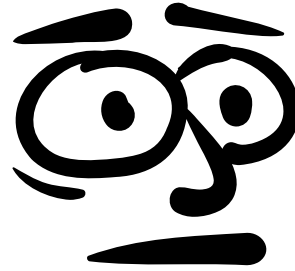




Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

Assessing Vulnerabilities



Advanced Cybersecurity
(ACCB6000)

Applied Computing - WISA



VM Download

\\192.168.135.200\ACCB6000\$

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.



Previous sessions...

Scanning and Enumeration

- *Network Scanning, Tools and Techniques*
- *Banner Grabbing*
- *Scanning – Pen Testing*

Enumeration

- *Concepts, Techniques*
- *Countermeasures*

Lab/ Tutorials

- *Coursework Description.*
- *Activity 1 Getting Ready*
- *Activity 2 Information Gathering*
- *Activity 3 Scanning and Enumeration*

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.*



Understanding and Assessing Vulnerabilities

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

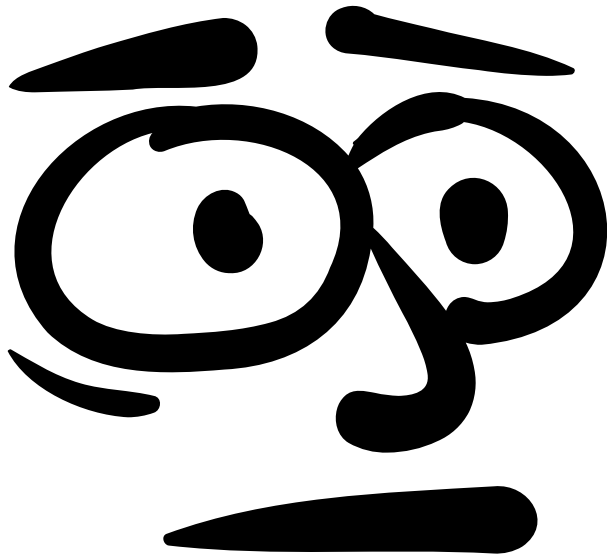
During this week, with applied knowledge and understanding on Footprinting, Network Scanning, and Enumeration, we shall move forward focusing on assessing vulnerabilities within a network (either it is our target to attack or defend), different tools used to assess and techniques

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

Lab/ Tutorials

- ***Activity 4 – Vulnerability Assessment***

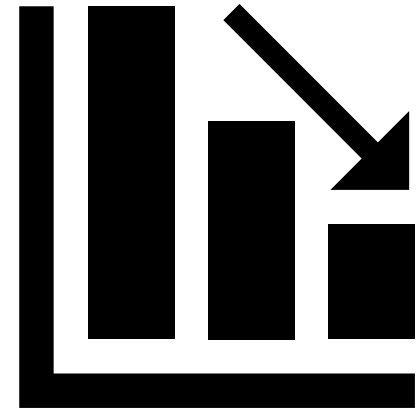
Vulnerability



- 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.**

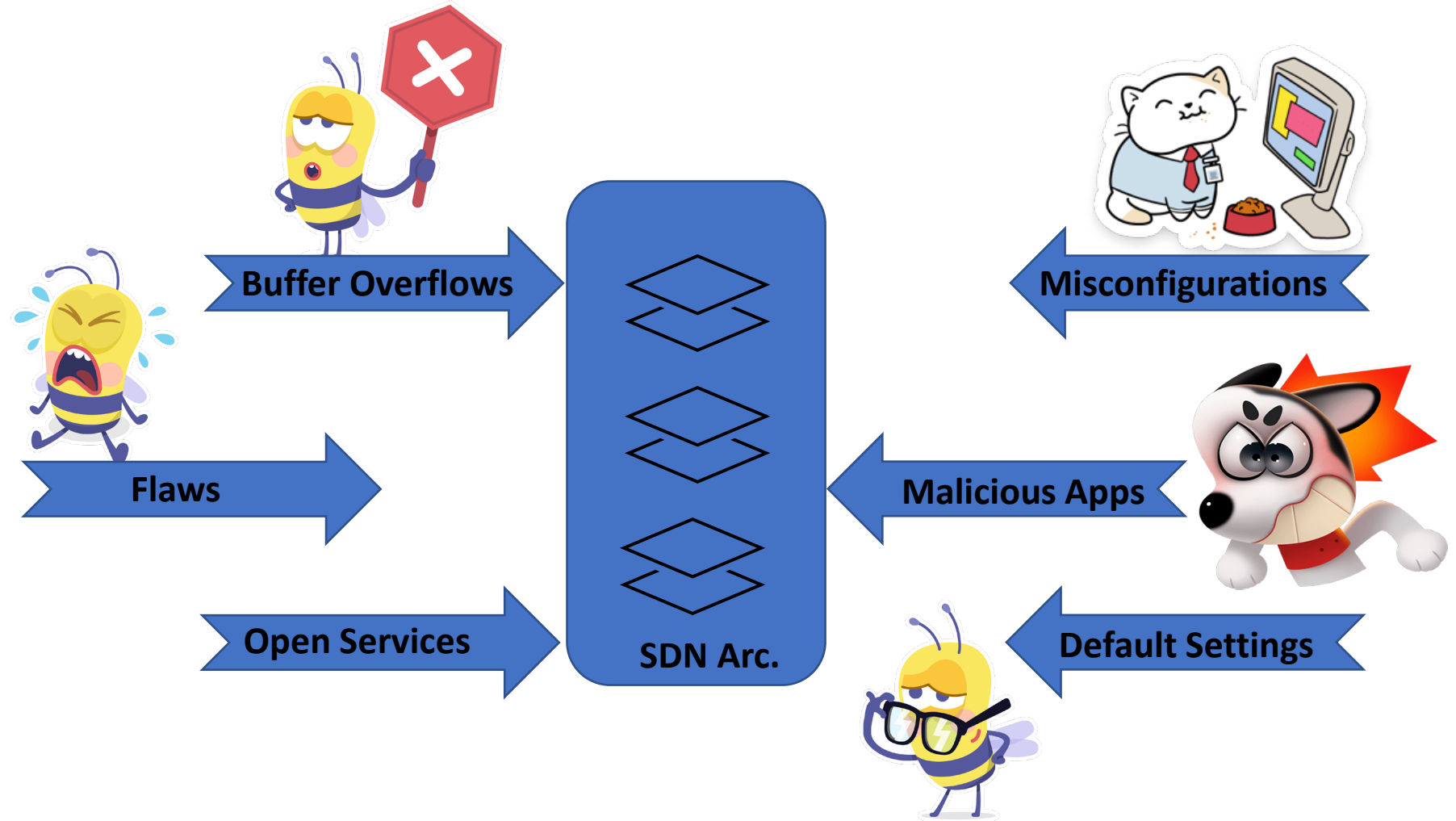
Vulnerability - Classification

- 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
 - Passive Assessment
 - External Assessment
 - Internal Assessment
 - Host-based Assessment
 - Network Assessment
 - Application 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**

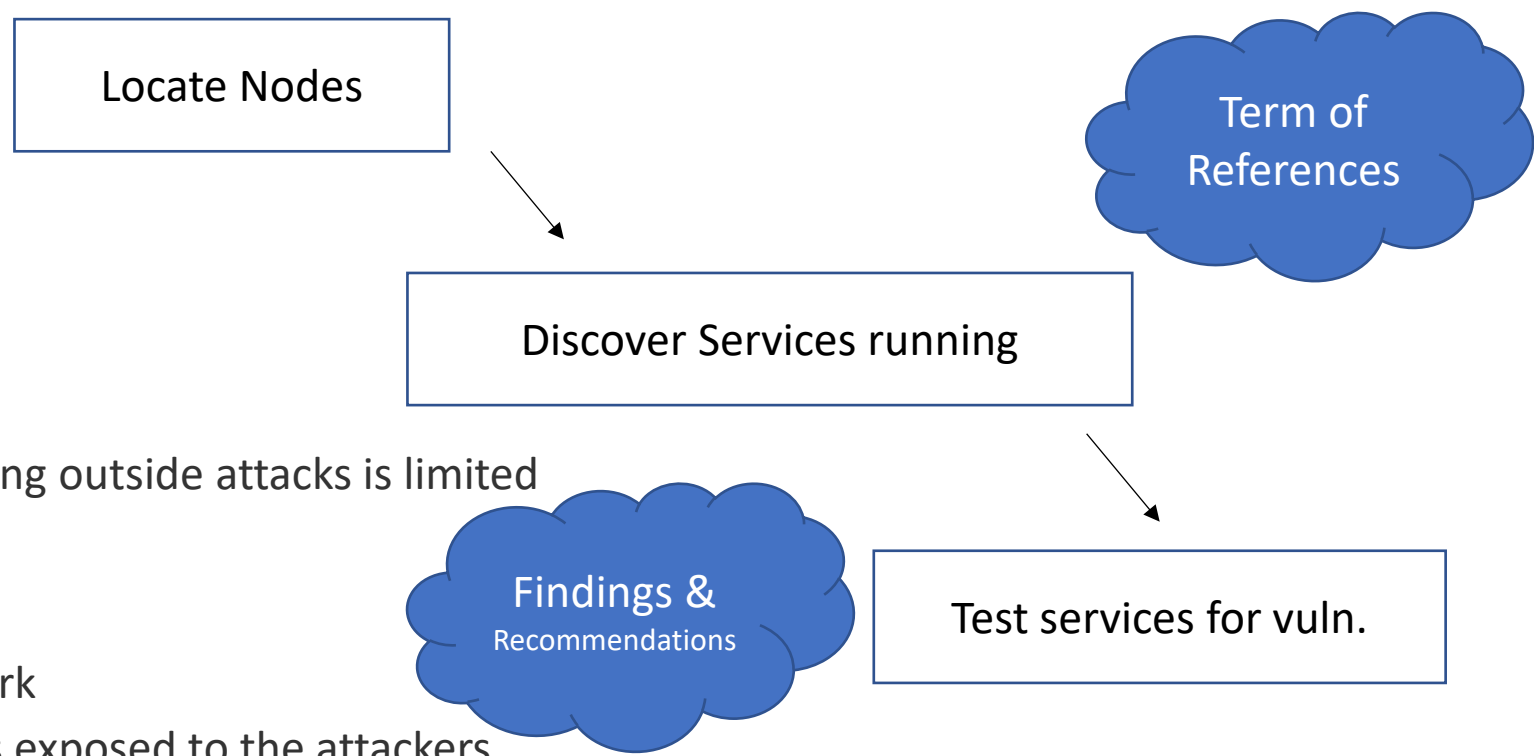
- Third Party Operation
- Inside the network or outside the network
- Because, it is outside the network, this is exposed to the attackers

- **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

$$\text{BaseScore} = (.6 * \text{Impact} + .4 * \text{Exploitability} - 1.5) * f(\text{Impact})$$
$$\text{Impact} = 10.41 * (1 - (1 - \text{ConfImpact}) * (1 - \text{IntegImpact}) * (1 - \text{AvailImpact}))$$
$$\text{Exploitability} = 20 * \text{AccessComplexity} * \text{Authentication} * \text{AccessVector}$$
$$f(\text{Impact}) = 0 \text{ if } \text{Impact}=0; 1.176 \text{ otherwise}$$

Vulnerability - Scoring System

CVE

- Common Vulnerabilities and Exposures is a public/ free to use list of standardized identifiers for commonly found vulnerabilities and its exposures.

[illegible]

🚩 CVE-2021-43619 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

Trusted Firmware M 1.4.x through 1.4.1 has a buffer overflow issue in the Firmware Update partition. In the IPC model, a `psa_fwu_write` caller from SPE or NSPE can overwrite stack memory locations.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:


NIST

NVD

Base Score:

N/A

NVD score not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. 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 rvd@nist.gov.

CVE-2020-35391 Detail

Current Description

Tenda N300 F3 12.01.01.48 devices allow remote attackers to obtain sensitive information (possibly including an `http_passwd` line) via a direct request for `cgi-bin/DownloadCfg/RouterCfm.cfg`, a related issue to CVE-2017-14942. NOTE: the vulnerability report may suggest that either a ? character must be placed after the `RouterCfm.cfg` filename, or that the HTTP request headers must be unusual, but it is not known why these are relevant to the device's HTTP response behavior.

[+View Analysis Description](#)

Severity

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

	NIST: NVD	Base Score: 6.5 MEDIUM	Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
	CNA: MITRE	Base Score: 9.6 CRITICAL	Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: It is possible that the NVD CVSS may not match that of the CNA. The most common reason for this is that publicly available information does not provide sufficient detail or that information simply was not available at the time the CVSS vector string was assigned.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. 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.

Hyperlink	Resource
https://medium.com/@signalhilltech/tenda-n300-authentication-bypass-via-malformed-http-request-header-5b8744ca685e	Exploit Third Party Advisory

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.**
 - Demonstration Time: 10 Minutes
 - Do the scan in advance – Demo on what your scan picked up and your approach in detailing the vulnerabilities and enumerating them.
 - Demonstration slot will be done by ChatGPT. Others will use the assignment link to submit their demonstration by recordings.

Volunteers are welcome to do the demonstration.

This could be a good exercise for your Coursework Demonstration.

Module Feedback

VM Download



\\192.168.135.200\ACCB6000\$

Any Questions?

References

- **EC-Council CEH**
- **Cisco Networking Academy**
- **Tevel Cyber Corps**
- **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**