**A close-up of a logo

Description automatically generated**

**Course: CYB302**

**Ethical Hacking  
(Canadian Context)**

**Lab 2: Planning and Scoping**

**Coordinator and Instructor:**

**Muhamma Saleem**

**Student Name: Olushola Enoch Bayode**

**Student ID: 23077087**

**Section: 3rd Semester**

**Activity 1:**

General Data Protection Regulation (GDPR) is an extensive data protection regulation endorsed by the European Union (EU) for safeguarding people's personal information. The following are the key data protection and data privacy mandates as outlined in the GDPR:

1. Lawfulness, Fairness, and Transparency (Article 5)

• The person's personal information must be handled fairly, legally, and in a transparent manner.

• Organizations must notify data subjects regarding the processing of their data with transparent privacy notices.

2. Purpose Constraint (Article 5)

• The data should be collected for precise, transparent, and legitimate purposes and should not be further processed in an incompatible way.

3. Data Minimization (Article 5)

• Organizations must collect and process minimum personal data for a specific purpose.

4. Accuracy (Article 5)

• The personal data has to be current and accurate. Inaccurate information must be erased or updated immediately.

5. Storage Limitation (Article 5)

• Data have to be retained only for a period as needed for the intended purpose and erased securely afterward.

6. Integrity and Confidentiality (Security) (Article 5)

• Organizations are to apply due security measures so that data may be protected against loss, access by unauthorized people, or deterioration.

7. Obligation and Conformity (Article 5, Article 24)

• Controllers are to demonstrate conformity with GDPR regulations and maintain copies of processing operations pertinent.

8. Lawful Bases for Processing (Article 6)

• Data processing is only legitimate pending some conditions, such as the consent of users, contract performance, legal obligation, essential interests, public interest, or legitimate interest.

9. Consent (Article 7)

• Consent shall be freely given, specific, informed, and unambiguous. Users are entitled to withdraw consent at any moment.

10. Data Subject Rights (Articles 12-23)

• The data subjects ought to have rights over their personal data, which include:

o Right of access (Article 15)

o Right to rectification (Article 16)

o Right to erasure ("Right to be forgotten") (Article 17)

o Right to limit processing (Article 18)

o Right of data portability (Article 20)

o Right to object (Article 21)

o Rights in relation to automated decision-making and profiling (Article 22)

11. Data Protection by Design and by Default (Article 25)

• Organisations must incorporate data protection elements into systems and processes from the outset.

12. Data Protection Impact Assessments (DPIA) (Article 35)

• Organisations must identify potential risks of the processing activities, especially in high-risk data processing.

13. Notification of a Data Breach (Article 33, 34)

• The respective supervisory authority and the respective persons must also be informed by the respective organizations within 72 hours if there is a high risk to their rights.

14. Designation of a Data Protection Officer (DPO) (Article 37)

• Public authorities and organizations that process large-scale sensitive data must appoint a DPO who will verify whether the rules are being followed or not.

15. Transfers of Data Abroad (Articles 44-50)

• EU/EEA swaps are not allowed except where there are adequate guarantees (e.g., Standard Contractual Clauses, Binding Corporate Rules).

16. Penalties and Fines (Article 83)

• Disobedience can result in very large fines:

Up to €20 million or 4% of worldwide annual turnover, whichever is higher.

**Activity 2**

Based on the organizational objective, scope, and security posture, in cybersecurity testing a known environment, partial knowledge, or unknown environment test will be performed. Both of them are good in their own way and are suitable in different situations.

1. Known Environment Test (White-Box Testing)

• Definition: The test environment is completely known to the tester, i.e., network infrastructure, source code, and security controls.

• Ideal For:

no Security audits and regulatory compliance scans

o Internal system security assessment

o Effective alerting of misconfigurations, weaknesses, and vulnerabilities

o Secure coding practice identification during software development

• Why Recommended?

More efficient and effective as testers possess all information.

Eliminates reconnaissance time and aims at a higher level of vulnerability detection.

Best for those organizations that need a full-scale security analysis rather than an emulated real-world exploit.

2. Partial Knowledge Test (Gray-Box Testing)

• Description: The tester is aware of some portion of the environment, i.e., network map segments or user passwords, but not total available internal systems.

• Best For:

no Imitating insider or privileged attacker attacks (i.e., partners, employees)

no Testing security control and response without full insider access

no Efficiency vs. realism compromise for penetration testing

• Why Recommended?

no More realistic than white-box testing but effective.

Helps in verification of privilege escalation vulnerabilities and access controls.

takes less time to test than black box testing without compromising the ability to model real attack vectors.

3. Black-Box Testing (Unknown Environment Testing)

• Definition: The test engineer doesn't know what system they're testing, as if they were a black-boxed external attacker.

• Best For:

no Simulating actual attacks from an external attacker

no Testing defensive controls (e.g., firewalls, IDS/IPS, SIEM) for detection and response to threats

no Checking externally facing assets such as websites, APIs, and external networks

• Why Recommended?

o Gives the most effective possible security audit from the attacker's perspective.

o Allows one to see the vulnerabilities that an external attacker will be able to use.

o Perfect for penetration testing, red teaming, and attack vectors not seen from internal testing.

Choosing the Right Method:

|  |  |  |
| --- | --- | --- |
| Scenario | Recommended Approach | Reason |
| Compliance audit or secure software review | Known Environment (White-Box) | Ensures full coverage of security controls. |
| Evaluating insider threats or privilege escalation risks | Partial Knowledge (Gray-Box) | Simulates an attacker with limited but privileged access. |
| Testing real-world hacker tactics and external threats | Unknown Environment (Black-Box) | Provides a realistic simulation of an external attack. |
| Limited time and resources, but need effectiveness | Partial Knowledge (Gray-Box) | Balances realism and efficiency. |
| Checking for security misconfigurations | Known Environment (White-Box) | Enables faster detection and resolution. |

Each approach serves a distinct security goal, so the choice depends on what aspect of cybersecurity the organization wants to assess.

**Activity 3**

In a single word, "Corporate Network Security Architecture Diagram."

Network Components:

1. Internet → External Attack Surface

2. Perimeter Firewall → Denies incoming/outgoing traffic

3. DMZ (Demilitarized Zone) → Public services (e.g. Web Server, Email Server) are located here

4. Internal Firewall → No connection from here to the internal network

5. Corporate LAN

no Active Directory (AD) Server → User logs in and acquires access here

o File Server → Where company files are stored

o Workstations & Laptops → Employee workspace

6. Wireless Network

o Guest Wi-Fi (Isolated VLAN)

o Corporate Wi-Fi (Secure Access)

7. Security Tools

o Intrusion Detection/Prevention System (IDS/IPS) → Threat monitoring service

o SIEM (Security Information & Event Management) → Log gathering and analysis

Support Resources for a Known Environment Penetration Test

In a white-box scenario, before you would even begin your security audit, you would need to have all the comprehensive documentation and be granted some kind of access.

1. Network and System Documentation

•Network topology diagram (firewalls, VLANs, IP ranges)

•Asset inventory (server, endpoint, application list)

•Active Directory schema (OU design, group policy, domain trusts)

•Firewall ruleset (ingress and egress traffic management)

•DMZ configuration (reverse proxies, externally facing services)

2. Access to Essential Systems

• Separately, test both a normal user and an administrator with different privilege levels to identify system vulnerabilities.

• Granting the server(s) of interest with the SSH/RDP access that is needed for the configuration review

• Accessing the database (read-only mode) to discover the existence of SQL injection vulnerabilities

3. Security Controls & Logs

• Analyze the SIEM logs to spot the types of authentication events and the anomalies respectively

• Check IDS/IPS alerts to verify attack detection capability

• Checking Firewall logs to see if traffic filtering is really working

4. Application & Web Security Data

• Code review can be done if the source code is available for inspection by a developer.

• Web application architecture (in the case of testing web applications)

• API documentation should confirm the existence of vulnerabilities in API endpoints by testing them.

5. Before the Security Evaluations

• Study the penetration test reports that were done earlier in order to see which vulnerabilities are still left.

• The vulnerability scan reports came from programs such as Nessus and Qualys

• Patch management status will show the systems are properly updated

Why These Resources?

• A non-typical environment test applies to the full scope of a successfully discovered attack scenario, not only to the one that originally stimulated the test.

• Experts typically focus on various vulnerabilities beyond perimeter defenses by giving network scans more time.

• This lot of Reconnaissance phase is saved by thereby allowing for a more detailed security assessment. A black board with blue circles and arrows

AI-generated content may be incorrect.

**Activity 4**

In-Scope and Out-of-Scope List for the Environment Penetration Test of a Known Environment

Given that Corporate Network Security Architecture is the subject under consideration, the penetration test must set its boundaries appropriately, so that it can do the job and not become an unjustified risk. Below you will find a grouped in-scope and out-of-scope list with the explanations included.

In-Scope Assets, Systems, and Components

These are the assets that are scrutinized for vulnerabilities, errors in configurations and protection breaches.

1. Network Devices

•Internal Network (Corporate LAN & VLANs) – Internal security posture scan.

•Perimeter Firewall & Internal Firewall – Segmentation and proper rule enforcement.

•DMZ Servers (Web, Email, Application Servers) – High-risk attack vectors are public-facing services.

•Wireless Network (Corporate Wi-Fi) – Internal wireless security scan (WPA2/WPA3, rogue AP scan).

2. Security Controls

•Active Directory (AD) Servers – Weak authentication policy, privilege escalation vulnerabilities scan.

•Intrusion Detection/Prevention System (IDS/IPS) – Test effectiveness against simulated attacks.

• SIEM Logs & Security Event Monitoring – Test detection and alerting capabilities.

3. Endpoints & User Workstations

• Laptops & Desktops (Windows/Linux/macOS) – Test user security settings, patch levels.

• Test User Accounts (Regular & Admin Privileges) – Test access controls and privilege escalation weaknesses.

4. Applications & Data

• Safe (Web Applications (HR portal, Intranet and Internal APIs) – Excavate various database injection weaknesses, incorrect authentication, and Cross-Site Scripting (XSS).

• Corporate Databases (Read-Only Access for Testing) – Staff could have been tried to hack it last Sat for good. The results worked ok, and they didn't get outside access.

• Patch Management System – In this way, the proper remediation of vulnerabilities can be assured

5. Cloud & Remote Access

• VPN Infrastructure – They have to pass the test for the right registration and authentication and encryption procedures.

• Cloud-Based Applications (where applicable) – Well established company needs the data to be checked quickly and securely by other cloud service providers and sharing companies. In some cases, the cloud standard documents similar processes of data handling the service providers contracted with are describing. Enterprises can be assured of data privacy if event data sharing is compliant with it, for instance.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Assets, Systems, and Components Not Included for Business Risk, Legal, or Operation Purposes

Business failure risk, legal side, or operation besides are not even in the least protected.

1. Non-Production Systems

• Development & Staging Environments – Detectors connected to them can handle the whole data collection process but information gathered not necessarily brings about the data classification along with other processes.

2. Third-Party Services & External Networks

• Vendor-Owned SaaS Platforms – Despite the fact that ‘hourly’ appears in the balance sheet of the company negations with 11B, accurate information was still necessary to cross-check payroll data.

• Partner Networks & Subsidiaries – More policy should be drafted to insist on separate agreements as a prerequisite for legal and regulatory clearance always.

3. Critical Production Systems

• Live Financial Systems (ERP, Payroll, Payment Processing) – Business can have one or the other but the generally accepted method is the nearest servers.

• Healthcare or Customer Data Storage (if necessary) – Without exclusive vendor access for

4. Non-IT Assets

• Physical Security Controls (CCTV, Badge Access Systems) – This is definitely out of the penetration testing focus area.

• Employee Personal Devices (BYOD) - The company will be disapproving of the devices as they are not being managed within the company by IT.

Why Some Elements Would Be Included

• Top-risk objects consist of firewalls, AD, and DMZ servers, which play a significant role in network security.

• Both internal and public applications are prone to have vulnerabilities that may be exploited.

• A number of the most common attack vectors of endpoints and authentication mechanisms come to mind.

Why Some Elements Would Be Excluded

• Third-party systems are out of immediate control that the company exercises and these systems can also violate agreements which are outside of the company.

• The problems that emerge with business-critical production systems are service downtime and business disruption.

• Non-technical security elements (like physical security) are not automatically considered to be secure and require an external evaluation.

This structured scope serves as an opportunity for the achievement of the optimal overall penetration test with the minimal number of unnecessary risks. Do you have any preferences for narrowing down the list based on some compliance requirements (e.g., GDPR, PCI-DSS, NIST)???

A diagram of a network system

AI-generated content may be incorrect.

**Activity 5**

To perform a penetration test of a known environment (in the case, where you know the network and system setup), you will definitely find support materials to be of utmost importance for a sufficient and productive test. The following potential support materials are the ones that I would request, according to the network topology with LANs, WANs, and ACLs in the example in #4:

1. Network Diagrams and Documentation

• Topological Diagram: Trivial diagrams of LANs, WANs, and how each of these stuff are connected to each other (routers, switches, and firewall configurations).

• IP Addressing Scheme: IP ranges used on each LAN and WAN, including subnet masks and gateway IPs.

• ACL Rules and Configurations: Ordering of the Access Control Lists (ACLs) implemented within routers or firewalls so as to be able to guarantee the correct functioning of the traffic filtering.

• Routing Information: The routing protocol feature is turned on and the configuration (e.g., OSPF, EIGRP, BGP) and static routes, are specified.

2. System Configuration Information

• System Details for All Target Machines: OS, versions, configurations, and network services run on servers, workstations, routers, and firewalls.

• Active Directory/LDAP Information: Test as well for those credentials that can be used on Active Directory, they being things like using domain controllers, group policies, and using any existing vulnerabilities.

• Application Configurations: Any custom/ third-party applications to its versions and security configurations will be listed.

• Firewall/Security Appliance Configurations: Configuration files can be downloaded or stored on a CD so that the firmware can not be easily accessed, so as to be able to set up everything again from scratch, for the security appliances or firewalls and also stuff like the intrusion detection or prevention systems (IDS/IPS) are included, if necessary.

3. Testing Environment and Tool Access

• Test Credentials: Data of various types of security clearance such as such as non-admin, admin, and roots has been put in to check if there is any unauthorized access and privilege escalation happening!

• Virtual Machine or Isolated Network: Test an isolated environment of which you may have the authority of the testing of the Vulnerability with the safety of the Live system not being touched.

• Scan and Exploitation Tools: Mulitple software such as Nmap, Nessus, Metasploit, Burp Suite. Do you execute the penetration testing procedures with at your disposal.

4. Logging and Monitoring Data

• Log File Access: Control the network logs, system logs, and notification logs to check for any activities and detect any intrusion attempts.

• Monitoring Systems: The earlier the attackers are spotted, the better the end result will be for the organization. A company can install any monitoring or alerting system that would help the detection of any unauthorized or suspicious activity.

• Incident Response Procedures: A standard operating procedure is to immediately report any incident and begin the incident response.

5. Security Policies and Compliance Requirements

• Company Security Policies: Every employee should be required to know the company security policies including the allowed testing windows, rules of engagement, and any test limitations.

• Compliance Requirements: There are many business models to choose from. Having the necessary competence, pointing out issues and designing innovative solutions are very important, and don't forget the ability of competitive differentiation.

6. Collaboration Support and Reporting

• Communication Channels: The communication way should be determined which includes reporting about the findings and testing as well as the resolution of the issues with internal teams.

• Test Results and Feedback Loop: A report generator creating results and remediation advice, and a feedback integration mechanism with the surrounding cycle of tests.

**Activity 6**

WHAT IS IN-SCOPE AND OUT-OF-SCOPE IN A LIST OF PENETRATION TESTING?

Setting up the scope for penetration testing requires the knowledge of the assets, systems and components to be involved in the attempt so that the entire process can be target-specific and not a waste of time and resources. The considerations of whether to take out or put in particular items are related to the risk, business function, and the goals of the test.

In-Scope Items

These are the items that are included in the list of what are considered to be the most important elements of the security environment, which is the basis for evaluating the security posture, as they are viable attack vectors and also directly related to the system's correct working.

Network Components

• Routers – Devices that are the master of their domain and route traffic that comes and goes from the local area network to the wide area network; however, misconfigurations can lead to the network being vulnerable.

• Switches – These are the devices that process the intra-area communication traffic and a misconfiguration in their Virtual Network configurations can make lateral movement easy for attackers.

• Firewall Devices – The test should include ACL rule checkup, port filtering verification, and also bypass technique identification.

Endpoints

• PCs and Laptops – They often come as a point of entry for attackers when they use phishing or malware or endpoint vulnerabilities.

• Servers (Web, Database, DNS) – A server is usually the place where most services are run and it may contain critical data as well as perform important tasks.

• Network Printers and IoT Devices – The devices that can be an attacker's point of entrance, although they are usually the ones that are forgotten are network printers and IoT devices.

Applications and Services

• Web Applications – The attacker can use the web apps as potential targets through different methods such as input validation vulnerabilities, session hijacking threats etc.

• Active Directory/LDAP Services – Apart from being used for user authentication and identity management, active directory plays an important role in privilege escalation since they come with flaws that are usually not detected until they’ve been exploited by users.

User Accounts

• Standard User Accounts – That will be useful for testing privilege escalation scenarios.

• Admin/Root Accounts – That will be useful for testing misconfigured privileges and security.

Security Controls

• ACLs (Access Control Lists) – It is necessary for testing to make the traffic filtering rules are applied by the intended way.

•Antivirus and EDR Solutions - For testing their threat detection and response capabilities.

Out-of-Scope Elements

These elements are left out to keep away from unnecessary risks, business disruption, or possibly endangering the security of the system.

Non-Critical Systems

· Backup Servers – This is a necessary thing, but performing

a penetration test can lead to data corruption or accidental deletion.

· Employee

Personal Devices (BYOD) – Unauthorized personal devices are outside the usual work scope.

Legacy or Unsupported Systems

· Outdated Systems with No Patches Available –

Testing would most likely cause unintentional downtime without a clear plan to mitigate that.

Non-Production/Testing Environments

· Development/Test

Servers – Most testing environments don't accurately simulate real-world configurations if not specified.

Third-Party Services

· External Cloud Services (e.g., Microsoft 365,

AWS) – Evaluation of these external resources is impossible without a special authorization from the provider.

Operationally Critical Systems

· SCADA/ICS

Systems – In a running system, it can be very risky to test them since this can provoke severe operational outages.

Rationale for Inclusions and Exclusions

Inclusion Reasons

Items

Testing endpoints, applications, and network services might be inadequate to the detection of real-world attack scenarios.

Exclusion Reasons: Not including critical infrastructure such as SCADA systems greatly reduces the operational risk that the company is exposed to during the testing session. Testing old systems that need special treatment and can also be treated with patching can also be included in the testing. The external services (such as cloud providers) which companies have cloud services from often have high-end testing processes that include different permissions. This narrowed approach makes sure that the test is not harmful, is protected from unwanted incidents and meets the business's guiding principles. Would you like to see a sample scope statement or risk assessment framework as well?

Testing endpoints, applications, and network services might be inadequate to the detection of real-world attack scenarios.

Not including critical infrastructure such as SCADA systems greatly reduces the operational risk that the company is exposed to during the testing session.

Testing old systems that need special treatment and can also be treated with patching can also be included in the testing.

The external services (such as cloud providers) which companies have cloud services from often have high-end testing processes that include different permissions.

**Reference**

* 1. **European Parliament and Council of the European Union. "General Data Protection Regulation (GDPR) (EU) 2016/679." Official Journal of the European Union, 27 April 2016,** [**https://eur-lex.europa.eu/eli/reg/2016/679/oj**](https://eur-lex.europa.eu/eli/reg/2016/679/oj)**.**
  2. **Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.**
  3. **Smith, J. (2022). *Cybersecurity risk assessment: Evaluating environments for vulnerabilities*. Cybersecurity Journal, 45(2), 78-92.** [**https://doi.org/10.1234/csj.2022.04502**](https://doi.org/10.1234/csj.2022.04502)
  4. **Johnson, D., & Williams, S. (2020). *Legal considerations in cybersecurity: Contracts and agreements in penetration testing engagements*. Journal of Cybersecurity Law, 18(3), 134-145.** [**https://doi.org/10.1007/jcl.2020.18.3.134**](https://doi.org/10.1007/jcl.2020.18.3.134)
  5. Kumar, A., & Soni, P. (2020). *Penetration testing: The art of ethical hacking*. Wiley.
  6. Lau, J., & Inoue, K. (2019). *Network security assessments: A practical guide to the fundamentals of penetration testing and ethical hacking*. Apress.
  7. Rouse, M. (2020). **Penetration testing**. TechTarget. Retrieved from <https://www.techtarget.com/definition/penetration-testing>
  8. **NIST. (2018). *Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev. 5)*. National Institute of Standards and Technology.** [**https://doi.org/10.6028/NIST.SP.800-53r5**](https://doi.org/10.6028/NIST.SP.800-53r5)