Vulnerability Assessment and Asset Discovery - Activity Guide

Activity Overview

In this activity, you will perform vulnerability assessment and asset discovery on a provided target network range. You will use tools available in Parrot OS to scan, identify, and classify vulnerabilities and assets.

Required Tools

- Parrot OS
- Nmap
- OpenVAS (Optional)
- Network access to target range [192.168.1.0/24]

Part 1: Asset Discovery Scan

Initial Network Mapping

1. Perform host discovery:

bash

Copy

```
# Basic host discovery
sudo nmap -sn 192.168.1.0/24

# Save output
sudo nmap -sn 192.168.1.0/24 -oN initial_hosts.txt
```

2. Identify live hosts:
    - Document number of responsive hosts
    - List IP addresses found
    - Note any hostnames resolved

Service Enumeration

1. Scan discovered hosts for services:

bash

Copy

```
# Service version detection
sudo nmap -sV -p- [discovered_host_ip]

# Save detailed output
sudo nmap -sV -p- [discovered_host_ip] -oN services.txt
```

2. Document for each host:
    - Open ports
    - Running services
    - Service versions
    - Operating system details (if available)

Required Documentation

- Network map showing discovered hosts

- List of critical assets identified
- Service inventory table
- Initial risk assessment based on exposed services

Part 2: Vulnerability Scan

Basic Vulnerability Scan Using Nmap

1. Perform vulnerability scan:

bash

Copy

```
# Using NSE scripts for vulnerabilities
sudo nmap -sV --script vuln [target_ip]

# Save vulnerability scan output
sudo nmap -sV --script vuln [target_ip] -oN vulns.txt
```

2. Additional targeted scans based on discovered services:

bash

Copy

```
# Web vulnerability scripts
sudo nmap -p80,443 --script "http-* and not http-brute*" [target_ip]

# SMB vulnerability scripts
sudo nmap -p445 --script "smb-vuln*" [target_ip]
```

Vulnerability Classification

For each vulnerability found:

1. Record:
   - Vulnerability name/ID
   - Affected service
   - CVSS score (if available)
   - Potential impact
2. Classify vulnerabilities by severity:
   - Critical (CVSS 9.0-10.0)
   - High (CVSS 7.0-8.9)
   - Medium (CVSS 4.0-6.9)
   - Low (CVSS 0.1-3.9)

Required Documentation

1. Asset Discovery Report

- Network topology diagram
- List of discovered hosts
- Service inventory table
- Critical asset identification

2. Vulnerability Assessment Report

- Executive Summary

- Methodology
- Detailed Findings
  - Vulnerability description
  - Affected systems
  - Severity classification
  - Potential impact
  - Remediation recommendations
- Risk Assessment
  - Risk rating for each finding
  - Overall system risk assessment
  - Priority recommendations

Submission Format

Create a professional report including:

1. Methodology Section
   - Tools used
   - Scan configurations
   - Assessment approach
2. Findings Section
   - Asset inventory
   - Vulnerability details
   - Supporting evidence (scan outputs)
3. Risk Assessment
   - Severity classifications
   - Impact analysis
   - Remediation priorities
4. Appendices
   - Raw scan outputs
   - Commands used
   - Additional technical details

Safety Notes

- Only scan authorized targets
- Follow provided scope
- Document any unexpected findings
- Stop scanning if systems become unresponsive

Evaluation Criteria

Your submission will be evaluated on:

1. Thoroughness of discovery
2. Accuracy of vulnerability classification
3. Quality of documentation
4. Clarity of risk assessment
5. Professionalism of report