**CYBR430, Penetration Testing and Incident Response**  
**Week 4 Lab – Vulnerability Scanning**

**NAME: \_\_\_Chad Ballay\_\_\_\_\_\_\_\_**

**DATE: \_\_\_\_12/13/2020\_\_\_\_\_\_\_\_**

**Chad Ballay**

**CYBR430-342**

**Week 4 – Vulnerability Scanning**

**12/14/2020**

**Part 1: Scanning with OpenVas (25 points)**

**Complete scans on all the HAL assets. Once complete provide a screen shot of your task dashboard showing the completed scans. It’s the screen that looks like the below but should show all your scanning tasks complete.**



**Part 2: Vulnerability Research (25 points)**

**Using the information in openvas and the CVE and NVD databases research the vulnerabilities you have found**. **Complete the table below based on your research.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Host(s) IP | CVE or other Identifier | Severity | CVSS Score (if Available) | Vulnerability Name/Description |
| 10.19.99.10 | CVE-2017-0143, | High | 8.1 | The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148. |
| 10.19.99.10 | CVE-2017-0144 | High | 8.1 | The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148. |
| 10.19.99.10 | CVE-2017-0145 | High | 8.1 | The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0146, and CVE-2017-0148. |
| 10.19.99.10 | CVE-2017-0146 | High | 8.1 | The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0148. |
| 10.19.99.10 | CVE-2017-0147 | Med | 5.9 | The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packets, aka "Windows SMB Information Disclosure Vulnerability." |
| 10.19.99.10 | CVE-2017-0148 | High | 8.1 | The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0146. |
| 10.19.99.10, 10.19.99.12, 10.19.99.14, 10.19.99.16, 10.19.99.18 | CVE-1999-0519 | NA(3.0) High(2.0) | 7.5 | A NETBIOS/SMB share password is the default, null, or missing. |
| 10.19.99.5 |  |  |  | The service is using a SSL/TLS certificate from a known untrusted certificate authority. An attacker could use this for a MitM attacks, accessing sensible data and other attacks. |
| 10.19.99.10, 10.19.99.12, 10.19.99.14, 10.19.99.16, 10.19.99.18 |  |  |  | Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. |
| 10.19.99.1 |  |  |  | The host / application transmits sensitive information (username, passwords) in cleartext via HTTP. |