Penetration Test Proposal

Deliverable 4: Final Penetration Test Proposal

Name: Dmitry Landy

Course Number and Section: CMIT 321 6383

Instructor: Travis Trupp

Date: March 5, 2020

Rules of Engagement

Overview

Centralia Security Lab (CSL) will conduct an announced, grey-box penetration test for Haverbrook Investment Group L.L.L.P. (HIG) in order to discover, exploit, and report vulnerabilities in Haverbrook's network security. A penetration test is used to prepare an organization's defenses by simulating an intruder's attempt to access an organization's network systems (EC-Council, 2018, p.71). This Rules of Engagement (ROE) provides the schedule, scope, checklist and ethical consideration for the testing against HIG's network. The test will consist of five phases of hacking: recon, scanning, gaining access, maintaining access, covering tracks. These phases will require the employment of various tools and techniques, specified in the scope, to conduct an effective test.

The testing will be conducted from March 15, 2020 - March 21, 2020 in accordance with the following schedule:

- Time: 08:00 a.m. to 06:00 p.m EST
- Days: Monday - Friday

HIG employees are aware of the test and will follow the appropriate procedures for reporting any critical alarms for verification to prevent reporting false alarms to law enforcement. Any questions or concerns can be directed to the following:

Name: Dmitry Landy (Penetration Testing Team Lead)

Email: dmitrylandy@email.com

Phone: (301)-456-7890

Name: Jimmy J. John (HIG Network Administrator)

Email: jimmyjjohn@email.com

Phone: (301)-333-7351

Scope

The test described in the ROE will adhere to the limitations outlined in this section. As HIG is providing information about the network infrastructure ahead of time, the test will be categorized as a grey-box test. This test will be announced to HIG employees ahead of time in order to minimize false alarms reported to law enforcement.

The following are the devices and respective IP addresses of HIG's network that the tests will focus on (based on the network diagram provided by HIG):

- Network Server
- Router
- Switch
- Printer (10.4.12.20-31) (ports 1/1-11)

- Computers (10.x.x.x) (ports 2/1-11)
- Network Firewall

In addition to testing HIG's network devices, testing of physical security measures and social engineering will occur. Possible issues regarding ethics will be further detailed in the "Ethical Considerations" section of this ROE.

The test will be broken into five phases as detailed below. These phases will state the types of tools and techniques they will use during the testing period.

- Phase 1- Recon: This step involves passive reconnaissance, which is done by gathering publicly available information about the organization (EC-Council, p. 83). This information can be discovered by using search engines, organization websites, Shodan, WHOIS information of an organization's website, and Wireshark (Poston, n.d.).
- Phase 2- Scanning: This step involves active reconnaissance, which is done by probing the organization's network through port scanning and network enumeration (EC-Council, p. 84). This can be done by using tools such as Nmap, Metasploit, and Nessus (Poston, n.d.).
- Phase 3- Gaining Access: This step involves using the gathered information to penetrate the organization's security to access internally stored data (EC-Council, p. 86). This is done by exploiting vulnerabilities in order to take control of devices (Ryan, 2015).
- Phase 4- Maintaining access: This step focuses on the ability to persist within the network, gather more data, and extract data without being caught (Ryan, 2015). Escalating privileges will allow for more information to be gathered and maintain better control (EC-Council, p.88).
- Phase 5- Covering tracks: This step involves removing any trace of the intrusion (Ryan, 2015).

Tools:

- Angry IP Scanner
- Auditpol
- Cain & Abel
- Firebug
- Google
- HTTrack
- Metasploit Framework
- Nessus
- Nmap/Zenmap
- SET
- SMAC
- Shodan
- Wireshark

This test does not currently have any restriction set. However, if during the course of the test a restriction needs to be applied, the testing team lead should be contacted. These restrictions may be applied, but not limited, to devices, times of day, IP addresses, and personnel.

Checklist

This checklist is used to keep track of items to be tested and tasks to complete (EC-Council, p. 83-90):

- ❏ ITems:
  - ❏ Servers
  - ❏ Workstations
  - ❏ Printers
  - ❏ Routers
  - ❏ Firewalls
  - ❏ Intrusion Prevention Systems
  - ❏ Intrusion Detection Systems
  - ❏ Physical Security
- ❏ Tasks:
  - ❏ Analyze HIG's Job Postings
  - ❏ Discover Key Personnel
  - ❏ Identify the Network Layout
  - ❏ Identify Any Mobile Devices in the Network
  - ❏ Analyze and Profile HIG's Website
  - ❏ Gather Usernames and Passwords
  - ❏ Run vulnerability scans
  - ❏ Identify Critical Systems
  - ❏ Identify Critical System Applications, Active Services, Version information
  - ❏ Conduct Social Engineering Against Key Personnel
  - ❏ Gain Access to a Network Device
  - ❏ Escalate Privilege Within the Network
  - ❏ Install a Backdoor for Later Access
  - ❏ Sanitize Log files of Attack Traces

Ethical Considerations

Since the test conducted will employ tools and methods that actual criminals may use, ethical considerations will be observed to protect both key stakeholders and assets tested. The following are will be observed (EC-Council, p.25):

- The test will work within the approved limits established in the ROE.
- A Non-Disclosure Agreement will be signed to ensure that any sensitive information will not be used or discussed after the testing period.
- The testing will be done with intentions to expose vulnerabilities without causing irreparable damage (which can be done by working within the limits of the approved testing scope).
- Test findings will be reported HIG after the testing is complete.
- Unexpected critical issues that occur during the testing process will be reported and assessed before testing can continue.

Reconnaissance Plan

Overview

The reconnaissance phase is the first phase of the five stages of hacking (EC-Council, 2018). This phase focuses on footprinting. Footprinting is the process for collecting information about a target's network and the target itself (p. 103). The information collected will provide as a starting point for gaining access into the target network. Footprinting allows for the discovery of an organization's employee information and specific network specifications, such as IP addresses or network devices. There are two types of footprinting:

- Passive Footprinting - this process requires the gathering of information without interacting with the target network (p. 104). It involves searching for publicly available information, such as that found on search engines, the target's website, and social media.
- Active Footprinting - this process requires the gathering of information by interacting with the target network (p. 105). This involves actions such as querying for WHOIS information, using traceroute, and performing ping sweeps.

Reconnaissance Methods

The reconnaissance stage in a penetration test is best done when using the appropriate methods and techniques to get the best and most accurate information about the target. It can be broken down into the following stages (EC-Council, 2018, pp. 181 - 183):

1. **Authorization:** Before any test can be conducted, authorization must be given by the organization.
2. **Assessment Scope:** After the test has been authorized, the scope of the test must be established. This can be done by creating a Rules of Engagement (ROE) document. This allows all parties involved in the test to be fully aware of the test and its limits to avoid damage.
3. **Footprint Search Engines:** Search engines such as Google and Bing can reveal information about a target and its assets. The Google Hacking Database (GHDB) can provide techniques on getting more accurate search results about the target. This helps find "hidden" information that may be more difficult to find using standard search techniques.
4. **Footprint through Web Services:** Netcraft, Piple, and Google Alerts are all web services that can be used to gather additional information about a target's organization and infrastructure.
5. **Footprint through Social Networking sites:** Facebook, LinkedIn, and Twitter are all places that can contain public information about the target organization and its employees. This can greatly help in performing social engineering.
6. **Website Footprinting:** Tools such as HTTrack and Web Data Extractor can be used to replicate a target's website and gather detailed information about the organization's architecture.

7. **Email Footprinting:** Tools such as eMailTrackerPro and ContactMonkey can find a target's physical location which can be used to perform social engineering. Email headers can also provide technical information that can be used in mapping out an organization's architecture.
8. **Gather competitive intelligence:** Business Wire and Hoover's are tools that can get data about a competitor's business, such as location, product analysis, and marketing details.
9. **WHOIS Footprinting:** WHOIS lookups, through the command-line or tools such as SmartWhois, allow information about a domain to be gathered. This can include IP address, domain owner, contact information, and email addresses. This can be used to map the target's network as well as perform social engineering.
10. **DNS Footprinting:** Gathering DNS information using DNSstuff or dig can reveal DNS records that can be used for social engineering.
11. **Network Footprinting:** Tools such as Path Analyzer Pro and GEO spider can find a variety of information about a target, such as IP address ranges, DNS records, emails, and network availability (Vostrom, n.d.)
12. **Social Engineering:** This is done by directly or indirectly collecting information about a target by exploiting people through techniques such as shoulder surfing, impersonation, phishing, and persuasion. Depending on the victim's security awareness and training, this could reveal information about the network layout or provide usernames and password to gain access into the system.
13. **Document Findings:** The final step in footprinting is to ensure that the collected information is properly documented so that the process can be reported after the testing. This allows the client's organization to implement security measures to prevent exploitation.

Scanning Plan

Overview

Scanning is the second phase, and its objective is to find detailed information about a network and its devices so they may be exploited (EC-Council, 2018, pp. 187-188). The scanning phase provides the necessary information to gain access in the next phase. This requires a variety of tools and techniques in order to systematically gather the required information and fulfill the following objectives (p. 189):

- Discover live hosts, IP addresses, and vulnerable ports.
- Identify operating systems and architecture of the target's network to analyze for vulnerabilities.
- Discover active services to analyze for any vulnerabilities.
- Identify application versions of a service and its vulnerabilities.

To fulfill the objective, different types of scans can be done to reveal various information about a network (EC-Council, p. 188):

- Port Scanning – This lists open ports as well as their respective services.
- Network Scanning - This lists IP addresses of active network hosts so they can be attacked or analyzed for vulnerabilities.
- Vulnerability Scanning – This reveals weaknesses in a network by scanning for known vulnerabilities.

Tactics, Techniques, and Procedures

Scanning allows specific information about the target network and systems to be identified to that vulnerabilities can be discovered. The vulnerabilities discovered through scanning can lead to gaining access. This stage can be broken down into the following steps (EC-Council, 2018, pp. 263-264):

- **Host Discovery:** Before a network can be analyzed, active hosts should first be identified. These hosts will be able to provide information about the activity in the network and can be detected using ping sweep and network scanning tools such as Nmap, Hping3, and Angry IP Scanner. Ping sweeps, or ICMP sweeps, can identify the range of IP addresses, and live hosts in a network. ICMP ECHO requests are sent to a range of specified IP addresses and any reply will identify a live host. This will not work very well when a firewall is present.
- **Port Scanning:** This scans for open ports in order to discover which services are allowed into the network. Open ports are a vulnerability that can allow malware into the network. These scans can be done using tools such as Nmap, Hping3, Network Monitor and SuperScan.
- **Beyond IDS and firewall Scans:** Since scanning is intrusive to a network, it can be identified by intrusion detection systems (IDS) and firewalls. IDS/firewall evasion techniques should be used in order to prevent detection. Tools such as Tor, Proxy Switcher, and CyberGhost can be used to accomplish this as well. The following are some techniques (p.230):
    - Packet Fragmentation: Packets are broken into smaller fragments to make them more difficult to analyze by network perimeter devices.
    - Source Routing: The packet route is specified in order to reach the intended source by bypassing any route restrictions imposed by the firewall or IDS.
    - IP Address Decoy: Multiple packets are generated in order to prevent the true source IP address from being identified.
    - IP Address Spoofing: The source IP address is changed in order to mask the true source of the packets.
    - Proxy Server: Packets are sent through multiple proxy servers in order to make it more difficult to trace the packets to the original source and/or bypass IDS/firewall restrictions.
    - Anonymizers:This server is similar to a proxy server since it works as an intermediary between the source and destination (p. 245). It can remove information about the source system to make it difficult or even impossible to identify.
- **Banner Grabbing:** Manually crafted packets are sent to the target device in order to determine the target's OS by analyzing the response. The version of the OS can be

further analyzed for vulnerabilities to exploit to try and gain access into the network via the target system.

- **Draw Network Diagrams:** Scanning tools such as Network Topology Mapper can be used to create a network diagram of the target network. This diagram will include identified vulnerable hosts and their specifications.
- **Document Findings:** After the scanning is complete, the findings and methods, techniques, and tools used to get them must be properly documented. This allows the client's organization to implement security countermeasures to prevent exploitation.

Gaining Access Plan

Overview

The gaining access phase is the third phase of the five phases of hacking. It is the main goal of an attacker to gain access to the target system. The amount of success in this phase depends on the information gathered during the reconnaissance and scanning phases. Gaining access is done by reviewing the vulnerabilities discovered from the previous phases and exploiting those vulnerabilities (EC-Council, 2018, p.20). Some of the data gathered during the previous phases can include the following (pp.351-352):

- **Reconnaissance:** Employee information, a profile of the target organization, associated websites, domain names, and IP address range.
- **Scanning:** Open ports, active hosts, active services, and IP addresses.
- **Vulnerability Analysis:** Security procedures and controls of various systems, security loopholes, and security vulnerabilities.
- **Enumeration:** User lists, routing tables, SNMP data, and network layout.

Depending on the vulnerabilities (regarding the gathered information), the attacker can gain access at different levels of a system or network (operating system, application, network, etc.) (EC-Council, 2018,p. 20). A variety of techniques and tools should be used to effectively and efficiently gain access. Since this phase requires the attacker to gain unauthorized access into the systems, the attacker has to do so without being detected. The ability to stay undetected while gaining access depends on what information was gathered in the previous phases as well as tools and methods to clear tracks.

Vulnerable Resources

Gaining access to a system or network relies on present vulnerabilities and how they can be exploited. Vulnerability research is a necessary process of discovering the flaws and vulnerabilities of an operating system, its applications, and services (EC-Council, 2018, p. 312). New vulnerabilities are being discovered all the time as appliances change and systems are updated. These weaknesses allow an opening for attackers to exploit. Once the organization's systems and network layout are known, vulnerabilities relating to them should be researched. The following databases can be used:

- **NVD**: The National Vulnerability Database is a government repository containing standards for vulnerability management (NVD, n.d.). Security Content Automation Protocol (SCAP) is part of NVD to automate vulnerability management for systems. It performs analysis on Common Vulnerabilities and Exposures in order to create associated metrics such as Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE), and Common Platform Enumeration (CPE). The NVD database can be used to query for known vulnerabilities of identified systems to assist in gaining access.
- **CVE**: Common Vulnerabilities and Exposures is a dictionary of entries that contain an identifier, a description, and reference of the vulnerability or exposure (CVE, n.d.). This is a credible source to gain specific information on a vulnerability. The references included would be able to provide additional information to better understand the vulnerability.
- **VND:** CERT/CC Vulnerability Notes Database is a database by the CERT division of Carnegie Mellon University which contains software vulnerabilities that provide summaries, details, remediation information, and affected vendors of that specific vulnerability (CERT, n.d.). It also includes references to the vulnerability as well as CVE IDs.

There are many other vulnerability databases that can be used for vulnerability research. These databases should be thoroughly explored to see which offer the most useful information. Regardless of the database, they should certainly be used to identify system vulnerabilities so that they can be effectively exploited. This would greatly assist in gaining access to a system.

Techniques and Software

Gaining access to a system or network requires considerable preparation and a smart approach. After the information from the previous phases has been analyzed for vulnerabilities, there are various methods or techniques that can be used to increase the likelihood of success. These techniques are based on the CEH Hacking Methodology (CHM) which has 3 steps: gaining access, maintaining access, and clearing logs (EC-Council, 2018, p.352). This section will discuss the first step of CHM.

The best way to gain access to a system is to have the credentials to accounts (preferably administrator accounts). However, passwords can be rather difficult to acquire depending on the organization's security policy and the system. Password cracking is a process of recovering a password (or other supplementary credentials) during transmission or extracting them from storage (p. 354). This can be done using the following types of attacks:

- **Non-electronic**- Does not require technical knowledge or tools, but instead focuses on social engineering, dumpster diving, and shoulder surfing:
    - Social Engineering: This technique focuses on exploiting human behavior in order to extract certain types of information or obtain access to a system (p. 356). This is a way to bypass security measures by having someone with access perform various acts to grant access to the attacker.
    - Dumpster Diving: Since organizations throw many documents in the trash, there is a chance that some of them include credentials that someone didn't bother to

shred. Dumpster diving is a process of gathering discarded trash in order to analyze it for pertinent information for gaining access (p. 355).
    - Shoulder Surfing: This technique is simply looking over a person's shoulder in order to see what the user inputs into a system, such as usernames, passwords, and PINs (p. 356). This requires a certain degree of physical access to accomplish.
- **Active Online** - Actively using tools to conduct dictionary attacks, brute-force attacks, rule-based attacks, password guessing (including the use of databases to input default passwords), and LLMNR/NBT-NS poisoning (pp. 356-363). Some of the tools that can be used for this are John the Ripper, Brutus, RainbowCrack, Cain and Abel, THC Hydra, OphCrack, and Aircrack-NG (Shankdhar, 2018).
- **Passive Online**- Using tools to passively collect information to discover credentials by wire sniffing and MITM attacks (p. 365). Wireshark is a good tool for this type of attack.
- **Offline** - Analyzing how passwords are stored in order to determine the password (p. 366). This can be accomplished by using rainbow table attacks and distributed network attacks. RainbowCrack and password recovery tools are possible tools to accomplish these attacks.

Maintaining Access Plan

Overview

The fourth phase of the hacking is maintaining access. As the name implies, this phase focuses on maintaining access to the system and network while avoiding detection (EC-Council, 2018, p. 352). Since it is likely that access was gained through a low-level account, this phase will work to escalate the privilege to be able to perform a larger variety of tasks such as executing applications (p. 353). Once the appropriate level of privilege is acquired, the attacker can begin executing applications. These applications can be used to exploit vulnerabilities in code, steal personal information, monitor systems, and install backdoors for easy access into the system (p. 390). The last step of this phase is to ensure the executed applications are persistent and are able to avoid anti-malware or anti-spyware applications (p. 418).

Techniques and Software

To properly maintain access in a system, various tools and techniques should be used. Improper or lack of use of these tools and techniques can result in detection and loss of access to the network or system. The following are the three main areas of maintaining access:

- **Escalating Privileges:** Different privileges limit users in functionality and access to data (EC-Council, 2018, p.383). Privilege escalation can occur by taking advantage of identified systems and their known vulnerabilities (discussed in phase 3: gaining access). This is an important process of this phase as it allows the attacker to gain different or additional privileges depending on the type of privilege escalation. There are two types of privilege escalation:
    - Horizontal Escalation: This type of escalation seeks to get different privileges and access as opposed to more (p. 383). For example, if the current account has

access to the accounting department resources, but the desired data is with the HR department, then horizontal escalation would be appropriate.
    - Vertical Escalation: This type of escalation seeks to get increased privileges and allow access to more data. For example, the current account is part of the accounting department, but the attacker needs access to all of the departments of the branch. Vertical escalation would allow the attacker to gain perhaps the administrator account to satisfy this need.

  Some ways to accomplish this are through DLL hijacking, vulnerability exploitation, CPU vulnerabilities, access token manipulation, and application shimming (pp. 384-388).

- **Executing Applications:** Once the desired access has been acquired, the attacker can execute malicious code in order to steal information, gain additional access, acquire passwords, install a backdoor, install spyware to "own the system" (p. 390). This establishes persistence in case access is lost or changed. The tools used here can be pre-made or created manually using various programming languages (C, C++, Java, Python, etc.). Some available tools are RemoteExec, KeyGrabber, SpyTeck SpyAgent, and PowerSpy (pp. 391-409).
- **Hiding Files:** To ensure persistence in the system, the attacker can use a variety of techniques to hide their files and programs from detection and removal (p. 418). Rootkits can be installed in order to gain access without detection. Using escalated privileges, the attacker can ensure that the rootkit is well hidden. There are different types of rootkits that are installed in various parts of a system (operating system, kernel, hypervisor, etc.)(p. 419). Horse Pill, GreyFish, and Sirefef are some rootkits that may be used.

Covering Your Tracks Plan

Overview

The final phase of hacking is covering tracks. This is a critical step for ensuring that the actions and intrusions taken in the previous steps cannot be traced back to the attacker (Arora, 2019). This phase requires the attacker to identify appropriate log files that tracked their actions and remove the suspicious activity (EC-Council, 2018, p. 457). Additionally, auditing should be disabled, BASH shell tracks should be cleared, tracks on the network should be erased, and any remote connections should be closed (p. 472). If done properly, the attacker's actions and the attacker themselves should not be able to be identified.

Techniques and Software

Covering tracks is an important phase of hacking that requires an understanding of log files and some system configurations. The ideal purpose is to leave the network how it was found before the intrusion (EC-Council, 2018, p. 457). Some files can only be manipulated with the appropriate privileges, which should have been gained in the fourth phase (maintaining access). Proper use of tools and conducting the appropriate techniques will allow this to happen. The following are the techniques that can be used:

- **Disable Auditing:** Auditing capabilities for the targeted systems should be identified early on to ensure that the attacker's actions will not alert or notify system administrators and cause the access to be restricted (p. 458). Audipol is a command-line tool that can manipulate audit policies set for a system. However, this requires the attacker to gain administrative privileges before disabling auditing.
- **Clearing Logs:** Since various intrusive actions occurred and malware was run during the other phases, even logs would have captured those actions. This can be done manually by the attacker or through the use of tools. To do this manually, the attacker would have to go to the event viewer in Windows or /var/logs directory in Linux to clear the logs (p. 462). This does require a decent knowledge of log files to accomplish properly. Tools can be downloaded to do this as well. The Clear_Event_Viewer_Logs.bat utility can be used in the command prompt to remove the log files in Windows (p. 459). Meterpreter shell of the Metasploit Framework could also be used to clear logs by using the "clearev" command (p. 461).
- **Clearing Online Tracks:** Since the first phase is done through the use of web browsers, it is important to remove the tracks left behind on them. This involves removing the history, clearing the cache, deleting downloads, clearing stored password data, removing private data, and clearing cookies (p. 462). CCleaner is a tool that can conduct the activities discussed for clearing online tracks based on the parameters and actions the user specifies (p. 467). It will do these actions for a variety of web browsers.
- **Covering BASH Tracks:** If the BASH shell was used in a Linux environment, it is important to not forget to remove suspicious activity in the command history file (p. 463). This can be simply done by using the "history -c" command. The "shred ~/.bash_history" command could also be used to make the file unreadable. However, this does cause suspicion to arise as to why that file is unreadable.

References

Arora, S. (2019). The Five Phases of Ethical Hacking. Retrieved from https://www.simplilearn.com/phases-of-ethical-hacking-article

CERT. (n.d.). Vulnerability Notes Database. Retrieved from https://www.kb.cert.org/vuls/

CVE. (n.d.). About CVE. Retrieved from https://cve.mitre.org/about/index.html

EC-Council. (2018). Certified Ethical Hacker (CEH) Version 10 eBook. [eVantage]. Retrieved from https://evantage.gilmoreglobal.com/#/books/9781635671919/

NVD. (n.d.). General Information. Retrieved from https://nvd.nist.gov/general

Poston, H. (n.d.). Top 10 Network Recon Tools. Retrieved from https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/network-recon/#gref

Ryan. (2015). Summarizing The Five Phases of Penetration Testing. Retrieved from https://www.cybrary.it/2015/05/summarizing-the-five-phases-of-penetration-testing/

Shankdhar, P. (2018). 10 Most Popular Password Cracking Tools. Retrieved from https://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref

Vostrom. (n.d.). Path Analyzer Pro. Retrieved from https://www.pathanalyzer.com/