Laboratory #5

Lab 5: How to Identify Risks, Threats & Vulnerabilities in an IT Infrastructure Using ZeNmap GUI (Nmap) & Nessus® Reports

Learning Objectives and Outcomes

Upon completing this lab, students will be able to:

- Review a ZeNmap GUI (Nmap) network discovery and port scanning report and a Nessus® software vulnerability report from a risk management perspective
- Identify hosts, operating systems, services, applications, and open ports on devices from the ZeNmap GUI (Nmap) scan report from a risk management perspective
- Identify critical, major, and minor software vulnerabilities from the Nessus® vulnerability assessment scan report
- Assess the exploit potential of the identified software vulnerabilities by conducting a high-level risk impact by visiting the Common Vulnerabilities & Exposures (CVE) online listing of software vulnerabilities at http://cve.mitre.org/
- Craft an executive summary prioritizing the identified critical and major threats and vulnerabilities and their risk impact on the IT organization

Required Setup and Tools

This is a paper-based lab and does not require the use of a "mock" IT infrastructure or virtualized server farm.

The standard Instructor and Student VM workstation with Microsoft Office 2007 or higher is required for this lab. Students will need access to the Internet to correlate found software vulnerabilities on the IT infrastructure with the Common Vulnerabilities and Exposures (CVE) online listing located at: http://cve.mitre.org/.

In addition, Microsoft Word is a required tool for the student to craft an executive summary for management summarizing the findings from the ZeNmap GUI (Nmap) and Nessus® vulnerability assessment scan reports and for completing the lab assessment questions and answers.

Recommended Procedures

Lab #5 – Student Steps:

Student steps needed to perform Lab #5 – Identify Threats & Vulnerabilities in an IT Infrastructure Using ZeNmap GUI (Nmap) & Nessus Reports:

1. Connect your removable hard drive or USB hard drive to a classroom workstation.
2. Boot up your classroom workstation and DHCP for an IP host address.
3. Login to your classroom workstation and enable Microsoft Word.
4. Review Figure 1 – Seven Domains of a Typical IT Infrastructure.
5. Load your workstation's browser and go to: http://cve.mitre.org/ .
6. Familiarize yourself with the CVE listing and search engine tool.
   - Load sample search criteria: "Microsoft XP 2003 Service Pack 1", "Cisco ASA 5505 Security +", etc.
7. Review the ZeNmap GUI (Nmap) network discovery and vulnerability assessment scan report and identify the following:
   - What was the date and time stamp of the Nmap host scan?
   - How many total tests or scripts ran during the scan?
   - A SYN stealth scan discovers all open ports on the targeted host. How many ports are open on the targeted host?
   - What ports are open on the targeted host?
   - What services/applications are on the targeted host?
   - What is the MAC layer address of the targeted host?
   - What OS is loaded on the targeted host?
   - How many router hops away is the targeted host?
   - Does the ZeNmap GUI (Nmap) scan report provide any information regarding to risk, threats, or vulnerabilities found?
   - What must you do to confirm or verify if the identified OS, software, application has the latest release and/or software updates and patches?
8. Review the Nessus vulnerability assessment scan report and identify the following:
   - What was the date and time stamp of the Nessus host scan?
   - How many total vulnerabilities were found per host?
   - Of these vulnerabilities, how many were open ports, high, medium, or low criticality vulnerabilities?

- What specific information was obtained regarding the targeted host:
  - Name:
  - Operating System:
- Does the Nessus vulnerability assessment scan report provide any information regarding to risk, threats, or vulnerabilities found?
- What must you do to confirm or verify if the identified OS, software, application has the latest release and/or software updates and patches?

9. Answer the Lab #5 – Assessment Questions and submit to the Instructor.

Deliverables

Upon completion of Lab #5 – Identify Risks, Threats & Vulnerabilities in an IT Infrastructure Using ZeNmap GUI (Nmap) & Nessus® Reports, students are required to provide the following deliverables as part of this lab:

1. Lab #5 – A four-paragraph executive summary written to executive management providing a summary of findings, risk impact to the IT asset and organization, and recommendations for next steps
2. Lab #5 - Assessment Questions and Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #5 that the students must perform:

1. Was the student able to review a ZeNmap GUI (Nmap) network discovery and port scanning report and a Nessus® software vulnerability report from a risk management perspective? – [**20%**]
2. Was the student able to identify hosts, operating systems, services, applications, and open ports on devices from the ZeNmap GUI (Nmap) scan report from a risk management perspective? – [**20%**]
3. Was the student able to identify critical, major, and minor software vulnerabilities from the Nessus® vulnerability assessment scan report? – [**20%**]
4. Was the student able to assess the exploit potential of the identified software vulnerabilities by conducting a high-level risk impact by visiting the Common Vulnerabilities & Exposures (CVE) online listing of software vulnerabilities at http://cve.mitre.org/ ? – [**20%**]
5. Was the student able to craft an executive summary prioritizing the identified critical and major threats and vulnerabilities and their risk impact on the IT organization? – [**20%**]

Lab #5: Assessment Worksheet

Identify Threats and Vulnerabilities in an IT Infrastructure

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

One of the most important first steps to risk management and implementing a security strategy is to identify all resources and hosts within the IT infrastructure. Once you identify the workstations and servers, you now must then find the threats and vulnerabilities found on these workstations and servers. Servers that support mission critical applications require security operations and management procedures to ensure C-I-A throughout. Servers that house customer privacy data or intellectual property require additional security controls to ensure the C-I-A of that data. This lab requires the students to identify threats and vulnerabilities found within the Workstation, LAN, and Systems/Applications Domains.

Lab Assessment Questions

1. What are the differences between ZeNmap GUI (Nmap) and Nessus?

2. Which scanning application is better for performing a network discovery reconnaissance probing of an IP network infrastructure?

3. Which scanning application is better for performing a software vulnerability assessment with suggested remediation steps?

4. How many total scripts (i.e., test scans) does the Intense Scan using ZenMap GUI perform?

5. From the ZenMap GUI pdf report page 6, what ports and services are enabled on the Cisco Security Appliance device?

6. What is the source IP address of the Cisco Security Appliance device (refer to page 6 of the pdf report)?

7. How many IP hosts were identified in the Nessus® vulnerability scan? List them.

8. While Nessus provides suggestions for remediation steps, what else does Nessus provide that can help you assess the risk impact of the identified software vulnerability?

9. Are open ports necessarily a risk? Why or why not?

10. When you identify a known software vulnerability, where can you go to assess the risk impact of the software vulnerability?

11. If Nessus provides a pointer in the vulnerability assessment scan report to look up CVE-2009-3555 when using the CVE search listing, specify what this CVE is, what the potential exploits are, and assess the severity of the vulnerability.

12. Explain how the CVE search listing can be a tool for security practitioners and a tool for hackers.

13. What must an IT organization do to ensure that software updates and security patches are implemented timely?

14. What would you define in a vulnerability management policy for an organization?

15. Which tool should be used first if performing an ethical hacking penetration test and why?