Student’s Name:

Professor’s Name

Course Number

Date

**Project 2 & Project 3**

Modern companies are becoming complex day by day. This is due to technologies such as networking, cloud computing, storage devices, servers among other modern technologies. since no single person is able to handle all these things and also it is impossible to have complete knowledge, teams are formed to handle various tasks such as network configurations, network monitoring among others. While performing these tasks, the teams may leaves spaces for exploitation or vulnerabilities in the system. An attacker or pen tester can identify such vulnerabilities and perform attacks which may cause damage to the company. Due to this there is need for the company to involve an ethical hacker to test their system. Havenbrook Investment Group being such company has requested an ethical hacker who after a mutual agreement with the company tries to penetrate into the company system. The pen tester goes through the process of pen testing giving all tools required. Throughout this paper we will consider the process taken by the pen tester to try and break into the company’s system.

# Reconnaissance Plan

Reconnaissance phase is the first step in the penetration testing. The pen tester will be undertaking research about the organization and their site during this phase. This will begin by the attacker first visiting the organization’s website to learn about the structure of the organization and their hierarchy, phone contacts and other information which are made public in order to an attack plan. The pen tester will collect as much information about the Havenbrook Investment Group as possible such as domain names, network topology, their mail servers, their ip addresses among other to help in other phases of attack.

The attacker will make use of two important methods to collect information about the organization: Active and Passive. The Active reconnaissance is where the pen tester compromises the system to gain information. Passive reconnaissance is where the pen tester collects target information without having to actively compromise the system. The pen tester will use both of these methods and software for the pen testing on Havenbrook Investment Group. The following are the methods of reconnaissance. Passive reconnaissance: War Driving, Dumpster diving, WHOIS, SQLMAP, Nessus. Active reconnaissance: Port scanning. The given software and methods will be used for this pen test purpose to try and collect information about the network of Havenbrook Investment Group.

# Scanning Plan

This is where the pen tester will interact with the company with the aim of identifying the vulnerabilities and also to collect collects specific information about the given system target such as passwords, network resources, machine names, software being used in the system, user names among others services from the system. This will enable the pen tester to research further on the vulnerabilities within the network and come up with a more precise attack plan and how to exploit the system. The attacker will identify all vulnerable options in the logic, functions and libraries used in the systems of the organization. In case of the companies site, the pen tester will identify injections, remote executions of code and scripting of cross-sites in this phase. This will aid the attacker on the next stage by having identified all the vulnerabilities.

The pen tester will now start using the given software to start scanning for vulnerabilities and all available open ports on the network. The tools most commonly used tools which the pen tester will use are as described. War Driving: this is an access point mapping tool through which the pen tester looks for wireless access points by driving within the company’s building radius, WHOIS: this script/command is used to gather details about the employees such as user names, names, phone contacts, emails, their passwords, among other details within the company, SQLMAP: this is an open source software that allows the pen tester to detect and exploit any SQL injections in order to take control of the database, Dumpster diving: the pen tester goes through the company’s trash looking for any documents that might contain valuable information such as user names and passwords which can be used to gain access into the system, Nessus: this is also an open source software which can used by the pen tester to discover devices such as mobile devices and printers on the network and to also show information about their vulnerabilities to the pen tester who can use these details to exploit the devices, Port Scanning: this software will be used by the pen tester to scan for any open port in the target network which will the be used to exploit and enter into the network.

Based on employees activities, the pen tester can also make use of attack vectors such as email attachments since almost every communication in the company takes place via email. The pen tester can also use other attack vectors such as pop-ups on company’s website and system,text messages, instant messages and social engineering to gain more vulnerability and breach deep into the system network. Some of these are considered when it comes to situations where the company is using outdated software, outdated software to protects the system from malware attack and outdated anti-viruses. This makes the system difficult to detect attack vectors such as viruses and ransomware making it easy for the pen tester to penetrate into these systems. This may also be due to cases where the company is not educating their employees about looking out before clicking any link and installing any software.

An Intrusion detection system can be used to detect and block this type of reconnaissance by monitoring the company’s network for malicious activities and policy violation. They perform an analysis of the traffic passing on the entire network and tries to match with known attack traffic. If an attack is identified it is reported to the network administrator. Therefore the pen tester will have to be authorized to try and bypass the intrusion detection system configuration. The pen tester can also use other tools like metasploit to enumerate hosts and the network and also to evade intrusion detection systems while executing remote attacks. However, tools such as host intrusion detection systems will detect this activity and alert alert the administrator. The pen tester will have to avoid detection by choosing the right target to exploit. By considering the level of risk of being detected, the pen tester is able to identify the most vulnerable target by choosing the one whose risk and level of security is low and then later tries to advance to other targets whose security is more advanced. By also being able to identify the right target, the pen tester will be able to accomplish the specifically intended penetration test more easily than in a situation where the pen tester fails to identify the right target.

**Gaining Access Plan**

By using the described software and techniques, the pen tester will be able to collect information about employee login details, the operating systems on employees computers, devices connected to the computers among other information about the activities carried out by the employee using the computer. Having this information, the pen tester will now be in a position to plan on how to gain access into the organizations network.

Once the pen tester finds an access point which is least secured, he will on how plan to penetrate the system using that access point. From here the pen tester will be able to monitor various users location within the company structure. This will enable the attacker to choose the target user to exploit based on the ease of access, the active time and the level of access the user possesses. As described above, the attacker can start with victims with lower privileges as the security is not complex then elevate gradually without the risk of being detected.

In order to find an open port, the attacker will make use of the port scanning software. This will explore information such as: the services which are running, the type of user owning the services, whether some network services need authentication and other crucial details. There are various techniques which are used for port scanning. The commonly used being Nmap and Nessus which enables for automated port scanning. As it was described earlier, Nessus enables the pen tester to scan the target network and get information about which ports are open and which are not. The pen tester will make use of an Nmap which is available in Kali Linux to scan and map out the target network and get information about which devices are connected to which port and which among the available ports are open. This will require the pen tester to first install the Nmap into the computer. The pen tester can then run both ping scan and host scan to identify active hosts and send ARP request packets to all the active hosts connected to the company’s network. Then the host will respond with another packet containing their status and MAC addresses which is crucial to the pen tester. The pen tester will also use Nmap for OS scanning by sending UDP and TCP packets to identified ports then analyze the received response. He then compares the responses to 2600 database of operating systems to get information about the host operating system. Based on the type of operating system, the pen tester will be able to plan on the type of attack to conduct. Other tools such as wireshark can also be used for this process.

Upon finding an open port the pen tester will try to extract machine names, and user names, network resources, among other information and services to invade the network though a process called enumeration. The attacker will use the gathered information to identify any vulnerabilities and weak points in the security of the system and then try to exploit it. There are various ways in which the pen tester might enumerate the network of Havenbrook Investment Group. Firstly through extracting user names by using email ids. Second through extraction of information by use of the default passwords, this is where employees forgets to change their defaults passwords assigned to them which will greatly help the pen tester to enumerate their information easily. Thirdly we have extracting user names through the use of SNMP. The pen tester guesses a string and uses it to extract the required username. Lastly we have brute force on active directory. This is because the active directory is prone to username weakness enumeration during user input validation.

The pen tester will be using a tool called enum4linux for this process since it also gives other properties which are attached to enumeration. The pen tester can then view all user groups and password policies.