UEEN4113 Network Security Management
Group Project (Jan 2017)

Project Deadline:
Week 14: Tuesday 18 April 2017

1 Project details

This is a group project. The minimum group size is 1 and the maximum group size is 4. Members of the group can be from any program (SE, ET) and year of study (2, 3 or 4).

The primary goal of this project is to set up a demonstration of a particular penetration test attack on a selected target system using a suitable combination of hacking tools. A possible defense against this attack should also be demonstrated using suitable security applications or via an appropriate security policy

To prevent multiple groups selecting the same attack avenue and potential copying and replicating among groups, all groups **MUST REGISTER** their selected attack venue at the link below. Each unique attack venue can be selected by at most 4 different groups, on a first-come-first-serve basis. Please ensure that you are logged into your UTAR student portal on your browser before attempting to access this link:

https://docs.google.com/a/1utar.my/spreadsheets/d/1SoEicVh_Cm-V5E7_1YI2OhFMg0ZTsCGbIyBAJln0U5g/edit?usp=sharing

The steps involved in this project are:

1. Select a particular technique or avenue of your choice to perform a penetration test or hacking attack on a targeted system. For e.g. directory traversal attack on a web server, SQL injection attack on a web application, buffer overflow attack on a vulnerable OS service or network application, etc. Once you have selected the technique of choice, register this on the link given above.

2. Provide a detailed description of the sequence of steps required to set up a sample system to demonstrate the attack. This includes

- specifying the target and attacking machine VM clearly (a specific version of Linux or Windows). If this VM is not a fresh install from an installation ISO, any additional patches or updates to the target machine VM needs to be clearly specified as well as how these patches and updates should be installed.

- Any additional applications that need to be installed on this target machine (for e.g. a web server, a web application, FTP clients, email clients)
- Links to download these applications and steps to install and configure them with the correct settings on the target VM

3. List and provide a short description of all the hacking tools and/or platforms that will be used to demonstrate this attack. Provide the steps required to install these tools and configure them properly on the attacking VM to perform the attack, if necessary.

4. Provide a detailed step-by-step outline of attack execution. For e.g. if Metasploit is used, the specific commands to be typed into `msfconsole` should be provided along with other supporting commands in a Kali Linux terminal. If a GUI tool like Nessus or Zenmap is used, then the option selections in the GUI interface for these tools must be specified in detail.

5. The attack should as far as possible proceed along the recommended steps for a standard penetration test methodology. All the attack outline steps outlined previously should be classifiable into one or more of the categories below:

    a) Enumeration and scanning
    b) Gaining access and escalating privileges
    c) Maintaining access
    d) Clearing tracks

6. List and provide a short description of all the security tools (e.g. firewalls, antiviruses applications, port monitors) that can be used to defend against this attack. Provide the steps required to install some (or all) of these tools and configure them properly to defend the attack. Show how the outlined attack fails when the tools are in operation.

7. Alternatively, provide a short description of the particular security policy that should be in place to prevent the attack (for e.g. don't download and install applications from unknown or untrusted web sites).

8. Identify a particular real life security incident or breach that involves the particular avenue of attack that you have chosen. Provide a brief summary of this incident (not more than 1500 words) with a link to a website that describes this incident in detail.

2 Additional notes

You can use the Kali Linux labs as a guideline for how to create your report detailing the setup and description of the hacking attack.

There are various websites that provide a database of exploits categorized according to attack techniques, some of which are listed below. You can use this as a starting point to determine which attack category you wish to demonstrate.

https://www.exploit-db.com
http://www.cvedetails.com/
https://cve.mitre.org/

The tools that you wish to employ for your hacking attack can be any one of the existing tools in the Kali Linux distribution (which covers all phases of the penetration testing) or other standalone tools that you are able to locate online. You are free to choose any particular tool(s) of choice.

I will attempt to replicate the attack procedure that you describe in your report. Marks will be awarded based on how easy it is for me to follow the outlined procedure easily and replicate the attack successfully on the VMs that I am using.

If you have a lot of difficulty finding a suitable hacking attack to describe in your report, then you can reuse the attacks described in the Kali Linux labs with additional procedures. However, your marks will be lower than a group which is able to formulate and document an original attack not covered in the lab.

There are many sites on the Internet that provide specific coverage on information security and cybercrime, some of these are listed below. This will be useful for you in completing step 8 of the assignment. Alternatively, you can also opt to search the news portals of major new sources such as CNN, BBC, etc by typing key search terms such as hacking, cybercrime, information security, etc.

https://nakedsecurity.sophos.com/
http://www.technewsworld.com/perl/section/cyber-security/
http://www.securityweek.com/cybercrime
http://www.darkreading.com/

Note that any attempt at plagiarism will be result in a penalty of zero marks. This includes reusing a previous project of your seniors. You may use their projects as a starting point for your project, with appropriate improvements or additions included from your group.

3 Submission details

- Both the softcopy **AND** hardcopy of the project must be submitted.
- The hard copy is a printed report containing the various project details described above. The front page of this printed report should hold the project marking scheme shown at the end of this document.
- The softcopy of this printed report should be emailed to me at: **hktan@utar.edu.my**
- A CD should be included with the hard copy submission. This CD will contain the installable executables for the various hacking and / or security tools that will be used in the project demonstration.
- There is no need to include the VM for the target and attacking machine on the CD. Your project report should however specify the VMs to be used.
- The hard copy should be handed up to me on your respective lab sessions on Week 14.

UEEN4113 Network Security Management
Group Project

Group members

Name	Student ID	Trimester and year of study
1. Xxxxxxxx	1234567890	YxTx
2. Xxxxxxxx	1234567890	YxTx
3.		

Marks breakdown

Parts	**Marks allocated**	**Comments**
a) The correct matching of the chosen hacking attack venue with the attack steps described	/ 10	
b) Proper and detailed description of the hacking tools and target system setup	/ 10	
c) Proper and detailed description of the attack procedure	/ 30	
d) Attack steps in categories other than hacking and gaining access (Scanning, Maintaining access, Clearing tracks)	/ 20	
e) Proper and detailed description of the defense procedure involving security applications or security policies	/ 10	
f) Correct identification and comprehensive description of security breach incident that relates to the chosen hacking attack venue	/ 20	
Total	/ 100	