosts, ports and services. (**Network scanning**)
- Using the identified hosts, ports and services, we tried to connect to the system to deliberately confirm more details. (**Enumeration**)
- **Now What? By deliberately confirming details, we now have the privilege to find out/ identify the vulnerabilities. i.e: Look for any flaws in the design, configurations etc., in the Operating Systems, Installed Applications etc., that could help us to attack.**

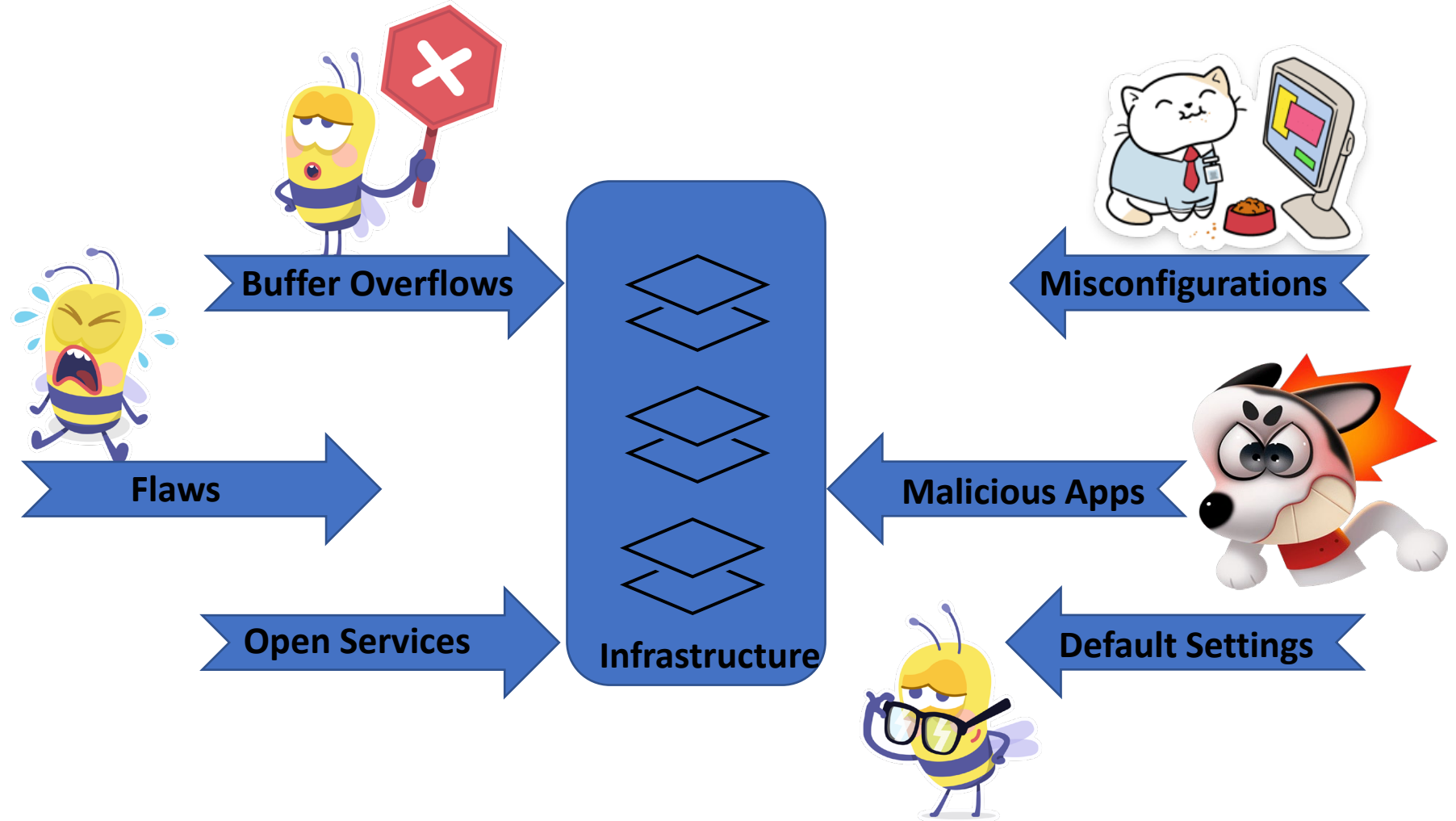
Vulnerability - Classification

- Vulnerabilities could be classified based on their **SEVERITY and EXPLOIT Range.**
 - ✓ SEVERITY (Low, Medium, High)
 - ✓ EXPLOIT Range (Local, Remote)
- **As a Security Professional, you need to assess vulnerability for**
 - ✓ Identify weaknesses before an attack
 - ✓ Gather Information to prevent an attack
 - ✓ Recover from an attack
 - ✓ Keep updated on recent security trends, threats and attacks



Vulnerability - Classification

- Look for



Vulnerability Assessment

- **Assessing Infrastructure**

- VA is testing the security aspects of the system/ application recognizing and classifying the weaknesses.
 - Identify weaknesses that could be exploited
 - Test the efficiency of the existing security implementations.
- VA can be done using various tools/ scanners. These scanners gather and classify information like
 - Vulnerabilities within a network
 - Port status (Open, Closed Ports and its associated services)
 - Application Status (Its Services, vulnerabilities, configuration errors etc)

- **Types:**

- | | |
|-----------------------|-------------------------------|
| ○ Active Assessment | ○ Host-based Assessment |
| ○ Passive Assessment | ○ Network Assessment |
| ○ External Assessment | ○ Application Assessment |
| ○ Internal Assessment | ○ Wireless Network Assessment |

Vulnerability Assessment– Life Cycle



○ **VA Approaches**

- Product Based Solutions
- Service Based Solutions
- Tree Based Assessment
- Inference Based Assessment

Life Cycle to manage Vulnerability

Vulnerability Assessment

- **Product Based Solutions**

- Internal Operation
- Installed in Internal Network
- Private/ Non-routable Network
- Because, it is behind the firewall, detecting outside attacks is limited

- **Service Based Solutions**

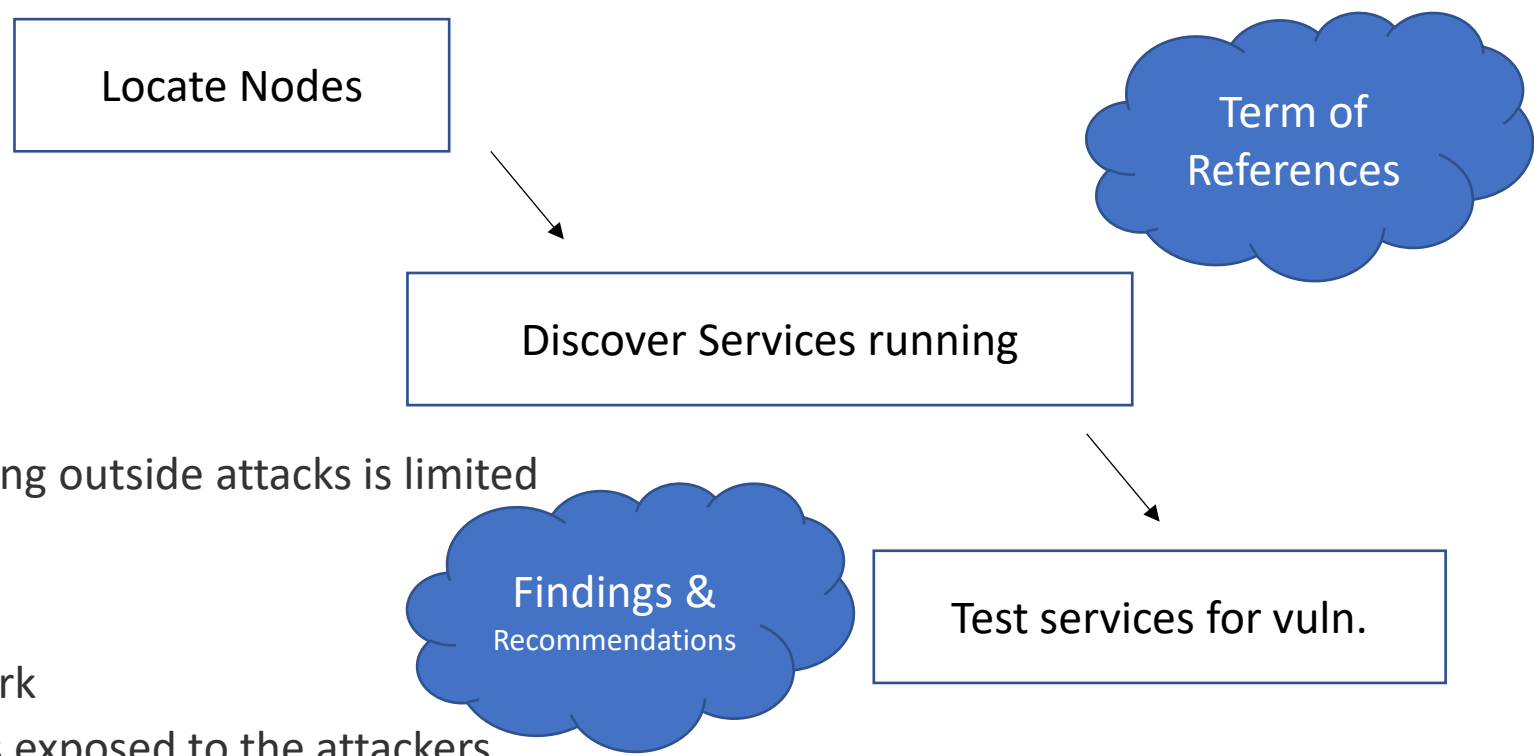
- Third Party Operation
- Inside the network or outside the network
- Because, it is outside the network, this is exposed to the attackers

- **Tree Based Assessment**

- Different strategies are selected for individual component of the Information System

- **Inference Based Assessment**

- An inventory of protocols is identified. Based on the identified services, vulnerabilities are selected on each machine and executed.



Vulnerability Assessment - Tools

- Host Based Vulnerability Assessment Tools
- Application Layer Vulnerability Assessment Tools
- Depth Assessment Tools
- Scope Assessment Tools
- Active/ Passive Tools
- Location/ Data Examined Tools

Vulnerability Assessment - Tools

- **Characteristics of a Good Vulnerability Assessment Solution:**

- Reliable Outcomes
- Inference Based Approach
- Classify vulnerabilities based on severity level
- Supports Multiple Networks
- Gives adequate solutions

- **Selecting Tools :**

- Test a wide range of vulnerabilities.
- Has different attack signatures
- Fits your infrastructure
- Updated scripts
- Report Generation
- Efficient and Accurate scanning results
- Smart Search Capabilities
- Logging Options

Vulnerability - Scoring System

CVSS

- Open Framework for communicating the characteristics and impacts of IT Vulnerabilities.
- CVSS is designed to give accurate measurement, enabling users to see the underlying vulnerability characteristics that were used to generate the scores.

CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. The official CVSS documentation can be found at <https://www.first.org/cvss/>.

NVD CVSS Calculators

[NVD CVSS v2 Calculator](#)

[NVD CVSS v3 Calculator](#)

NVD Vulnerability Severity Ratings

NVD provides qualitative severity ratings of "Low", "Medium", and "High" for CVSS v2.0 base score ranges in addition to the severity ratings for CVSS v3.0 as they are defined in the CVSS v3.0 specification.

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

DRAFT CVSS v2.10 Equations (last revised 3-20-07)

CVSS Base Score Equation

$$\text{BaseScore} = (.6 * \text{Impact} + .4 * \text{Exploitability} - 1.5) * f(\text{Impact})$$

$$\text{Impact} = 10.41 * (1 - (1 - \text{ConfImpact}) * (1 - \text{IntegImpact}) * (1 - \text{AvailImpact}))$$

$$\text{Exploitability} = 20 * \text{AccessComplexity} * \text{Authentication} * \text{AccessVector}$$

$$f(\text{Impact}) = 0 \text{ if } \text{Impact}=0; 1.176 \text{ otherwise}$$

By selecting these links, you will be leaving NIST workspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Vulnerability Assessment - Reports

- *The purpose of Vulnerability Assessment report is to give a clear picture on the detected risks once a scan is completed.*
- *Based on the detected risks (reports), adequate countermeasures to prevent the attacks/ mitigate the risks need to be proposed.*

Report Information on Scan

Information on Target

Results

Vulnerability Assessment - Overview

- Vulnerability research is a process of finding out vulnerabilities and configuration mistakes that could lead to an attack.
- Vulnerabilities need to be classified based on severity levels and exploit range
- Vulnerability Assessment is to test the ability of the system.
- Tools are used to test the host/ application for any vulnerability.
- The Assessment Report helps in listing out the risks.

Activities & Reminders

- **Demonstrate a simple Network Scan on your simulated environment, pick up a vulnerability and try to enumerate the vulnerability.**
 - Do the scan in advance – Demo on what your scan picked up and your approach in detailing the vulnerabilities and enumerating them.



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Any Questions?

*Advanced Cybersecurity
(ACCB6000)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

References

- EC-Council CEH
- Cisco Networking Academy
- Certified Ethical Hacker (CEH) Version 10 Cert Guide, 3rd edition
- Wikipedia
- Other website sources given in this presentation
- * The intension of usage is for Educational Purpose Only

Advanced Cybersecurity
(ACCB6000)

Applied Computing - WISA

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

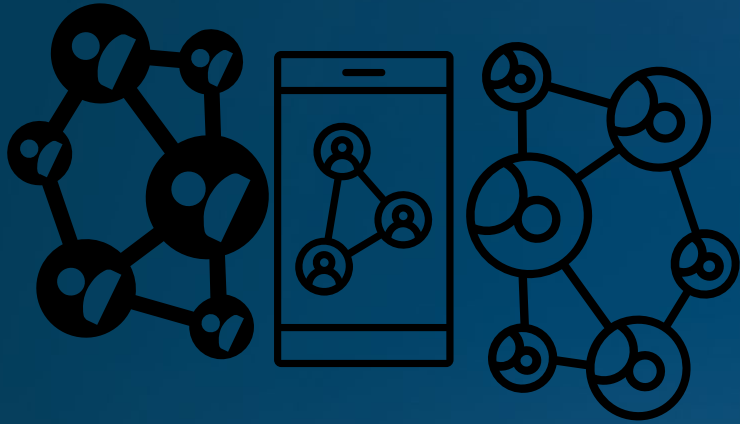
www.uwtsd.ac.uk



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Social Engineering



*Advanced Cybersecurity
(ACCB6000)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



Previous sessions...

- *Understanding Information Security, Risks involved, assessing, managing and monitoring Risks, Cyber risk resilience*
- *Purpose and role of Hackers, Penetration Testing, Various Laws and Standards*
- *Understanding Footprinting and Reconnaissance Concepts, Methodology.*
- *Using various Tools, Taking Countermeasures*

So far, we discussed about Information security, the threats and attack vectors. In continuation to that, I hope you all have understood the hacking concepts and the reasons to stay ethical. Add more insight, we also discussed various security laws and standards. To conclude, we covered various “Risk” concepts like risk factors, cyber risk resilience in the process of enhancing security.

In continuation, we discussed Footprinting concepts focusing on different methodologies like Search Engines, Google Hacking Techniques etc. giving a walkthrough on Website Footprinting, Email Footprinting, Competitive Intelligence, Network Footprinting etc.

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

Previous sessions...

Scanning and Enumeration

- *Network Scanning, Tools and Techniques*
- *Banner Grabbing*
- *Scanning – PenTesting*

Enumeration

- *Concepts, Techniques*
- *Countermeasures*

Understanding and Assessing Vulnerabilities

- *What is Vulnerability? How is it classified?*
- *Assessing Vulnerabilities.*
- *Managing Vulnerabilities*

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk

Continuing the earlier lecturers, we discussed on Network Scanning, different tools and methodologies used like Banner Grabbing and mitigation methods etc. following that enumeration concepts, its different tools and techniques were discussed. we continued focusing on assessing vulnerabilities within a network (either it is our target to attack or defend), different tools used to assess and techniques

During the tutorials, under isolated lab environment you might have practiced different Footprinting, scanning, enumerating methods using various tools and assessed the vulnerabilities.

Lab/ Tutorials

- *Activity 1: Download and Setup your Lab.*
- *Coursework Description.*
- *Activity 2 Information Gathering*
- *Activity 3 Vulnerability Assessment*



Social Engineering...

- ***Understand Social Engineering Concepts, Techniques***
- ***Understanding Threats, Impersonation***
- ***Countermeasures***

Lab/ Tutorials

- ***Activity 4 – Methods to Exploit Vulnerabilities***

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

During this week, with applied knowledge and understanding on Footprinting, Network Scanning, Enumerating the target, and assessing vulnerabilities, we shall move forward focusing on the social engineering concepts and techniques. Understand what is Insider Threats, Impersonation on Social Networking Sites, Identity Theft etc. We shall also look on what countermeasures are to be taken to overcome these.

During the tutorials, under isolated lab environment you will be using different Social Engineering techniques.

Social Engineering

- Social Engineering is an **art of convincing people to let them reveal information** that they know without understanding its confidential status.
- Focus would be on ***System Admins, Technical Support Executives, Receptionist*** etc.
- The concept of Social Engineering relies on Trust, Ignorance, Human Habits etc
- Even though, the information provided are not considered seriously by the victims, it might lead to huge economic loss, temporary or permanent closure etc.
- Exposed to Social Engineering Attacks due to
 - ✓ No adequate Security Training
 - ✓ Unregulated access to Information
 - ✓ No strong security Policies
- Social Engineering Attacks are
 - ✓ Difficult to detect
 - ✓ No specific method/ tools to prevent SEA
 - ✓ Humans are the most susceptible factor

Social Engineering



The 6 Principles of Persuasion



Reciprocity

When we receive something, we feel obliged to give something back.



Consistency

We feel compelled to be consistent with what we've said/done in the past.



Social Proof

When we're uncertain how to behave or react, we look to others for answers.



Liking

We're more likely to agree to someone's request if we know and like him/her.



Authority

We tend to obey figures of authority (people with titles or expertise).



Scarcity

We perceive something to be more valuable when it's less available.



Science of Persuasion:

https://readinggraphics.com/uploads/2018/02/Influence_6-Principles-of-Persuasion.png

Social Engineering - Phases

- Campus Visits
- Websites
- Dumpster Diving
- Etc

Do a research
on Target

- Disgruntled Employee
- Talkative
- Club Activities
- Etc

Choose the
Victim

- Friendship
- Chit-chat
- Offer Help
- Etc

Develop
relationship

- Gather required
Information (Account
details, Financial
Details, Tools/ Techs
- Etc

Exploit



Social Engineering - Types

Human Based

Interact with the human and gather information

Tailgating, Vishing,
Dumpster Diving, Eavesdropping,
Piggybacking, Shoulder Surfing,
Impersonation, Dumpster Diving
etc

Computer Based

Using computers/ tools to gather information

Spams, Phishing, Chats, Pop-up
Window Attacks etc

Mobile Based

Using Mobile Applications

Smishing, Fake and Malicious
Applications etc.

Social Engineering: HB-SEA

Impersonation

- ✓ Attackers could impersonate physically or via communication channels (like emails, sms, phone calls etc)
- ✓ Attacks trick the target to reveal important information.
- ✓ There is always an urgency in the act, that doesn't allow the victim to think.
- ✓ May be as a Legitimate End user, Premium User, Technical Support Guy etc
- **Vishing** (Voice or VOIP Phishing)
 - ✓ Use Telephone to do the trick.
- **Eavesdropping, Shoulder Surfing, Dumpster Diving.**
- **Reverse Social Engineering, Piggybacking, Tailgating.**



Social Engineering: CB-SEA

- Spam Email
- Pop-up Windows
- Instant Chat Messenger
- Chain Letters
- Hoax Letters



Phishing

Phishing is sending email that falsely resembles legitimate site to acquire user's personal information.

❑ Spear Phishing, Whaling, Pharming, Spimming etc

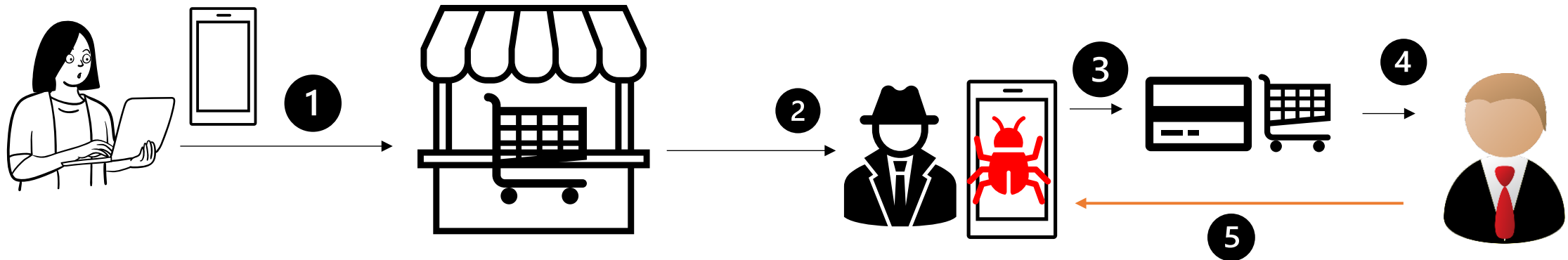


Social Engineering: MB-SEA

- Malicious Apps

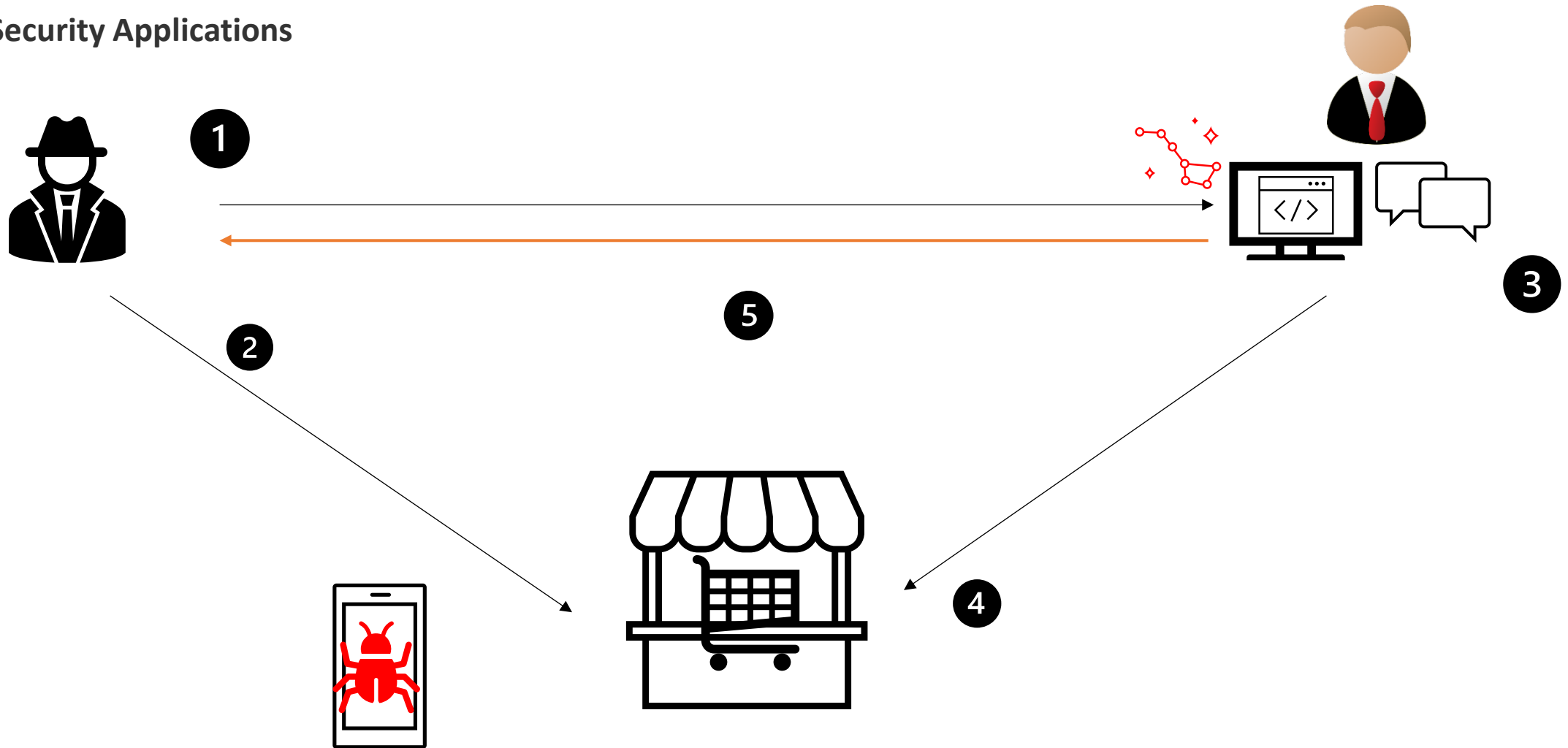


- Repackaging Legitimate Apps



Social Engineering: MB-SEA

○ Fake Security Applications



Social Engineering: Threats

Insider Threat:

- Anyone belonging to the organisation could be a threat.
- Depending on the level of information he/she knows and level of access to assets within the organisation, the impact could vary.

Reasons:

- ✓ Financial Gain
- ✓ Revenge
- ✓ Public Announcement
- ✓ Competition
- ✓ Stealing confidential data

Types:

- ✓ Malicious Insider
- ✓ Negligent Insider
- ✓ Professional Insider
- ✓ Compromised Insider

Types of Insider Threats Most Businesses Worry About



Source: AT&T Business

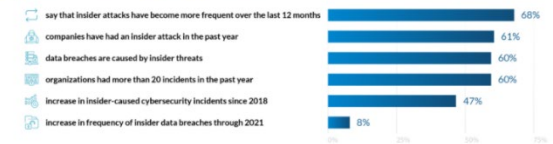
Designed by FinancesOnline



3 Insider Threat Statistics You Should See

FinancesOnline
REVIEWS FOR BUSINESS

1 Insider Threat Frequency of Attacks



2 Top Motivations for Insider Attacks



3 Top Insider Threat Actors

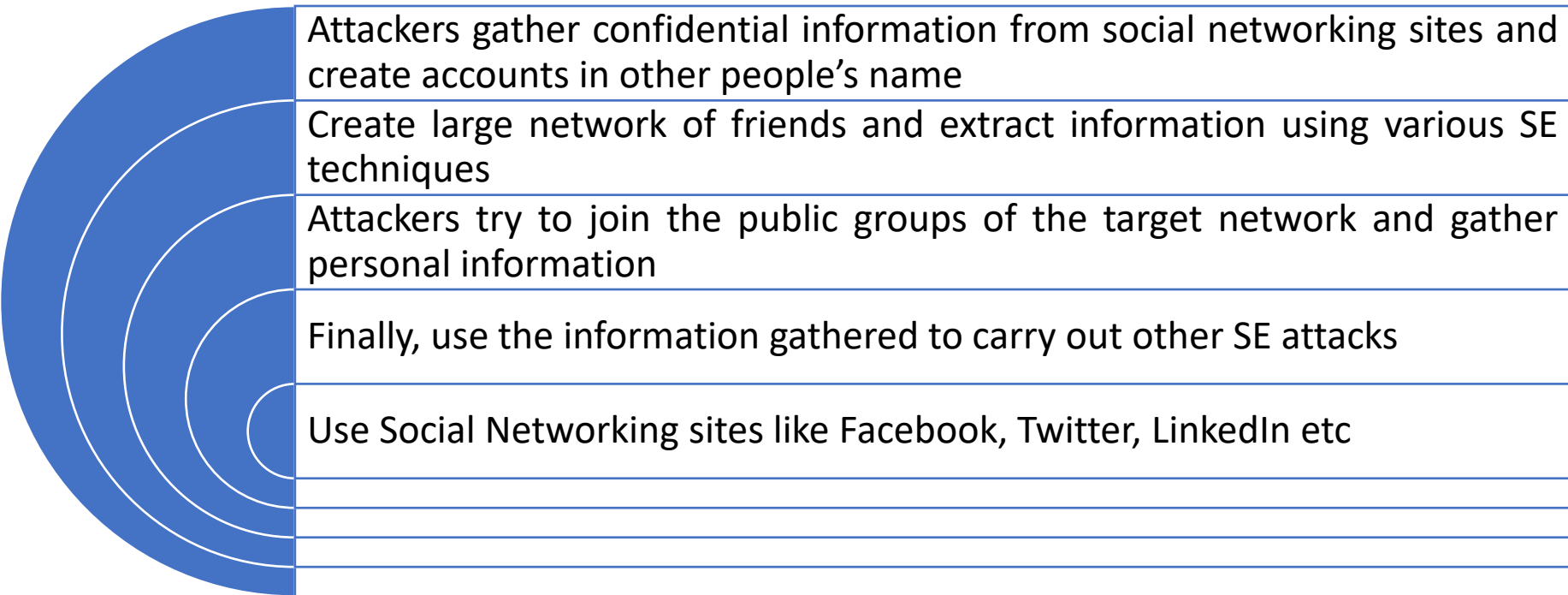


Social Engineering: Threats

Insider Threat: Why it is very effective?

- ✓ Easy to launch
- ✓ Difficult to prevent
- ✓ Success rate is high

Social Engineering: Social Networking Sites



This leads to

- ✓ **Data Theft**
- ✓ **Spam and Phishing**
- ✓ **Involuntary Data Leakage**

- ✓ **Infrastructure Maintenance Cost**
- ✓ **Network Vulnerability**
- ✓ **Malware Propagation**

- ✓ **Targeted Attacks**
- ✓ **Modification of Contents**
- ✓ **Business Reputation**

Social Engineering: Identity Theft

- **A theft that happens when your personally identifiable information such as Name, Credit Card Number, NI number, Passport, Driving License details are taken and used.**
 - ✓ Child Identity Theft
 - ✓ Tax Identity Theft
 - ✓ Insurance Identity Theft
 - ✓ Criminal Identity Theft
 - ✓ Medical Identity Theft
 - ✓ Identity Cloning
 - ✓ Etc
- **Identity Theft can be done using Personal Information. These information could be obtained by**
 - ✓ Social Engineering, Internet Searches, Theft of Wallets, Laptops, Mobile Phones, Phishing, Skimming, Wardiving, Pharming, Pretexting, Dumpster Diving, Shoulder Surfing, Malwares, Insider Theft etc.

Social Engineering: How to overcome?

- **Password Policies**
- **Physical Security Policies**
- **Defense Strategy**
 - ✓ Background Checks on Employees
 - ✓ Training on Security Policies
 - ✓ Appropriate Access Privileges
 - ✓ Incident Response Time
 - ✓ Scrutinize Information
 - ✓ MFA
 - ✓ Proper documented change management
 - ✓ Regular Software updates
 - ✓ Clear Termination Policy

Social Engineering: How to overcome?

○ Insider Threat

- ✓ Appropriate Access Privileges
- ✓ Employee Monitoring System
- ✓ Risk Assessment, Logs, Auditing
- ✓ Legal Policies
- ✓ Archive critical data
- ✓ Employee Training
- ✓ Background Checks
- ✓ Deactivating Terminated Accounts

○ Detect Phishing Emails

- ✓ Look for Malicious attachments
- ✓ Spoofed Websites
- ✓ Grammatical/Spelling mistakes
- ✓ Urgency
- ✓ Ant phishing Tools

From: GREENLAND UK PROPERTY <careers@greenlandsuk.com>
Date: Sat, 23 Oct 2021, 12:44
Subject: Greenland UK Property Appointment Letter
To: [REDACTED]@gmail.com>

Greenland UK Property,
Address: Greenland UK Property, 40 Basinghall St, London, EC2V 5DE
What's-App only: +441223976630
Website: www.greenlanduk.com

Dear Employee: [REDACTED]

We are happy to inform you that you have been selected for the position of (ADMINISTRATION MANAGER) at Greenland UK Property.

You were selected for the position based on your previous work experience and your impressive educational accomplishments. We are thrilled to offer you this position in our Real Estate Firm. We are confident you will thrive professionally and personally while working for our Firm.

You are scheduled to begin work on (13th of December 2021), your will spend the morning of your first day in Orientation classes at our Orientation Head Office building, located at Greenland UK Property, 40 Basinghall St, London, EC2V 5DE. Please arrive at 8:00 am. When you arrive, please check in at the reception desk and you will be given directions on where to go. Following lunch, a Team Member will escort you to your new work area and introduce you to your new co-workers.

You shall be briefed about our dress code. I have contacted the UK Immigration office here in London and have submitted all Documents needed for the processing of your Working Visa and copies of the same Documents have also been faxed to the UK Immigration service in (Asia) India.

It was clearly stated to us that the screening process for getting a UK Working Visa at the moment is very hard for the fact that many would not want to go back when their Visa or Work Permit get expired, as such much Documents will be needed from you as prove that you will return back on due time, and the process will take over 4 weeks for the Working Visa to be ready.

Because of the Express Traveling Approval of your Working Visa and considering the Documents that may be required from you to be presented by the UK Embassy and the nature of interview that you might face, the time of Visa delay, which might not be all that favourable to you, thereby resulting to refusal of the Visa to you.

With the help of our Firm's Lawyer, I was able to make contact with the UK Embassy senior representative in (Asia) INDIA Sir Philip Barton who is the (Permanent Under-Secretary to the Foreign & Commonwealth Office) and have concluded all arrangements with him to assist you for fast approval of your working permit Visa without much delay and long Visa protocol to enable you take your Visa Stamping in India.

You are to contact him via email as soon as possible with the following Documents.

1. Your signed Contract Agreement Letter
2. Mobile number,
3. Copy of your Appointment Letter

Below are his details;

Embassy of United Kingdom in INDIA

Contact Person: Sir Philip Barton

E-mail: philipbarton@vfsglobalnewdelhi.in

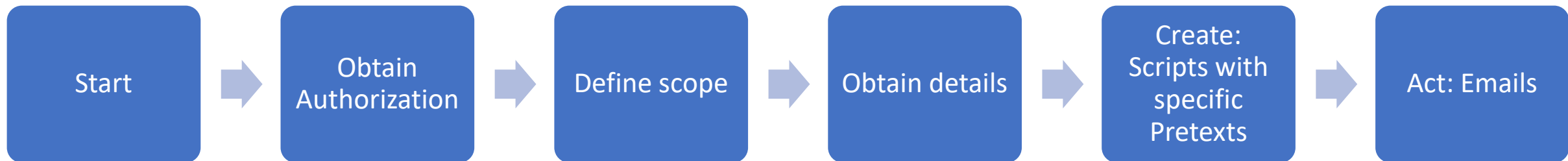
Office hours: 0900-1700 hrs

Social Engineering: How to overcome?



Social Engineering: Pen Test

- SE Pen Test
- **Needs:** Improve the level of Security Awareness within employees
- **Skills:**
 - As a Pen Tester, you must showcase care and professionalism.
 - With Good Interpersonal Skills
 - With Good Communication Skills
 - Creative, Talkative and Friendly





Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Any Questions?

*Advanced Cybersecurity
(ACCB6000)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

References

- EC-Council CEH
- Cisco Networking Academy
- Certified Ethical Hacker (CEH) Version 10 Cert Guide, 3rd edition
- Wikipedia
- Other website sources given in this presentation
- * The intension of usage is for Educational Purpose Only

Advanced Cybersecurity
(ACCB6000)

Applied Computing - WISA

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk