



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

Hardening Network!!!



Advanced Cybersecurity - Continuation (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**
- **Network Scanning, Tools and Techniques**
- **Banner Grabbing**
- **Scanning – PenTesting**
- **Enumeration Concepts, Techniques, 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...

Understanding and Assessing Vulnerabilities

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

Social Engineering

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

Lab/ Tutorials

- **Activity 1 Getting Ready**
- **Activity 2 Information Gathering**
- **Activity 3 Scanning and Enumeration**
- **Activity 4- Vulnerability Assessment**
- **Activity 5 – Social Engineering**

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. 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.

Gaining access and escalating privileges

- ***Hacking Methodology (Based on CEH)***
- ***Understanding techniques to gain access to the system***
- ***Techniques to escalate privileges***

Lab/ Tutorials

- ***Activity 6 – Exploiting and Testing***

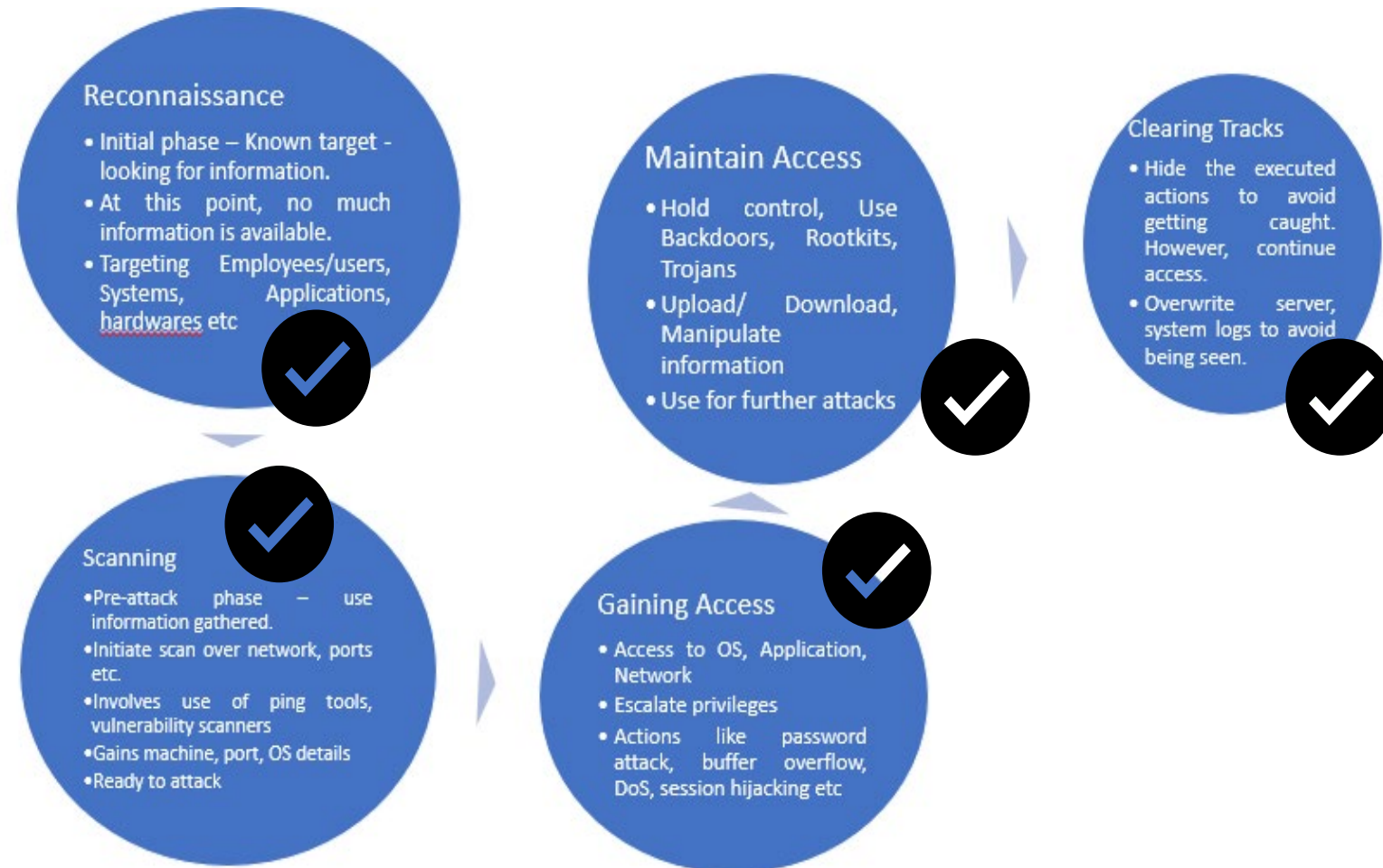
During this week, with applied knowledge and understanding on Footprinting, Network Scanning, Enumerating the target, and assessing vulnerabilities, we shall move forward focusing on the hacking methodology. We shall understand various techniques to gain access, escalate privileges, create and maintain remote access to the target.

During the tutorials, under isolated lab environment you will be using different techniques to gain access and escalate privileges.

Hacking - Methodology

○ Do you remember the process?

- ✓ Footprinting and Reconnaissance
- ✓ Scanning
- ✓ Enumeration
- ✓ Vulnerability Analysis
- Gaining Access
- Maintaining Access
- Clearing Logs



Pen Test

Identify Password Protected Systems: Do you have access to the password? Yes → Check the Password Complexity | No, → Go to next step

Perform Social Engineering, Shoulder Surfing, Dumpster Diving, Dictionary Attack, Brute Force Attack, Rule Based Attack, Guess the Password: Do you have access to the password? Yes → Good | No → Go to next step

Place Keyloggers/ Trojan/ Spyware, Hash Injection Attacks, Wire Sniffing, MiTM, Replay Attack, Rainbow Table Attack, Distributed Network Attack: Do you have access to the password? Yes → Escalate Privilege | No → Try Again (Go Home!!! Not your day)

Pen Test

Login using enumerated username and cracked passwords: Check your Privilege. Need more privilege? Yes → Go to next step

Perform DLL Hijacking, Exploit Vulnerabilities, Dylib Hijacking.

Privilege Escalated? Yes → Go to next step | No: Try other PE Techniques.

Check Firewall Status, Antivirus Status, Anti-Keylogging Software Status, Physical Security Status, Use Keyloggers, Spyware.

Application Executed? Yes → Go to next step | No: Try Remote tools to execute applications.



Pen Test

Install Rootkits in the target system: Perform Integrity Based Detection Technique, Signature Based Detection Technique, Cross View Based Detection Technique, Heuristic Detection Technique

Files Hidden? No → Go to next step | Yes: Great

Check Antivirus and Antispyware Software's, OS Patched and Updated: Use Windows hidden Stream to inject Malicious code, Steganography to hide secret message, Perform Steganalysis Techniques

Files Hidden? Yes → Go to next step | No: Try other Techniques.

Cover your Tracks: Remove Web activity tracks, Disable Auditing, Tamper Log files, Clear BASH Shell tracks, Clear Network Tracks, Close remote connections, Close opened ports



Report (Pen Test Outcomes)

Report

- A structured report that details the findings of the penetration tests that are conducted for a client.
- It is recorded by the involved pen testers
- It is a one-to-one correspondence exists between the documentation and the testing process.

Goal of the Penetration Testing Report

- Help **executive management** make decisions about implementing security controls in the organization.
- Help those **responsible for information system security** implement security controls and patch any flaw discovered during pen testing.
- Assure the organization that the testing team sincerely wishes to **improve the organization's security posture**.

Report (Pen Test Outcomes)

Objectives it to:

- List the security flaws, vulnerabilities, security misconfigurations, and other exploitable resources found during the testing.
- Analyze the options available to mitigate the vulnerability.
- Suggest solutions for security risks.
- Clarify prioritization of corrections for the client's assets
- Recommend actions to prevent possible future cyberattacks.

Report (Pen Test Outcomes)

Objectives it to:

- List the security flaws, vulnerabilities, security misconfigurations, and other exploitable resources found during the testing.
- Analyze the options available to mitigate the vulnerability.
- Suggest solutions for security risks.
- Clarify prioritization of corrections for the client's assets
- Recommend actions to prevent possible future cyberattacks.

Deliverables:

- Detailed analysis of the methodologies used in the testing.
- Detailed information about all the activities performed and their results in a clear standard format.
- Evidence of successful tests of the organizational resources in the form of pictures, videos, and documents.
- Detailed information about the affected resources, cyberattacks performed, tools used, etc..
- Documents that corroborate the test findings. *(Include information on the availability of updates, data from the compromised servers, details of the compromised accounts, etc)*
- Documents containing tips for remediating the security flaws, eliminating vulnerabilities, and strengthening the security of the tested components

Report (Pen Test Outcomes)

Types of Report

- **Executive report:**

- Complete testing process
- Includes details of the tested components, vulnerabilities, misconfigurations, updates required, and other details that can help the authorities make decisions for securing the target.

- **Host report:**

- Information about the hosts tested, vulnerabilities found, exploited hosts, etc.

- **Client-side test report:**

- Details of the client-side test such as phishing, spear-phishing, spam, and social engineering attacks used during the testing.
- Detailed information about compromised client-side systems.

Report (Pen Test Outcomes)

Types of Report

- **User report:**

- Information of users who were identified and targeted during the testing process along with the tasks performed by them.

- **Vulnerability report:**

- Detailed information about all the vulnerabilities found during the pen testing process.
- It is recommended that the report lists the components with vulnerabilities and also offers solutions to eliminate the vulnerabilities.

- **Activity report:**

- Activities that the testing team had performed across the organization
- Can also include various documents to support the claims.

Report (Pen Test Outcomes)

A good pen-test report should be:

- Written in simple language that everyone can easily understand.
- Written in a professional manner using formal language.
- Comprehensible to both technical and nontechnical personnel such as security admins and stakeholders.
- Clearly explain the purpose of the penetration test as well as that of writing the report.
- Provide complete information to the reader in a clear format and not contain unnecessary information.
- Grammatically correct, punctuated appropriately, and free of typographical errors.
- Provide accurate information and support it with proper evidence, such as screenshots of the test results and stolen credentials.
- Contain information sorted according to the security risks, with the highest risks being prioritized.
- Structured logically.
- The style of presentation and the usage of words should be attractive to readers.
- Should contain unbiased recommendations and suggestions based on the analysis by the pen testers

Report (Pen Test Outcomes)

A good pen-test report structure

- Final report delivery date
- Cover letter
- Executive summary:
 - Organization synopsis: This section includes a brief description of the organization and its network.
 - Purpose for the evaluation: This section defines the reason for undertaking penetration testing.
 - System description: This section includes a brief description of the systems used across the client organization.
 - Scope of the project: This section includes the total number of IP addresses, apps, devices, hosts, and other network resources that the organization had mentioned in the contract.
 - Summary of evaluation: This section should contain a summary of the tests performed by the pen testers and the results obtained.

Report (Pen Test Outcomes)

A good pen-test report structure

- Final report delivery date
- Cover letter
- Executive summary:
 - Assumptions/Timeline: This section should specify all the assumptions made during the testing process and include all the commencement and completion dates for each test.
 - Major findings and recommendations: This section should include a summary of the major findings and any issues that could lead to future cyberattacks. The testers should also mention any recommended actions to mitigate the vulnerabilities.
 - Testing methodology: This section specifies the standard frameworks and techniques followed to perform penetration testing.
 - Planning: This section includes the details of the planned penetration testing process and how the actual process was performed
 - Exploitation: This section includes all the detailed exploitation processes followed during the penetration test.
 - Conclusions: This is the concluding section of the report. These conclusions include any further suggestions from the testing team.

Report (Pen Test Outcomes)

Common Mistakes by Organisations/ you might come across

- Not understanding the scope of the pen testing service
- Not asking for a retest
- Not asking for a letter of attestation
- Using a vendor without creating and signing a contract
- Not receiving guidance on the type of test to conduct
- Not asking for a detailed debrief or report walkthrough
- Not asking for a report with detailed steps and reproducible results
- Using vendors and tools that provide reports with hundreds or thousands of vulnerabilities that are mostly not critical
- Employing an inexperienced pen tester who creates reports using automated tools

Checks to Harden

- Document
 - All devices (S-DC, LCD etc),
 - All services (DNS, DHCP, DHCP Relay, domain services),
 - network connections.
- Review findings from Nmap, Hping3, Nessus, and Metasploit to identify
 - exposed ports,
 - weak protocols,
 - unpatched vulnerabilities,
 - exploited payloads.
- Risk Prioritization
 - Classify risks using a matrix (e.g., high-impact: DC compromise; medium: client exploitation; low: misconfigurations).
 - Focus on internet exposure (VPN to LCD), domain admin privileges etc.

Checks to Harden

- Backup Critical Data
 - Create full backups of the DC (Active Directory, DNS zones), servers, and clients.
 - Test restores to ensure no data loss during hardening.
- Define and Establish security policies
 - Least privilege, password complexity, logging standards
 - Align with frameworks like NIST SP 800-53 or CIS Benchmarks.

Hardening

- **Segment and Isolate Networks**

- Enforce strict segmentation between 192.168.1.0/24 and 192.168.2.0/24
- Allow only necessary traffic (e.g., domain replication, DHCP relay).
- Disable unnecessary routing protocols and implement VLANs if hardware supports it.

- **Secure VPN Access**

- Setup VPN
- Harden the VPN gateway
- Enforce/ Propose multi-factor authentication (MFA),
- Use strong encryption (e.g., AES-256),
- Restrict VPN to specific Ips,
- Regularly rotate VPN certificates and keys.

Hardening

- **Implement Firewalls and IDS/IPS**

- Enable host-based firewalls on all devices (Windows Firewall on Windows hosts, ufw/iptables on Debian)
- Configure rules to block inbound internet traffic.
- Deploy network-level IDS/IPS (e.g., Snort on Debian Server) to monitor for anomalies (like port scans or exploit attempts).

- **Disable Unnecessary Protocols**

- Scan and disable weak protocols (e.g., SMBv1, LLMNR, NetBIOS) across the network to prevent lateral movement exploits seen in Metasploit.

- **Patch Management**

- Apply all critical updates to Windows Server 2022 (DC/DNS/DHCP), Windows 10 Client, Debian Server 12 (CLI).
- Use tools like WSUS for Windows and apt for Debian.
- Address Nessus-identified CVEs, especially those exploited in your Metasploit tests.

Hardening

- **Windows Server (DC at 192.168.1.1):**
 - Secure Active Directory:
 - Enforce strong password policies,
 - Enable account lockout,
 - Use Group Policy to restrict admin privileges.
 - DNS/DHCP Security:
 - Implement DNSSEC for DNS integrity,
 - Restrict DHCP to authorized MACs,
 - Log all queries/leases.
 - Disable unused services:
 - Stop and disable non-essential roles (e.g., if not needed, remove print services).

Hardening

- **Windows Client (at 192.168.1.10):**
 - Apply Group Policies:
 - Enforce antivirus (e.g., Windows Defender),
 - Auto-updates,
 - Screen locks.
 - User Access:
 - Run as standard user (not admin),
 - Enable BitLocker for disk encryption.

Hardening

- **Debian Server (DHCP Relay at 192.168.2.1) :**
 - Secure CLI Access:
 - Use SSH with key-based auth only (disable password login),
 - Restrict to specific IPs.
 - Service Configuration:
 - Harden DHCP relay (isc-dhcp-relay) by binding to specific interfaces, logging relays.
 - Kernel and Packages:
 - Remove unnecessary packages.
- **Kali Machine (in 192.168.1.0/24) Isolation:**
 - As a Pentest tool, isolate it in a DMZ-like subnet or use VLANs.
 - Revoke any domain memberships post-testing to prevent it from being a persistent threat vector.

Hardening

- Implement Least Privilege:
 - Audit and reduce admin accounts on the DC.
 - Use Just-In-Time (JIT) access if possible.
 - Enforce role-based access control (RBAC) for domain resources.
- Multi-Factor Authentication (MFA):
 - Enable/ Propose MFA for all logins (domain, SSH, VPN).
 - Integrate with tools like Duo or Microsoft Authenticator.
- Password and Credential Management:
 - Use a password manager for secrets.
 - Rotate credentials regularly and monitor for credential stuffing attacks.
- Encryption Everywhere:
 - Enable TLS for internal services (e.g., LDAPS for AD), encrypt disks (LUKS on Debian, BitLocker on Windows), and ensure secure boot on all hosts.

Hardening

- Incident Response Plan:
 - Develop a plan with steps for containment, eradication, and recovery.
 - Include regular tabletop exercises.
- Continuous Monitoring:
 - Use tools like Nessus for periodic scans and Metasploit for controlled exploit testing to validate hardening.
 - Repeat your initial pentest (footprinting, scanning, vuln assessment, exploitation attempts) to verify fixes. Ensure no regressions.
 - Document all changes, policies, and configurations.
 - Train "Blue Team" users on security awareness (e.g., phishing recognition).
 - Schedule monthly reviews: patch updates, log audits, and policy enforcement.
 - Automate where possible (e.g., Ansible for Debian configs, Group Policy for Windows).

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