ELEC 567 Project: Network Penetration Testing and Defense

	Part 1	Part 2
Due date	March 2, 2020	April 2, 2020
Weight	25%	20%

Overview

Neptune Bank is an online banking service provider. The company has a website for its employees and customers, and a private network.

As a financial service provider, their reputation relies not only on the quality of their services, but also on their ability to protect their own network and website. To anticipate and prevent possible breach, which would be damaging to Neptune's brand and reputation, you have been hired as an external cybersecurity consultant to conduct the penetration testing of Neptune' private network and website, and recommend appropriate mitigation solutions. Neptune' private network is accessible only by the employees, whereas the website can be accessed by the public, their customers and their employees.

Part I: Penetration Testing

As a penetration tester you've access only to the public website of Neptune Bank, and no access to the private network.

The project will be performed using Kali as attack machine and a virtual image that mirrors as much as possible the target network. You must download the image at the following link:

https://drive.google.com/open?id=1-M2JgY8mwzUepocD6OMTKdtzDjmnVPkn

Install it on your own machine. The installation guidelines are available here:

https://drive.google.com/open?id=1NxEZdzBeRqjJ0JQIBM60MD3d_c75o4Qi

The Neptune VLAN is in a .7zip archive file; the hashes for the archive as foillows:

MD5:

612b3fd7402f0caa6db626cc57cd0fa9

SHA1:

394bbf4a8f4c5534a479b4426badd3c7d7414b1b

Phase 1: Information gathering (7%)

1.1 Using network scanners, extract the topology information of the Neptune's private network. Identify available hosts, and for each host, find the IP address, Operating System, running services and open ports. Ensure that you specify the exact versions. (4%)

1.2 Identify vulnerable services; briefly explain why you think these services are vulnerable (by discussing a few samples) (3%).

Phase 2: Exploitation (18%)

2.1 Review the *network* scanning results and other information obtained in the previous phase, and exploit one or more of the vulnerable services to gain access to the private network. Justify the adopted strategy (6%).

2.2 After gaining access to the private network, perform the following security sensitive tasks (12%):
(i) Create an account for yourself and transfer to the account some fund from one of the existing customer accounts (4%).
(ii) Locate and exfiltrate the file containing the master secrets of the bank (4%). Recover the content of the corresponding file (4%).

Hints:

- The bank’s master secrets are the passcodes for various critical online accounts (e.g. federal reserve, trading, gold reserve) and offline accounts (e.g. bank vaults) that contain the bank’s assets.
- The master secrets file is encrypted, and protected by storing separately the encrypted file and the encryption key in two different users’ local accounts (i.e. network accounts).
- Neptune has a public website which can be accessed at http://<IP_address>:80
  The site runs on port 80, and the IP address of the server corresponds to one of the machines running a web server.
- The username format for both web and network accounts consists of the first character of the first name and the last name; e.g., for user John Doe, the username will be jdoe.
- Neptune’s Chief Technology Officer (CTO) has advised employees against using the same password for both network and web accounts, but it is unclear whether they really follow this recommendation.
- The CTO is a big fan of James Bond and believes that MD5 and Blowfish are great cryptosystems despite all the controversies about them.

- Many account passwords are dictionary words (characters/digits), but not all. You can start using the password dictionary available at: https://drive.google.com/open?id=1D9q8pdnyMRIKkfnASI3TcHGn9i7HLahp
  This can help with some of the key accounts, but not all. So additionally, you can generate your own dictionary or use some of the default dictionaries available in Kali or online.

Basic requirements for using the online banking service are as follows:

1. A user has to register first to create a new account.
2. Once the user is able to login, he/she has to provide the customer details.
3. Once the customer details are provided, he/she can request a new bank account (e.g. checking, savings, etc.). By default, the requested bank account will be in deactivated state until a manager (i.e. bank employee with at least branch manager privilege) approves the account. The user will not be able to do any transaction until the account is approved by a manager.
4. Once the account is approved, the user can perform payment transactions to/from the corresponding account; the user also can send money to added payees.

In practice, data on current bank staff and customers can be collected by gathering information through Google search, online forums, blogs, news releases, etc. Assume that some of the bank staff and customer names that were found through some previous search include the following:

- James Butt (Customer)
- Josephine Darakjy (Customer)
- Art Venere (Customer)
- Lenna Paprocki (Customer)
- Donette Foller (Customer)
- Simona Morasca (Customer)
- Mitsue Tollner (Customer)
- Leota Dilliard (Customer)
- Sage Wieser (Customer)
- Joe Bonano (Branch manager)
- Aashna Kunjus (Branch manager)
- Mehta Singh (Bank teller)
- Harry Lu (Bank teller)

Important Notes:

- Document your answer using screenshots of your scanning activities and explain the scanning methods you used. Report both your successful and failed attempts.

- It is assumed that the attacker does not have physical access to the target network. So all access should be performed (remotely) through the attack machine (i.e. Kali). Results obtained by analyzing directly the target machine are invalid, and will be assigned **zero**.
- The project must be done by groups of two. Any collaborative or plagiarism activities will be sanctioned (i.e. Groups are not allowed to collaborate).
- Your submissions need to be typeset and in pdf.
- Project reports should be submitted on or before the deadline by email at itraore@ece.uvic.ca

Part 2: Defense Strategies

In the second part of the project, you will use the attack intelligence obtained in part 1 to implement adequate defense strategy to prevent or detect similar attacks in the future. As part of the protection mechanisms, you'll setup snort IDS on the machine NeptuneR and IPTables on the machine NeptuneN.

Phase 1: Intrusion Detection (11%)

Identify and select one medium or high risk vulnerability (other than password cracking or unsupported OS version) against **NeptuneN**, for which you can identify an exploit code and execute successfully the exploit using Metasploit. The selected vulnerability can be derived from the earlier scans (nessus/nmap) or by searching online.

A straightforward solution to prevent attacks based on these vulnerabilities could simply be to install more recent versions of the services. But the goal here is to go beyond such obvious solution, as variations on the attack patterns may still be successful (even after installing the upgrades).

1. Explain briefly the generic attack scenario associated with the selected vulnerability (2 paragraphs maximum); a graphical sketch (in addition to the explanations) is required. Do not copy and paste paragraphs and figures from the Internet. You can search for such information online; but make sure that the explanation is reworded using your own terms, and the graph is your own (1.5%).
2. Execute the attack against machine NeptuneN by exploiting the selected vulnerability using Metasploit. Capture sample attack packets using wireshark (you can start wireshark, just before typing the "run" or "exploit" command in Metasploit; and stop it after the attack has completed) (1.5%).
3. Analyze the sample attack packets, and define new Snort rules (as many as you think are necessary) to detect the attack, and add the rules to the snort rule set. Justify the rationale for the rules. Make sure your Snort rules do not over-fit the attack scenarios. (5%).

4. Configure Snort (on the **NeptuneR** machine) and run it in intrusion detection mode. Execute the relevant exploit for the vulnerability using your attack machine (i.e. Kali) (1.5%).
5. Analyze the Snort alerts log generated after the attack, and discuss the results in terms of false positives and false negatives (in principle the snort configuration must successfully alerts on all suspicious packets, while not raising alerts on legitimate traffic) (1.5%).

Note: It matters that the exploit be relevant (you cannot pick one at random), and you must complete all the proper steps in Metasploit (initializing, launching, and completion). Provide screenshots documenting the different steps.

Phase 2: Intrusion Prevention (9%)

To protect against the above attacks, we would like to reinforce the IDS protection using IPTables firewall. The protection scope (in this phase) will be the **NeptuneN** machine, i.e., the IPTables rules will be deployed on **NeptuneN**. Since this part of the project focuses on protection, it is assumed that you'll have direct access to the internal network. This means you can update the firewall rules on the machine directly. The default root credentials for NeptuneN will be given after the deadline for Part 1.

Note that snort will run only in non-inline mode. That is, it does detection only, and does not actively prevent anything. We use IPTables for that.

1. Define the IPTables rules and provide rationale for each of the rules. You should minimize false negatives and false positives so that a legitimate client is allowed access, but a client that attempts the selected attacks is blocked. (5%).
2. Test the firewall rules by executing the attacks (in metasploit, when relevant exploit exists); provide screenshots documenting the results. (2%).
3. By reviewing the scan results (obtained in project – Part 1), suggest and describe any additional defense strategy to protect the target systems (2%).