This project is a security assessment of a small group of systems. In this assessment, students will apply security tools and resources learned in labs to a set of unknown systems. They will synthesize the output of security tools and the results of research into a report evaluating the security of each unknown system.

This document is divided into the following sections: scope of the assessment (which resources are to be assessed), the rules of engagement (specification of what actions are permitted during the assessment), resources required (security tools), references (information sources), procedure, and report format and submission details.

1 Scope of Assessment

The assessment is limited to the following IP addresses.

- 10.2.3.220
- 10.2.3.221

2 Rules of Engagement

Students may use any security tools to perform a security evaluation of the systems listed in the Scope of Assessment. These tools should include but are not limited to those listed in the Resources Required. Security tools can be used to identify potential vulnerabilities and verify these potential vulnerabilities through the use of exploits. However, no tools that are designed to crash a system or otherwise create a denial of service attack may be used.

Students may not port scan, vulnerability scan, or attempt to exploit any IP addresses outside those listed in the Scope of Assessment. In general, no security tool may be deployed against any IP addresses outside of the ones listed. Of course, students may contact other servers to search the web and perform research, such as by using the references below.
3 Resources Required

Students will need the following data and tools to create and test the software:

- Kali VM
- nmap port scanner
- OpenVAS vulnerability scanner
- Metasploit

4 References

Students will find the following references useful in performing the assessment and writing the assessment report.

- CVE Details, http://www.cvedetails.com/, provides information about reported vulnerabilities and can be searched by vendor, service, and vulnerability.
- Nmap Documentation, http://nmap.org/docs.html, will help to find scan options and show how to best understand nmap output.

5 Procedure

5.1 Network Scanning and Enumeration

Scan each IP address listed in the Scope with nmap. Scans should verify that the systems are up before proceeding, then identify the operating systems of each system, and finally identify both the names and versions of the running
services on each system. Students will need to scan all TCP and UDP ports as well as obtain all of the detailed data that nmap can offer by using the -A option.

5.2 Vulnerability Research

First, lookup the operating system type and version that were reported by network scanning tools on CVE details. Next, lookup any services, such as IIS or Apache, whose names were identified in the previous step. Use service versions to determine which vulnerabilities apply to the system under assessment. Compare these lists of vulnerabilities with the ones found in the next step: vulnerability scanning.

5.3 Vulnerability Scanning

We configured and used the OpenVAS vulnerability scanner in lab. Students may need to restart the three server daemons as we did at the end of the OpenVAS setup process, but no other setup should be necessary. Create scan configurations for each of the targets. Be sure that you can ping a target before beginning an OpenVAS scan. If an OpenVAS scan reports zero vulnerabilities, then there was an error during the scan or the target was not up.

5.4 Vulnerability Validation

With the exception of denial of service vulnerabilities, all reported vulnerabilities with a severity of high or medium must be validated. Severity levels are the level reported by OpenVAS or the CVSS score shown on CVE details.

Students should first search Metasploit to find exploits for validation. Search terms should include vulnerability identifiers like CVE numbers, service names like Apache or IIS, service versions, and text from the OpenVAS or CVE Details vulnerability description. If an exploit is successful against a system, then the reported vulnerability has been validated.

If an exploit cannot be found in Metasploit, research the vulnerability in
vulnerability databases, such as CVE Details. Use the vulnerability database to verify that the reported vulnerability affects the platform, service, and versions that the assessed system is running. If the vulnerability does affect the system according to the database, then the reported vulnerability has been validated.

6 Resolving Problems

While students are not permitted to use tools that are designed to crash systems, it is possible for exploitation of vulnerabilities to crash target VMs. If a target VM is not responding for more than 5 minutes, notify the instructor about the problem.

7 Report

The report will need to be at least 5 pages single spaced using a 12-point font. The report must be divided into six sections: the summary, procedure, one section for each assessed system, conclusion, and references. Sections must be identified by a heading in boldface in the same manner that sections in this document are formatted. References should include the references mentioned in this document that were used, along with any additional references found via the Sites page on the class web site or through other sources.

The report must begin with a summary of findings of the security assessment. For each system, describe its operating systems and services, speculate on what purposes it may serve in an organization, and describe how vulnerable it is to attack. The level of vulnerability depends not only on the number of vulnerabilities found, but also on the number of validated vulnerabilities and on the severity of each the vulnerabilities found. The summary must include a table of the following form, summarizing the findings at a high level:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Operating System</th>
<th>Number of Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.3.220</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.2.3.221</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The procedure section of the report describes the precise procedure followed based on the Procedure above. Do not include setup of OpenVAS or Metasploit, but do include the setup of any additional tools used. Describe the order of steps and include the full command lines used with all arguments, except for Metasploit. Details of Metasploit commands will be included in the following sections.

Each of the following sections will describe one of the systems assessed. These sections must have names of the form Assessment of IPADDRESS, where IPADDRESS is replaced by the IP address of the system whose assessment is described in that section. Each section should include an overall assessment of the security of the system, which will expand on the summary above. Following the summary, include a graph from CVE details showing vulnerabilities in the operating system type and version. Then create a table of the open ports, describing the services running on them, including their versions and vulnerabilities (if any). This table should summarize the results found via port scanning, vulnerability scanning, and vulnerability validation.

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Service</th>
<th>Version</th>
<th>Reported Vulnerabilities</th>
<th>Validated Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>ftp</td>
<td>vsftp 1.3.2</td>
<td>CVE-2006-1418, BID-1215</td>
<td>CVE-2006-1418</td>
</tr>
<tr>
<td>22/tcp</td>
<td>ssh</td>
<td>openSSH 3.9</td>
<td>CVE-2005-2798, CVE-2006-5051, BID-1397</td>
<td>None</td>
</tr>
<tr>
<td>53/udp</td>
<td>dns</td>
<td>bind 4.1</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Organize each section by service name, or port number if you were unable to identify the service running on the port. Under the service list the vulnerability details, including an identifier for the vulnerability, a one-line description, a detailed description, the results of validation, and how it was validated, in the format shown below. The best vulnerability identifier is a CVE number, but not all vulnerabilities will have those, and so another type of identifier, such as a BID or NVT number should be used.
CVE-2008-1414: One-line description

Detailed Description: Paragraph long description

Validation:

msf> search DCE
msf> use auxiliary/scanner/smb/smb_enumusers_domain
msf auxiliary(smb_enumusers_domain) > show options
msf auxiliary(smb_enumusers_domain) > set RHOSTS 10.2.3.220
msf auxiliary(smb_enumusers_domain) > exploit

Results of validation:
UUID 6bffd098-a112-3610-9833-46c3f87e345a 1.0 ERROR 0xc0000022
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

For vulnerabilities with no exploits in Metasploit, the validation section would indicate whether validation was successful or not, along with links to specific vulnerability reports and/or exploits that show that this particular service at the specified version was or was not vulnerable. For example:


The penultimate section should summarize the findings of the assessment, repeating the information from the first section, and provide a short description of how to mitigate the discovered vulnerabilities through patching, upgrades, service changes (i.e., use ssh instead of telnet), or deployment of security devices like firewalls. Be specific about mitigations: include the version or service pack name to upgrade to, which vulnerabilities it would fix, specify which ports to block on a firewall to fix specified vulnerabilities, etc. The final section should list references used.
8 Submission

The report must be turned in as a printed report at the beginning of the last class period, and it must also be sent as an attachment in Open Document Format (ODF) format named cit380-project-report.odt in an e-mail to the instructor with the following subject CIT 380 Project Report. The e-mail report is due at the same time as the printed report.

The printed report must be turned in on the last day of class, April 30.