Network Security and Penetration Testing

Terminal Assignment-based Assessment (60%)
Sem. 2, 2021-2022

DEADLINE: Sunday 8th May 2022 @ 23:55

WEIGHT: 60% of overall marks

COURSE: MSc / PGDip in Cybersecurity (January 2022 Intake)

SUBMISSION: The final report must be submitted as a Word or PDF document to Moodle before the deadline.

TURNITIN: This is an individual assessment. All report submissions will be electronically screened for evidence of academic misconduct (i.e., plagiarism and collusion)!

AIMS AND OBJECTIVES:

This assessment replaces the written examination, and primarily assesses the learning outcomes LO1 and LO3 of the module:

LO1. Critically assess network security characteristics and determine the scope of a penetration test of a network system.
LO2. Design, develop, and implement a security test on network infrastructure in a reasonable time frame.
LO3. Research and critically analyse network and network application security vulnerabilities.
LO4. Justify the choice of tools and techniques that are employed for penetration tests and evaluate the results of these tests.

The assessment consists of the following tasks:

1) Research and define a complex and realistic network setup, including specific devices that would make part of the network.
2) Research **2 or 3 attack vectors** (depending on complexity and amount of details), that hackers could use to gain access to the network (or parts of it), as well as mitigation solutions to protect against such attacks.
3) Write a report to document the research carried out.

IMPORTANT NOTES:

1) This is a research-based assessment, you are not required to do any practical work.
2) Network setup should mainly include recent devices and software versions that were released in the **past 3-12 months**, if older they should be supported by market statistics and justified.
3) For the attack vectors focus on recent vulnerabilities and security incidents from the **past 3-6 months**.
4) You need to demonstrate that your research focus is recent by providing release dates in the summary tables, and references (i.e., to device specification web pages, recent CVE numbers, real world security incidents, etc.), formatted in the IEEE style that include the full date or at least the month and year.

DELIVERABLE:

A **6-page** IEEE double column format report including all figures, tables, and references.

The IEEE template to be used is available on Moodle and can also be found at the below URL: https://www.ieee.org/conferences/publishing/templates.html.

REPORT STRUCTURE:

1. **Executive Summary**
   - Brief description of the scope and objectives.
   - Brief description of the network and justification why you chose this network type.
   - Summary of key findings and recommendations.

2. Network Setup

- Describe the process you followed to define the network setup (e.g., researched network types, researched specific devices, etc.).
- Discuss the aspects that make this a realistic and complex network setup.
- Draw and include a diagram of your network setup. Note that if you choose a large network, you should only draw its main components and devices (e.g., do not draw tens or hundreds of clients but draw 1-3 client devices from different categories such as HR, IT, lecturer, student, etc.).
- Describe the network characteristics, its type (e.g., LAN, WAN, etc.), its purpose (e.g., home network, SME network with only company devices or both company and BYOD devices, campus network, hospital network, etc.).
- Include a summary table of the main devices making up the network (e.g., client devices, servers, routers, switches, appliance firewalls, IoT devices, etc.). For each specific device include the main hardware (e.g., release date, manufacturer, model, etc.), and software details (e.g., OS version and release date, main service application like Apache/IIS web server, main client application, etc.). Do not include too many details but include details that are important for the attack vector (e.g., mention your network card chip and firmware if you will discuss some vulnerability with them, mention the vulnerable client application that can be exploited such as MS Word, Chrome, or Zoom, etc.).
- Describe any assumptions that you make related to your network setup (e.g., if client devices run older OS version like Windows 7 or Android 8, provide some market share statistics or estimates to show the percentage of devices using this version globally or in specific context, e.g., hospitals). *Your main assumption should be that the network and devices are quite secure, so focus on recent vulnerabilities and attacks (i.e., from the **past 3-6 months**).*
- The idea is not to just have a generic diagram but a personalised network. For example, if you choose to focus on a home network, personalise it with specific devices you personally have (e.g., smartphones, laptop/desktop PCs, gateway/router, TVs, game console, IP camera or other IoT devices, etc.). If you do not have many devices and your network would be too basic expand it by adding some more specific devices that you would like to have. If you choose to focus on a company network, connect to your work experience (if you have any) and/or do some research and exemplify with specific routers/switches/firewalls that a company may use (e.g., by Cisco, Juniper, etc.), servers and/or client desktops/laptops that a company may use (e.g., by Dell, Apple, etc.), client devices that BYOD employees would potentially use (e.g., Windows / Mac OS / Linux laptops, iPhones / Android smartphones, etc.). Note that you may also consider that these days many companies use cloud services, rather than buying and maintaining their own HW servers.
- Make sure to cite all relevant sources you consult while defining your network setup.

3. Attack Vectors

- Start the section with a justification of why you chose these attack vectors and discuss how they are different (e.g., in terms of techniques, targeted technologies / devices, vulnerabilities, exploits, etc.).
- Include a table summarising the main characteristics of the attack vectors (e.g., type, techniques, CVE number, brief description, exploit, date of incident, etc.).
- Have a separate subsection with meaningful heading for each of the attack vectors.
- In each subsection include a detailed description of the attack vector, interpretation and critical analysis of the findings. The details can include but may not be limited to:
  - Motives (e.g., eavesdrop, monitor activity, steal information, ransom, etc.).
  - Techniques (e.g., physical access, social engineering, firewall bypassing, password attacks, DDoS, implanting malware, exploiting software vulnerabilities, etc.).
  - Target devices / technologies – which specific devices and/or technologies from your network are being targeted (e.g., wireless technologies WiFi / 4G / Bluetooth, network devices like routers / switches, security systems like appliance firewalls / IDS, servers, client devices, IoT devices, etc.).
  - Vulnerabilities (e.g., in hardware, software, protocols). Include CVE numbers and details about specific vulnerabilities that could be exploited as part of the attack (i.e., you can search databases such as https://cve.mitre.org/ or https://nvd.nist.gov/).
  - Exploits – detail any known exploits for the vulnerabilities (e.g., you can search Google and/or exploit databases such as https://www.exploit-db.com/).
  - Impact of the attack if successful.

- Reference and briefly describe recent real world security incidents from the **past 3-6 months** that used this attack vector on individuals or companies to support your answers.

4. Mitigation Solutions

- Research and discuss mitigation solutions and provide recommendations on how individuals / organisations can protect themselves against these attacks (e.g., best practices, firewalls, IDS/IPS, anti-virus, network segregation, VLANs, etc.).
- Reference and discuss specific patches/update numbers, new guidelines (e.g., NIST SP 800-63 B (2020) for password guidance), legislation (e.g., California bans default passwords), or standards (e.g., WPA3), and discuss what would be the consequences for the users (e.g., using stronger passwords may be cheaper than buying WPA3 access points).

5. Conclusions

- Include an overall discussion of the main findings, limitations, and implications.
- Detail next steps (i.e., what else would you do if you had more time).

6. References:

- Include references to all the resources you consulted when preparing this assessment (e.g., device specification webpages, research papers, web resources, tutorials, etc.).
- Each reference in the list must include corresponding in-text citation(s) and be properly formatted according to the IEEE citation style (for more details consult the NCI Library Referencing Guide available at https://libguides.ncirl.ie/referencingandavoidingplagiarism).
- You can also use a tool such as Zotero which helps with collecting, organising, and citing your sources. You can watch this brief tutorial that shows how to save webpages and references from online databases (e.g., Google Scholar, IEEE Explore, ACM Digital Library, etc.), and cite them in MS Word: https://www.youtube.com/watch?v=ExmY4b3LvAA. However, make sure you carefully check each reference in your database and complete any missing details as sometimes Zotero cannot do it correctly. You can also export your Zotero references to BibTeX format if you use LaTeX to write the report.

MARKING SCHEME:

Component	Weight	Criteria for H1 (≥70%)
Executive Summary	10%	Objectives were clearly specified and fully achieved. Excellent concise summary and justification of the network chosen. Excellent concise summary of key findings and recommendations. Insightful executive summary.
Network Setup	20%	Detailed description of the process followed to define the network setup. Realistic and complex network setup with recent devices and software versions. Detailed, well-drawn diagram of the network setup. Excellent summary of the network characteristics and devices. Comprehensive discussion and justifications with supporting references.
Attack Vectors	40%	Detailed discussion of how the attack vectors are different. Excellent and comprehensive summary table of the attack vectors. At least three complex attack vectors are presented. Variety of attack techniques, target devices / technologies, vulnerabilities, exploits, etc. Thorough description and discussion of the attack vectors supported by recent references.
Mitigation & Conclusion	20%	Mitigations are thoroughly presented, discussed and supported by references to literature. Insightful conclusions that appreciate limitations and implications of the study.
Report Quality and Referencing	10%	Well written and structured report, with excellent use of language, headings, image/table captions. Consistent and complete citation and referencing of source material using the IEEE referencing style. IEEE template is well adhered to.