Footprinting and Reconnaissance Tools

Topic 1: Common Port Scanning Techniques

Do some research on computer ports that are most often scanned by hackers. Identify a port scanning exploit that is interesting to you and share it with the class. If you have experienced or witnessed port scanning activity on a computer network, consider including this in your response as well.

Edward Jackson

Check the Firewall

According to DOC-1068, from the Qualys Community, some common ports are 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445 and UDP Ports 53, 111, 135, 137, 161, 500” (Qualyx Community, 2015, para. 2). These ports represent specific services, that when a hacker scans them, they will know which services and applications are running. Port scanning can also allow attackers to assess other things as well, such as whether or not a firewall has been configured, detect operating systems, and tests for other potential vulnerabilities---vulnerabilities which hackers can exploit. Note, while the ports listed are the some of the popular ones, the activity of port scanning involves ports all the way up to 65,535. The port I chose is 53. Port 53 is the Domain Resolution Port (DNS). This means, that this port is usually required, and thus (over many years) has been the target of many exploits (I found many exploits targeting port 53). The specific exploit I chose to research further is how a hacker can bypass a firewall using port 53. For example, in the Kerio Personal Firewall (KPF) software, there is a default exception rule which opens up a path using the DNS port (Speed Guide, n.d.) By allowing port 53 traffic, attackers can go around the firewall’s defense, thus permitting a hacker to obtain more information about the target machine. Using that “extra” information, hackers can gain even more access to the machine (known as escalation), eventually taking over the machine altogether. This is all because DNS is normally required, and hackers have found ways to exploit that network necessity.

For some real world experiences, the company I work for denies most ports (by default), and then opens up specific ports based upon company need. We have two highly sensitive ports which are always monitored, they are the ports for FTP and RDP. Both of these ports could be used internally and externally to steal information, thus, pretty much all usage is monitored. When it comes to dealing with port scanning, we have software in place to determine whether someone is running a scan on our network. Honestly, our company has pretty tight security in general. We have Websense, ACLs on firewalls and routers, scanning/monitoring software, auditing enabled, and people who monitor port usage. Additionally, we have data loss prevention
software (to keep information from being copied to USB drives), email scanning software, AV, and a long list of security-related software. For physical security, everything is locked down via security cables, we have video surveillance everywhere, and security officers that patrol the site. I never really thought about it until now, but this place is like Fort Knox. When I worked in healthcare, the security was much more laid back, even though it shouldn't have been.

But, back to the original exploit I mentioned. It is worth noting, that no matter what security software and hardware you use, you really should understand what the default settings are, and whether are not they pose a security threat. In the Kerio Firewall software, a little research would have revealed the weakness in security.

References


**Topic 2: Popular Reconnaissance Tools**

Do some research and identify two popular reconnaissance tools. Compare and contrast your chosen reconnaissance tools and explain the benefits and limitations of each.

Edward Jackson


**Special Forces: Recon**

According to Oriyano (2014), reconnaissance (also known as footprinting) is the process of gathering information (usually remotely) from a computer network (Oriyano, 2014, p. 198). Black hats can use this information to find weaknesses and vulnerabilities in networks, and then exploit them. Ethical hackers can use reconnaissance tools to find computer network weaknesses, and then patch machines, harden security, and add extra layers of defense. For ethical hackers, footprinting a network also provides solid security data and reporting to present to management. This could be particularly useful when budgeting for security-related hardware and software. When it comes to two specific recon tools, I have selected Nmap and Netdiscover.
Nmap and Netdiscover can both be used to find vulnerabilities in target machines. They can both return mapped ports, IP addresses, and other TCP/IP session information. Both utilities have been around for many years, and have a lot of online support, which in theory, a black hat could use for nefarious reasons. Some major differences between the two utilities is that Netdiscover is meant more for wireless networks, to be used without DHCP servers, and was created for Linux/Unix operating systems (Peñalba, 2009). In contrast, nmap can be used on wired and wireless networks, with and without DHCP servers, and has been ported to many operating systems (Freeman, 2012). Something else, which is pretty significant, nmap is the swiss army tool of recon tools, meaning, nmap is small, easy to use, and extremely powerful. Netdiscover is great for what it is meant for. For example, Netdiscover scan and capture arp req/rep packets from multiple hosts. These packets are supposed to footprint wireless access points and connected hosts, thus allowing a hacker to obtain information that could be used to penetrate network defenses. I did download Netdiscover and run it on one of my Linux boxes. It returned a list IP addresses and MAC addresses; that was pretty interesting. Of course, in comparison, nmap is just so much better, and can return much information. For instance, running nmap can return services, ports, hosts, firewall/IDS information, and reverse IP addresses (and much more). The only issue with both of this tools is that they did not have graphic interfaces, and both required knowing which switches to use. Additionally, both tools were missing automatic/automated assessment, meaning, a person still has to comb through the data to determine weaknesses. This could become cumbersome to an ethical hacker who is performing regular scans and presenting reports to management.

I could see how using these tools against an improperly secured network could be bad for business. A criminal hacker could map out a company’s network, return host names, IP addresses, and MAC addresses, and then find weaknesses. Once weaknesses have been discovered (for example, unpatched workstations), a black hat could exploit those weaknesses. They could possibly remotely access the systems, perform a denial-of-service attack, or just send in a Trojan horse to spy on the user or steal data. This is one reason why I support the ethical hacking endeavor, and believe companies need to employ ethical hackers to manage and test security. At the very least, there should be one person in the company who understands things like reconnaissance, port scanning/mapping, and penetration testing.

References


Footprinting
The process of ethical hacking begins with Footprinting. Footprinting describes a process in which the hacker attempts to acquire important information about the target. This form of information gathering implies that the hacker does not take any actions that might expose the hacker or the target. As such, this unit will introduce you to the processes, tools, and techniques that are used to successfully complete the Footprinting phase.

Once the process of Footprinting is completed, the hacker will typically begin the process of port scanning. Port scanning is critical because it confirms what services are present and what services are not present. Port scanning is also critical because it is the first active process performed by the hacker, so it is often the first opportunity to detect a hacking attempt. The results of the port scanning process will then be used to plan out the rest of the hacking activities.

You should recognize that Social Engineering is a pervasive and continuous risk at every stage of hacking, and as such, it is something for which ethical hackers must test repeatedly. Black hat hackers will use Social Engineering when Footprinting, so ethical hackers should also be conscientious of risks in this area when conducting Footprinting activities.

Outcomes

After completing this unit you should be able to:

- Describe components and controls used to establish physical security.
- Outline the steps of the information gathering process.
- Explain the purpose of Footprinting.
- Explain common port scanning techniques.

Course outcomes practiced in this unit:

IT542-1: Perform vulnerability tests using computer and network tools and utilities.

What do you have to do in this unit?

- Complete assigned Reading.
- Participate in Discussion.
- Complete unit Assignment.
- Participate in Seminar or Alternative Assignment.
- Complete the unit Quiz.
Complete the optional Learning Activity.

Read the following chapters in your textbook:

Chapter 4: “Physical Security”

Chapter 5: “Footprinting Tools and Techniques”

Chapter 6: “Port Scanning”

These chapters begin by introducing you to physical security and its significance to an overall security plan. The chapters also discuss how hackers exploit weaknesses in physical security to gain access to a network. Computing professionals often overlook physical security, so take care to carefully read this material. Next, the processes associated with ethical hacking are introduced, beginning with passively gathering as much information about a target organization as possible without taking any active steps that might expose intrusion attempts. This process is always the first step and is known as Footprinting. Once the process of Footprinting is completed, the next step is to begin identifying the computers and services within the organization. The Readings conclude with an explanation of port scanning and how to use port scanning to identify computers and services within the organization being tested (or hacked).
**Biometrics:** A mechanism that authenticates an individual through the use of physical traits such as fingerprints, facial recognition, voiceprints, or other distinguishing characteristics.

**False acceptance rate (FAR):** A metric used to describe the probability that a biometric system will incorrectly accept an unauthorized user.

**False rejection rate (FRR):** A metric used to describe the probability that a biometric system will incorrectly reject an authorized user.

**Footprinting:** The process of gathering information about a target site (its computer systems and employees) by passive means without the organization's knowledge.

**Nslookup:** An application that allows a user to enter a host name and find the corresponding IP address.

**Traceroute:** A software tool used to trace the route taken by data packets.

**Whois:** A software tool used to identify the IP address and owner of a specific domain.

**Active fingerprinting:** A form of OS fingerprinting that involves actively requesting information from the target system. This means getting the information faster, but also at greater risk of exposure than is the case in passive fingerprinting.
Attending live Seminars is important to your academic success, and attendance is highly recommended. The Seminar allows you to review the important concepts presented in each unit, discuss work issues in your lives that pertain to these concepts, ask your instructor questions, and allow you to come together in real time with your fellow classmates. You must either attend the live Seminar or you must complete the Seminar alternative assignment in order to earn points for this part of the class.

**Option 1: Attend the Seminar:**

During the Seminar, the instructor will review the second lab, discuss the tools used, and lead a discussion on how to interpret the findings from the Footprinting activities.

**Option 2: Alternative Assignment:**

You will benefit most from attending the graded Seminar as an active participant. However, if you are unable to attend you have the opportunity to make up the points by completing the alternative assignment.

The alternative assignment consists of reviewing the recording from the live Seminar and then submitting a paper of at least three double-spaced pages in length that presents an overview of the topics covered during the Seminar. The paper must include at least one citation to research paper relating to one of the topics from the Seminar. Your paper should be in APA format and cite all references used. Submit to the Seminar Dropbox.

**Assignment 2**
Outcomes addressed in this activity:

Unit Outcomes:
- Describe components and controls used to establish physical security.
- Outline the steps of the information gathering process.
- Explain the purpose of Footprinting.
- Explain common port scanning techniques.

Course Outcomes:

IT542-1: Perform vulnerability tests using computer and network tools and utilities.
Assignment 2

Outcomes addressed in this activity:

Unit Outcomes:

• Describe components and controls used to establish physical security.
• Outline the steps of the information gathering process.
• Explain the purpose of Footprinting.
• Explain common port scanning techniques.

Course Outcomes:

IT542-1: Perform vulnerability tests using computer and network tools and utilities.

Assignment Instructions:

This Assignment provides the "hands on" element to your studies. It gives you the opportunity to gain practical experience using the tools and techniques associated with ethical hacking. Read and perform the lab entitled "Lab #3: Data Gathering and Footprinting on a Targeted Website" found in Doc Sharing. Complete all four parts of Lab #3. Compile your lab report in a Word document with a title page, labeling all screenshots you are required to capture, and including explanatory text where needed or required by the lab. Within your Word document, after your lab report, answer the Assessment Worksheet questions listed at the end of the lab. Conduct research and cite supporting sources in APA format where appropriate.

Directions for Submitting Your Assignment:

Save your Word document containing your lab report and Assessment questions using the following file name format: Username-IT542-Assignment -Unit#.docx (Example: TAllen- IT542 Assignment-Unit2.docx). Submit your file to the Unit 2 Assignment Dropbox by the end of Unit 2.

Assignment Requirements:

All lab steps are completed, including screenshots and explanations where required. Assessment question answers contain sufficient information to adequately address the questions. The lab report and the answers are accurate and complete, as well as free from grammar and spelling errors.

For more information and an example of APA formatting, see the resources in Doc sharing or visit the KU Writing Center from the KU Homepage.

Also review the KU Policy on Plagiarism. This policy will be strictly enforced on all applicable Assignments and Discussion posts. If you have any questions, please contact your professor.

Review the grading rubric below before beginning this activity.
## Assignment Grading Rubric = 90 points

<table>
<thead>
<tr>
<th>Assignment Requirements</th>
<th>Points Possible</th>
<th>Points Earned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab report contains data gathering and footprinting for three targeted domains.</td>
<td>0–15</td>
<td></td>
</tr>
<tr>
<td>Public domain information has been gathered for the targeted organization and its website.</td>
<td>0–15</td>
<td></td>
</tr>
<tr>
<td>Lab report includes discussion of what information is in the public domain, including information that should not be, if any.</td>
<td>0–15</td>
<td></td>
</tr>
<tr>
<td>Lab report includes a summary of research findings and how a hacker might exploit information discovered during the lab.</td>
<td>0–15</td>
<td></td>
</tr>
<tr>
<td>Assessment worksheet is completed, with responses that are accurate, complete and well written (3 points per question).</td>
<td>0–30</td>
<td></td>
</tr>
<tr>
<td>Assignment Total (Sum of all points)</td>
<td>0–90</td>
<td></td>
</tr>
<tr>
<td>Less deduction taken for spelling, grammar, and APA errors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New total after deductions</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>