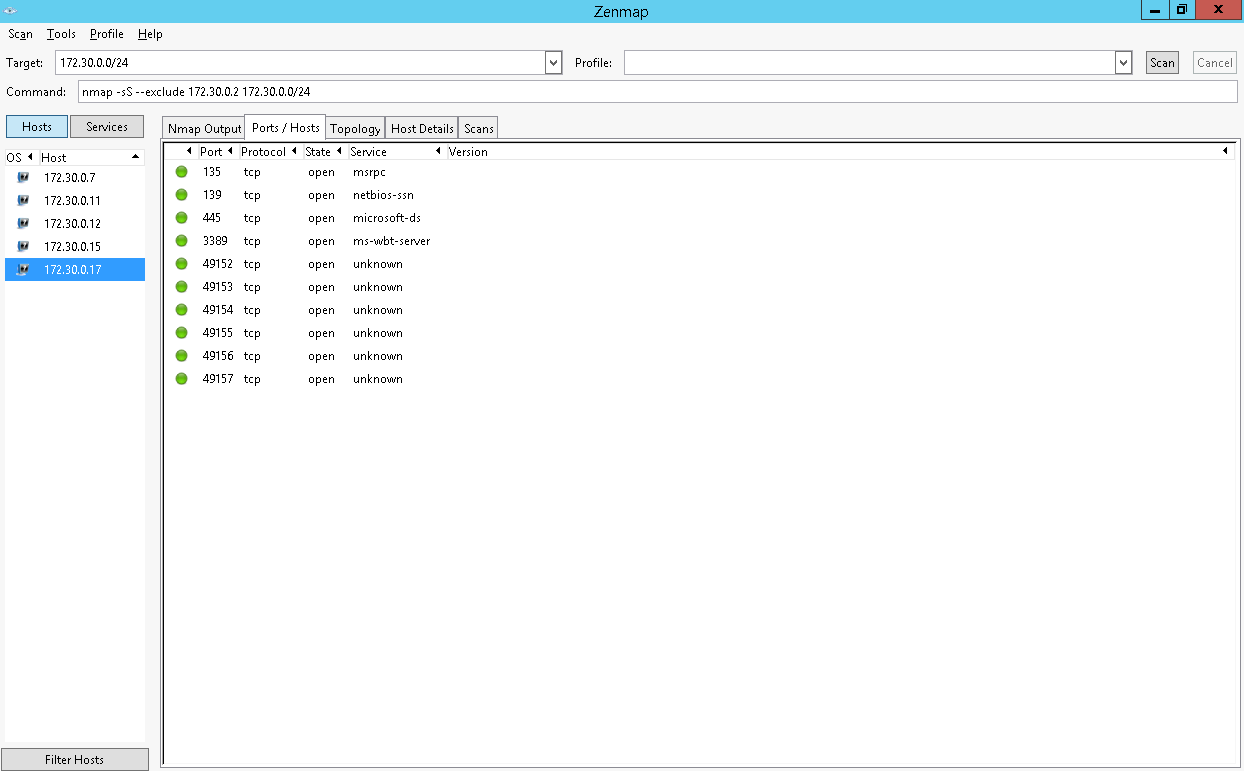
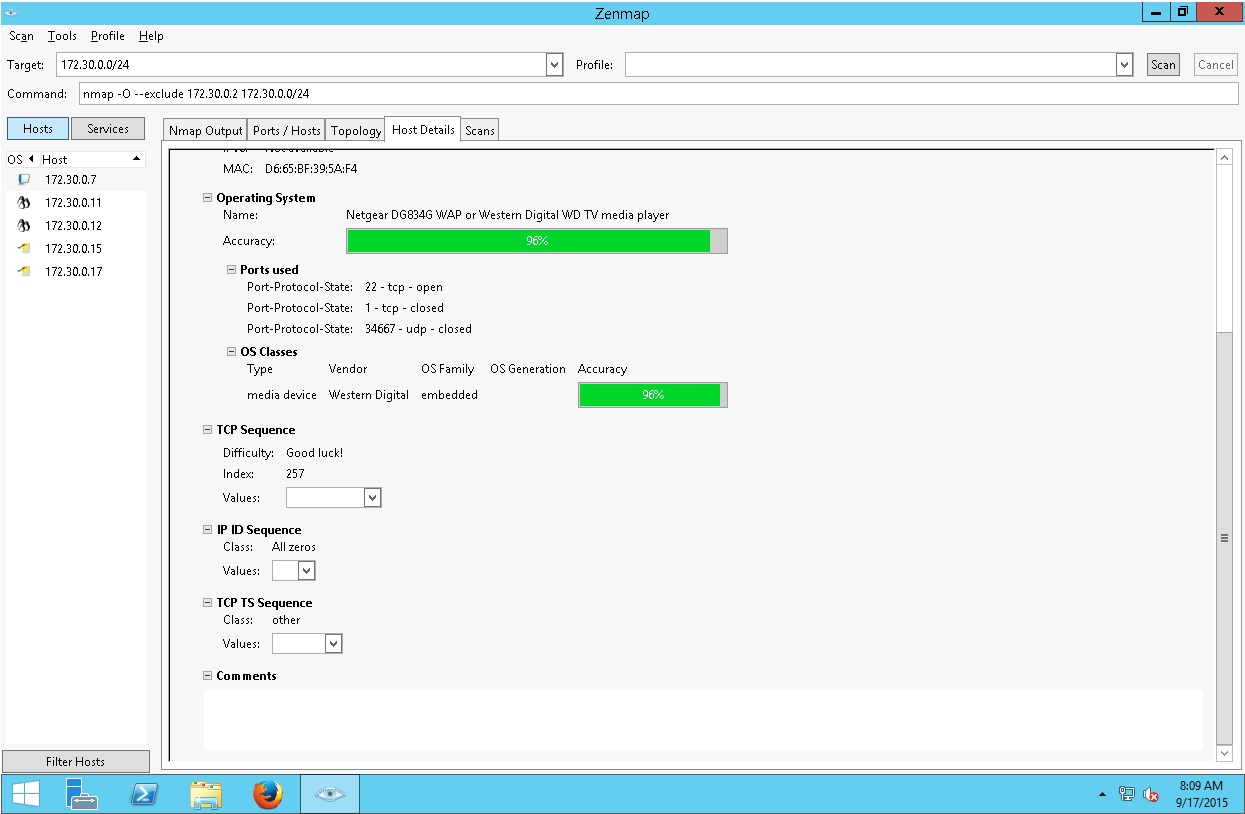
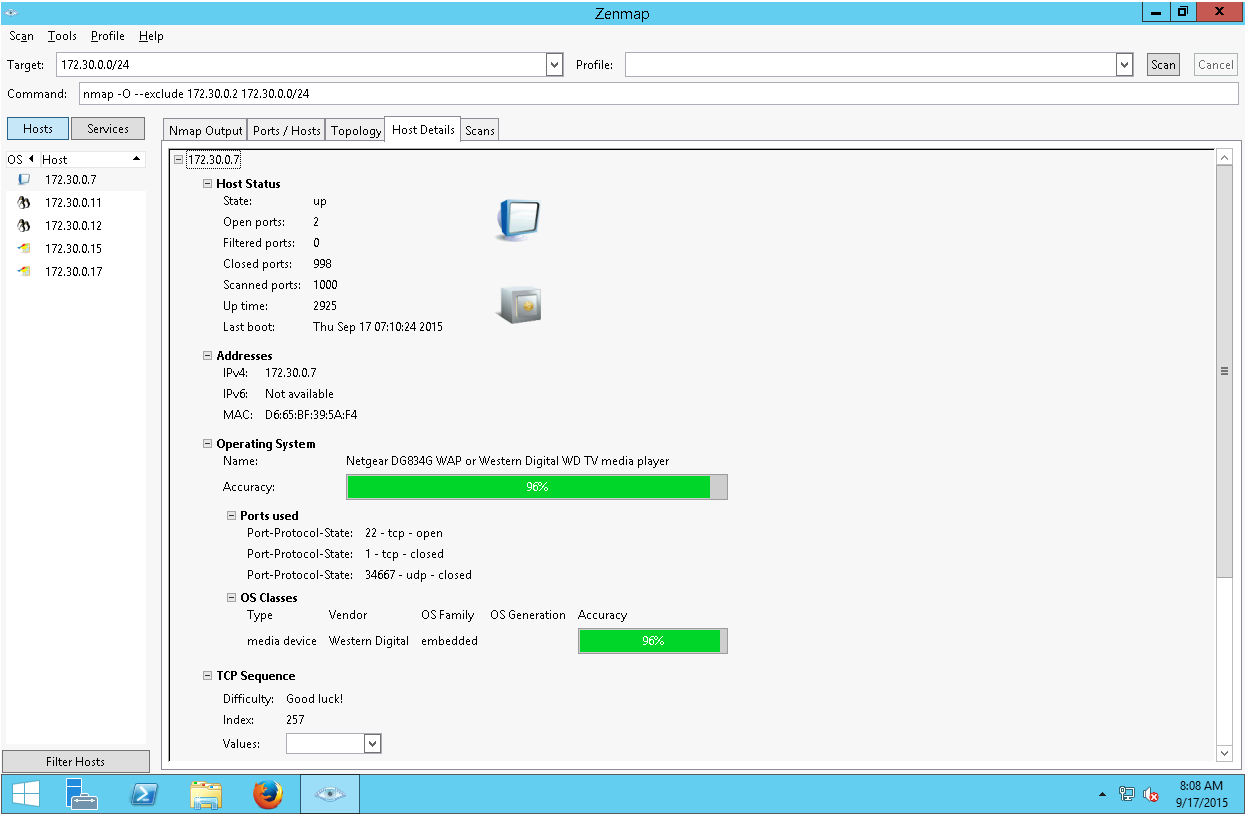
**Lab Report**

# Nmap commands screenshot

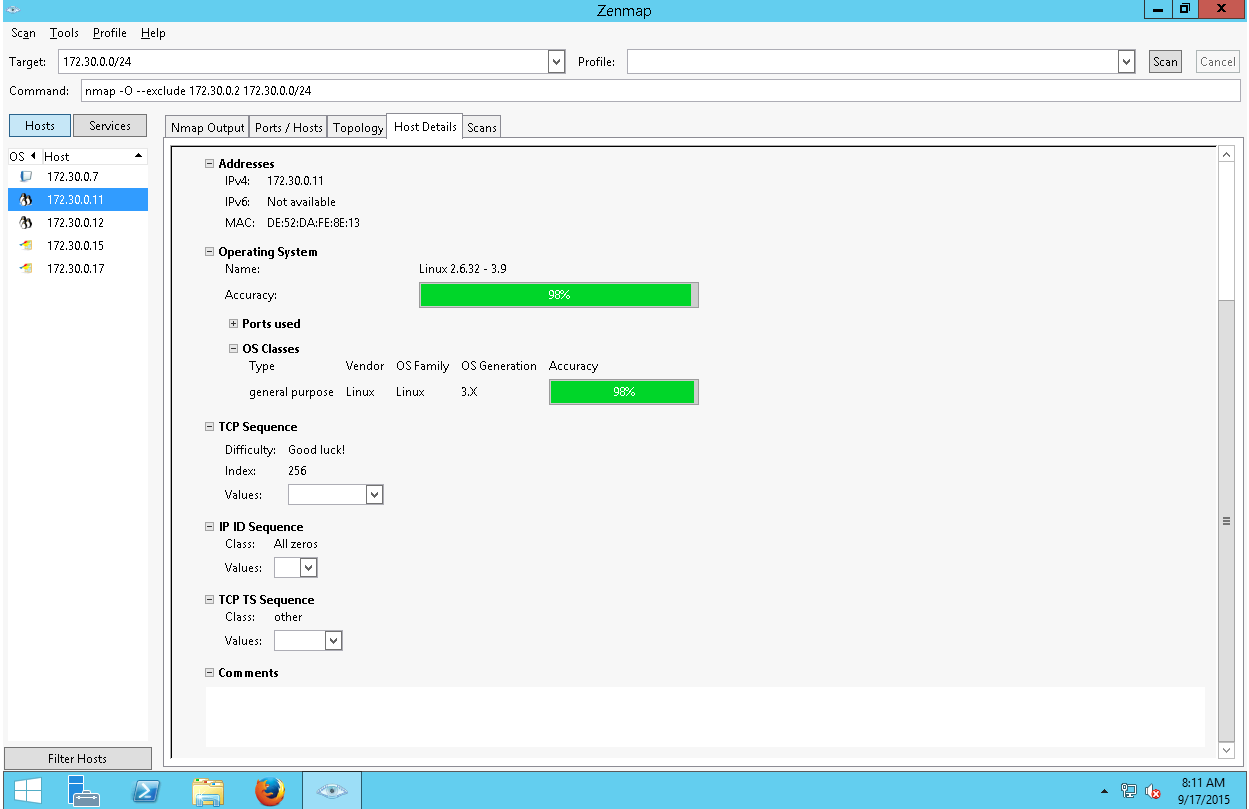
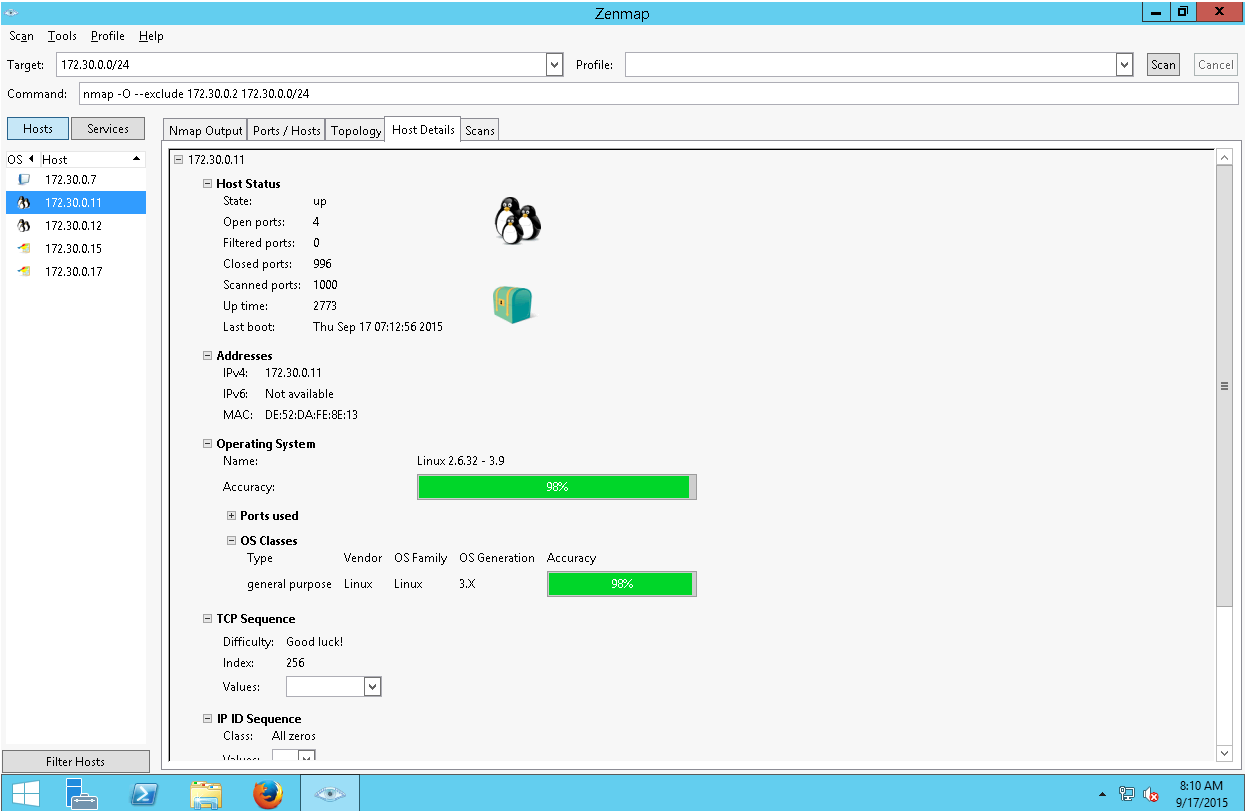
1. **Nmap -sS –exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.17 Ports/Hosts**



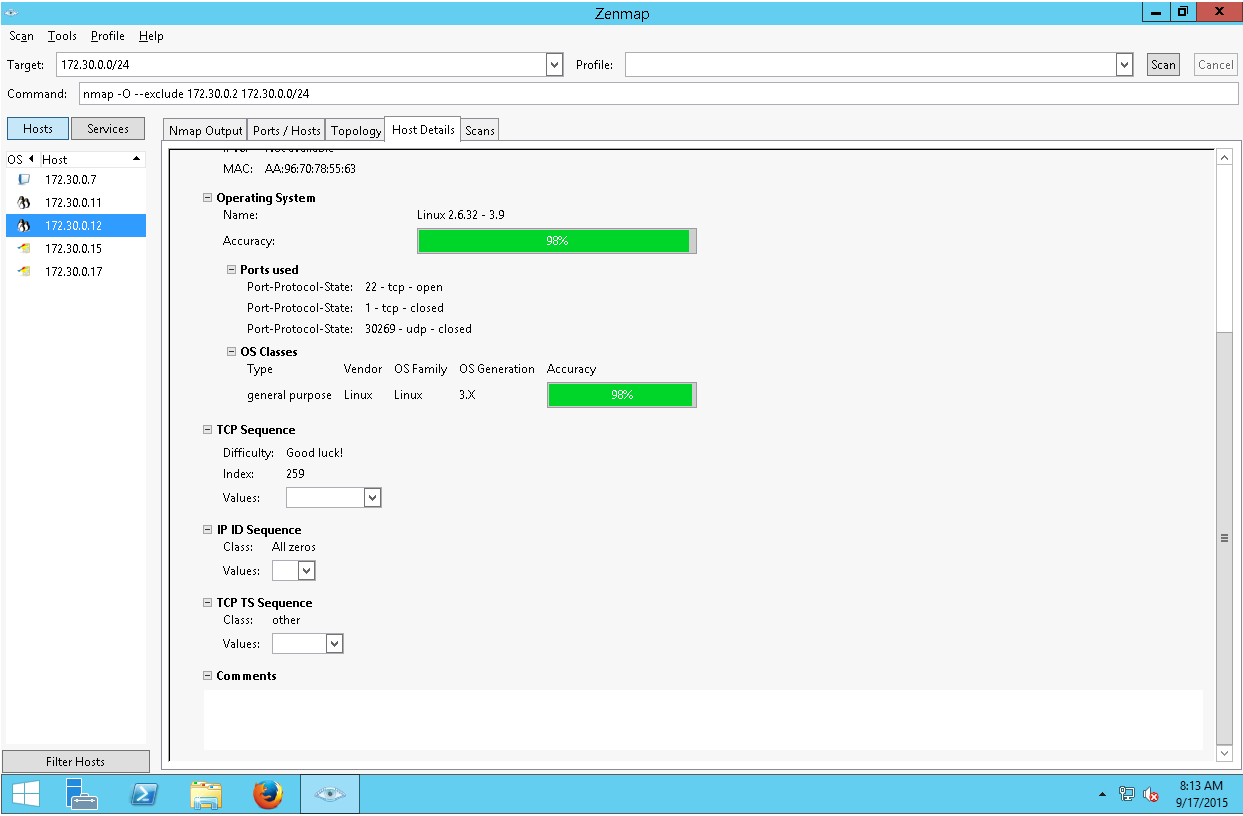
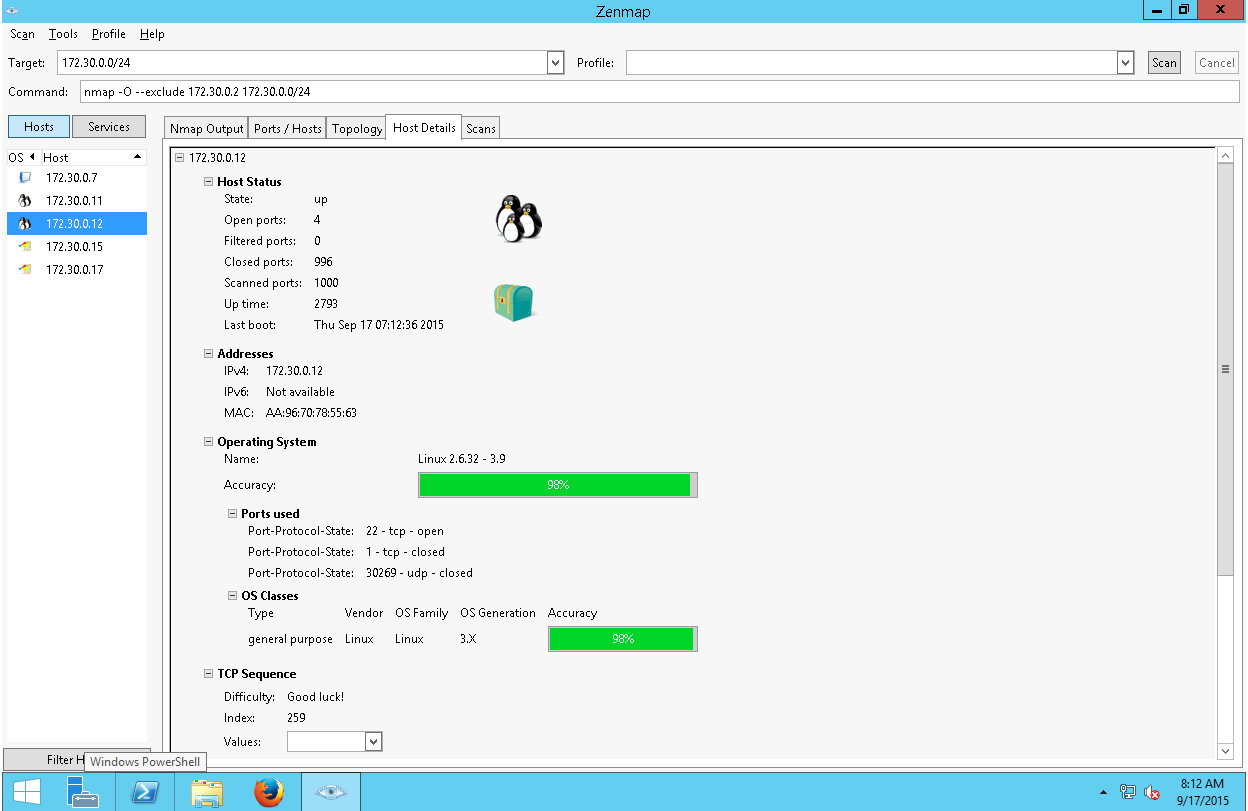
1. **Nmap -O -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.7 hostDetails**



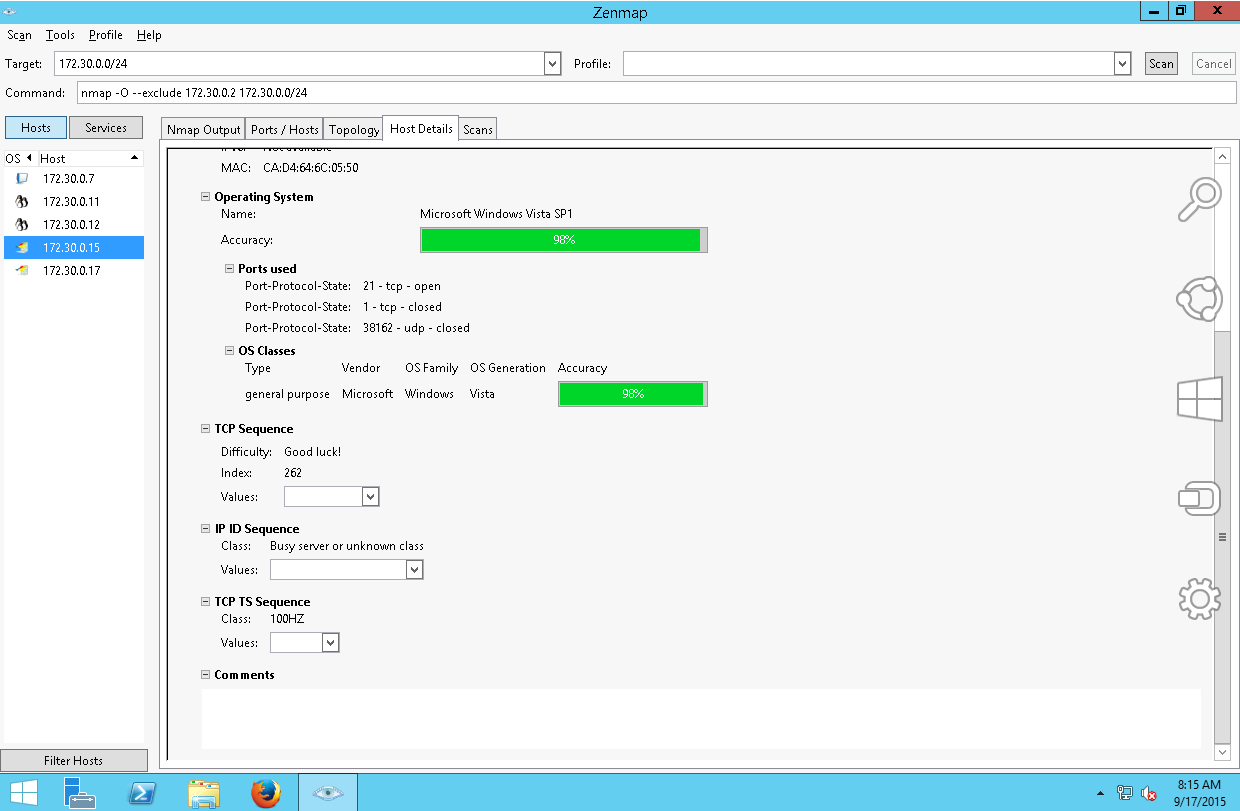
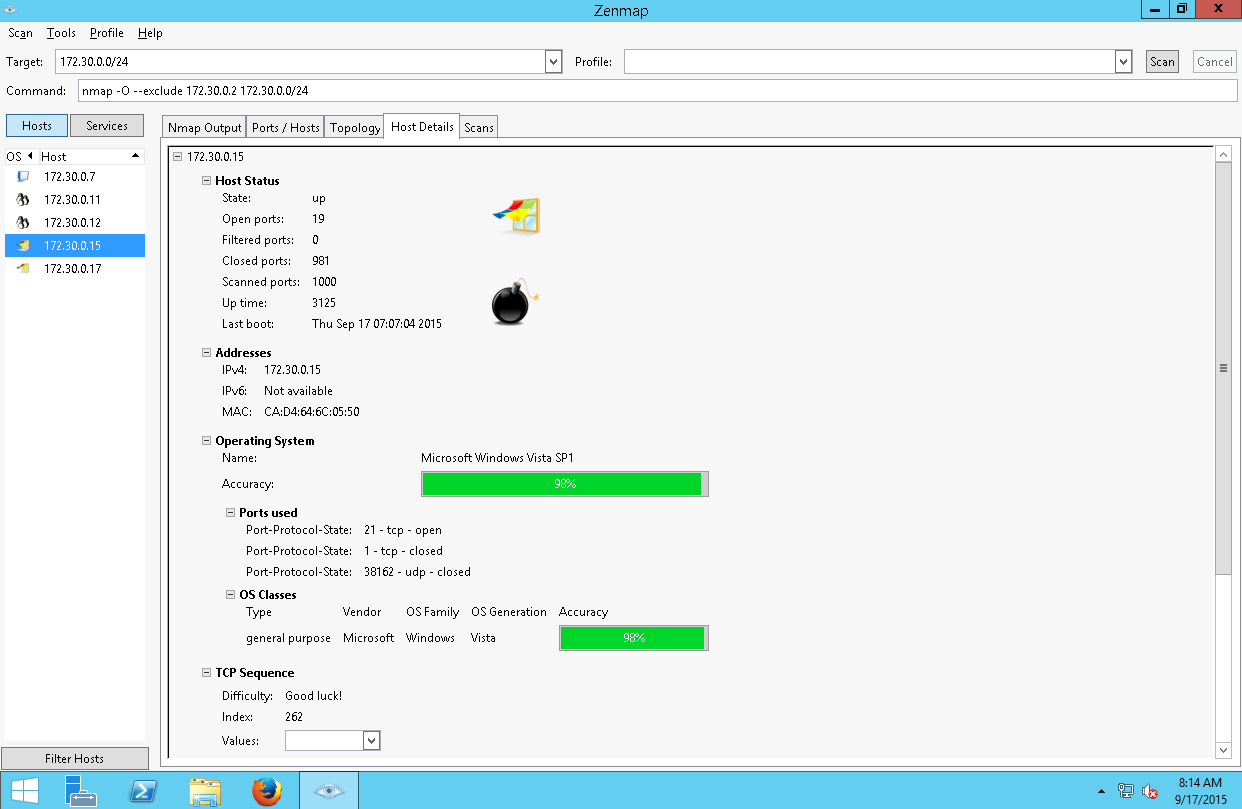
1. **Nmap -O -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.11 hostDetails**



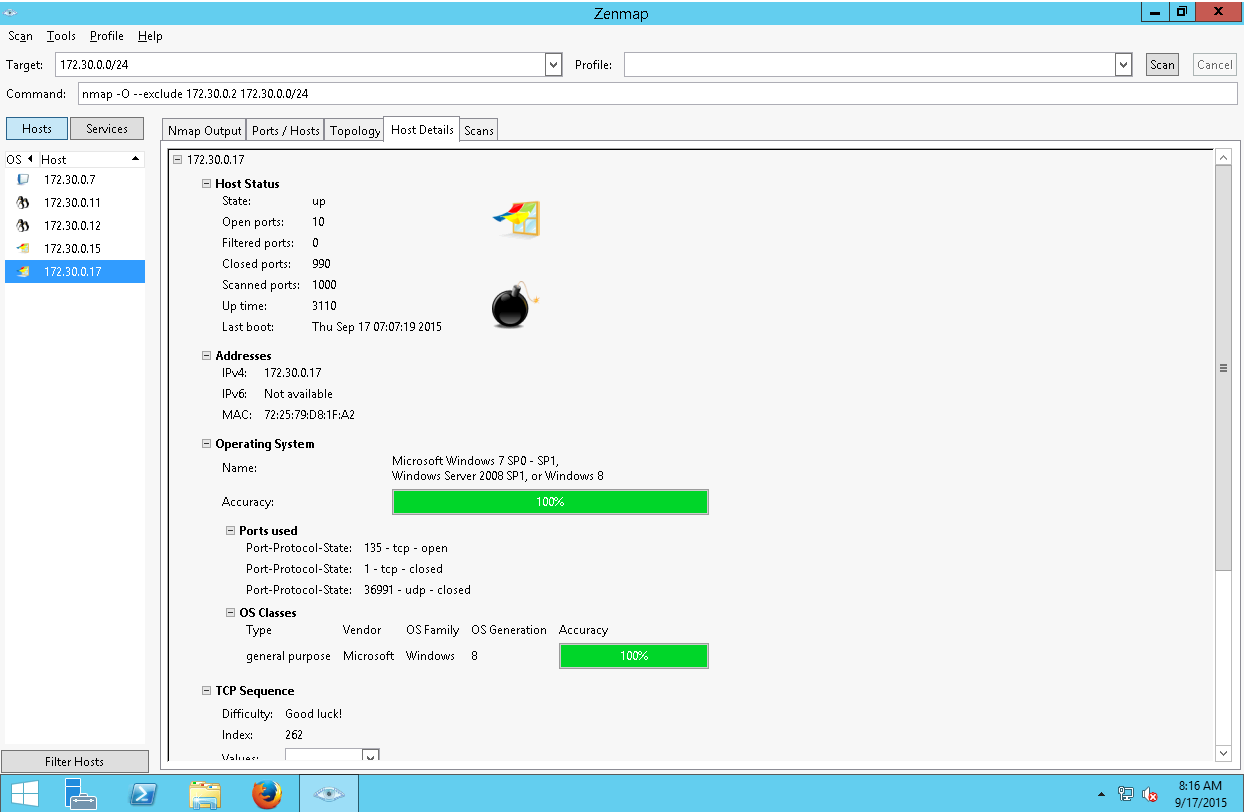
1. **Nmap -O -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.12 hostDetails**

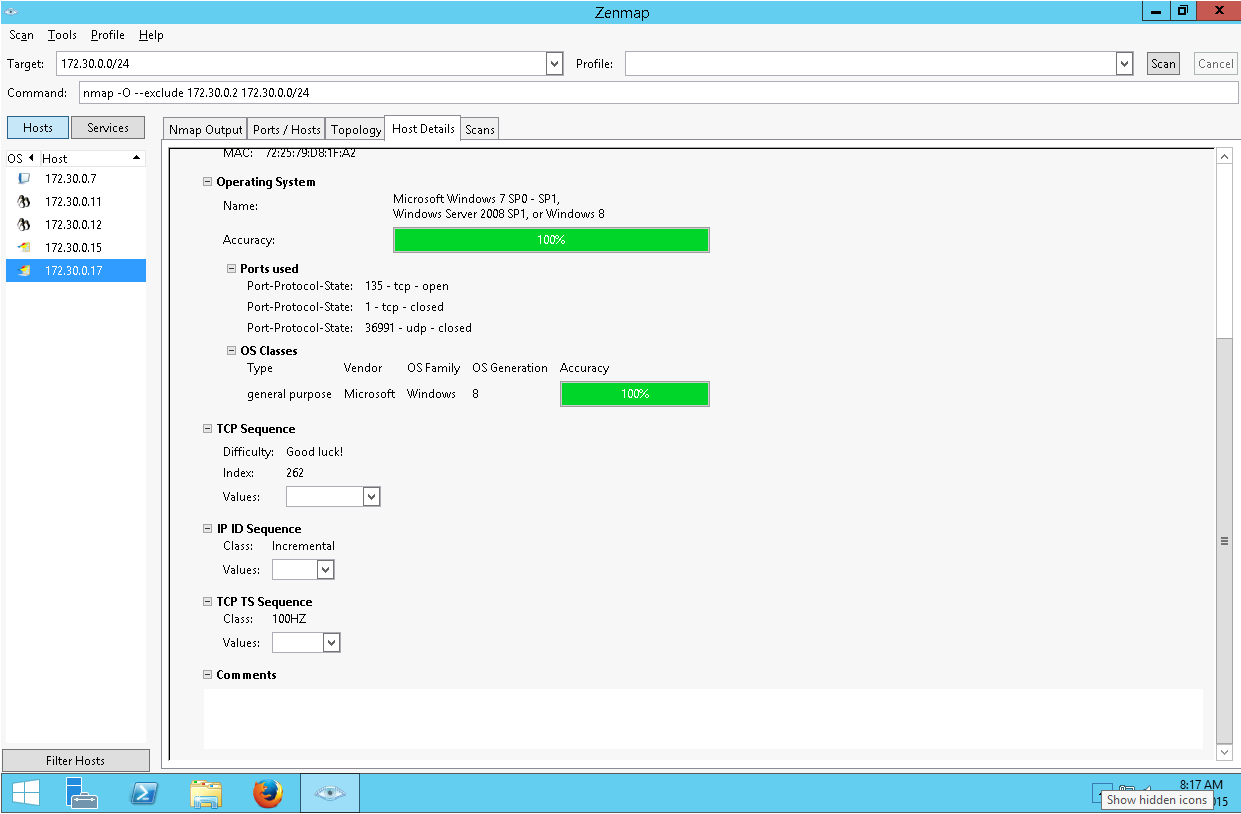


1. **Nmap -O -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.15 hostDetails**

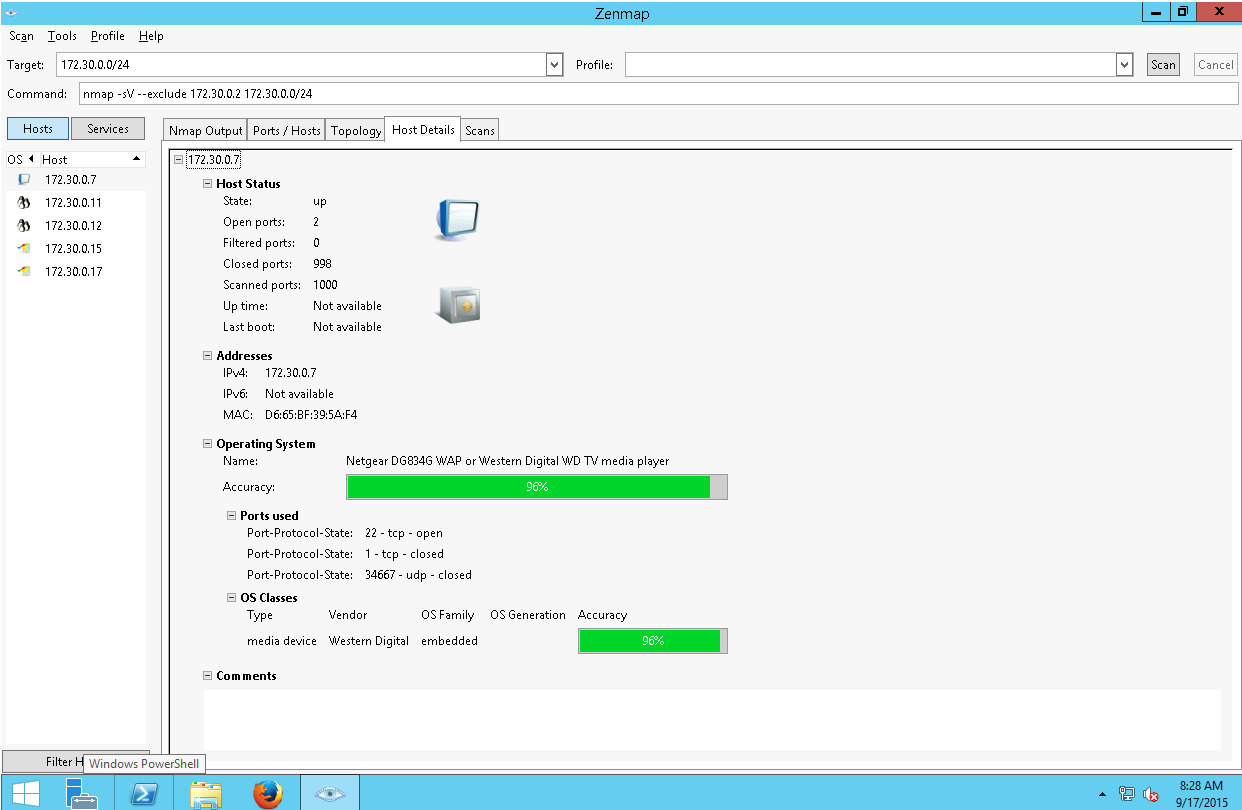


1. **Nmap -O -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.17 hostDetails**

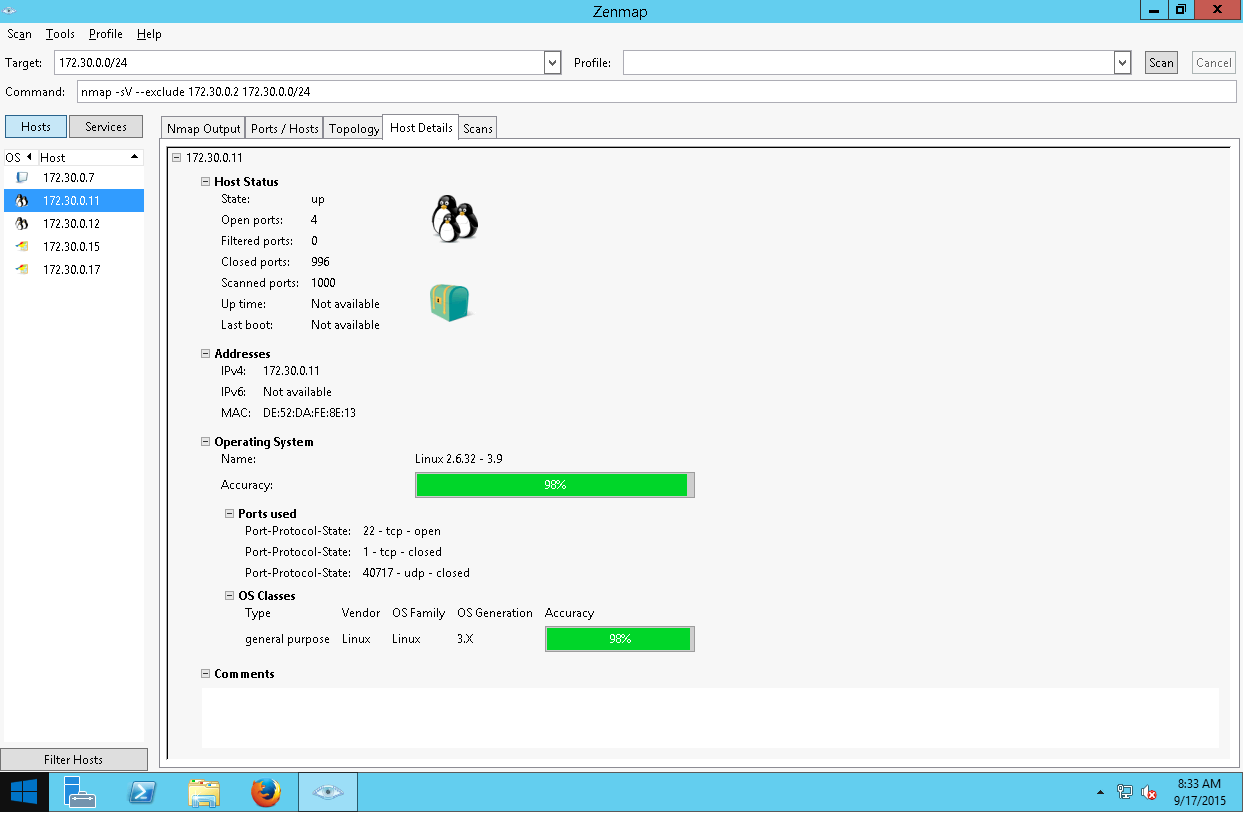




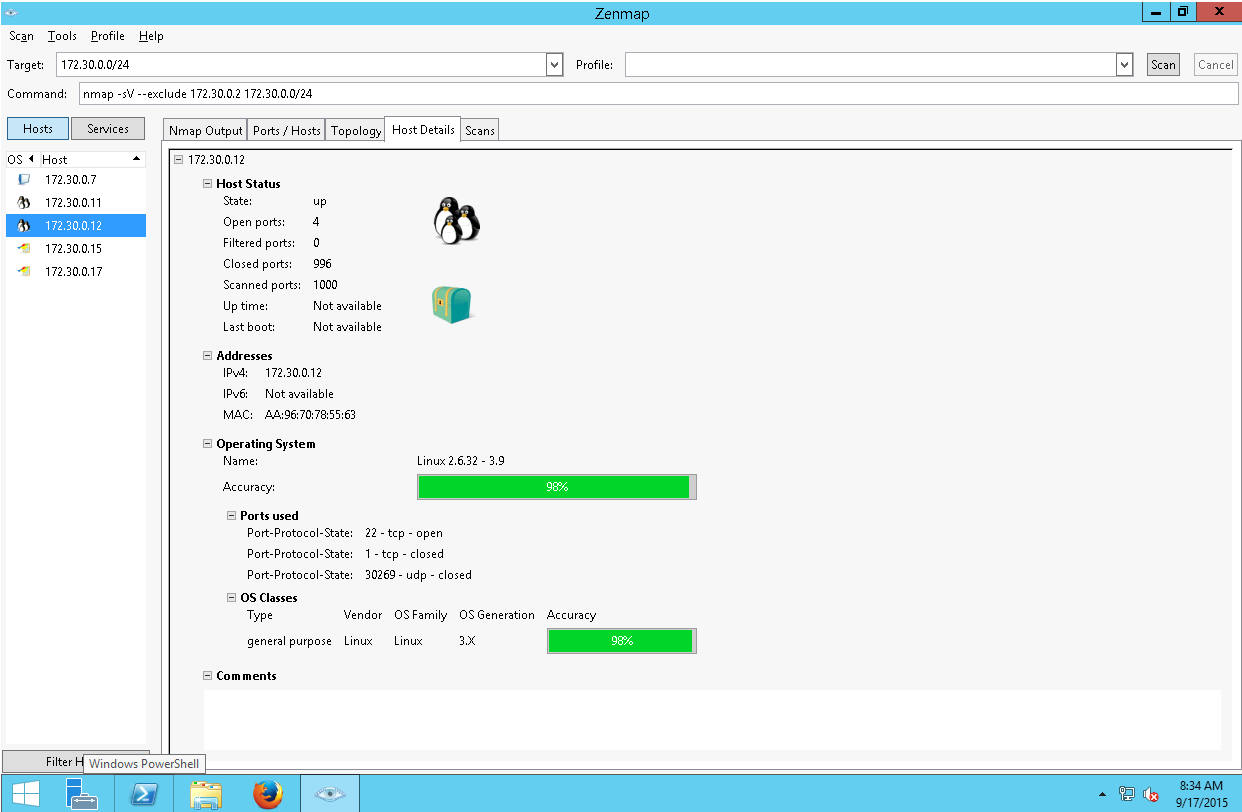
1. **Nmap -sV -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.07 hostDetails**



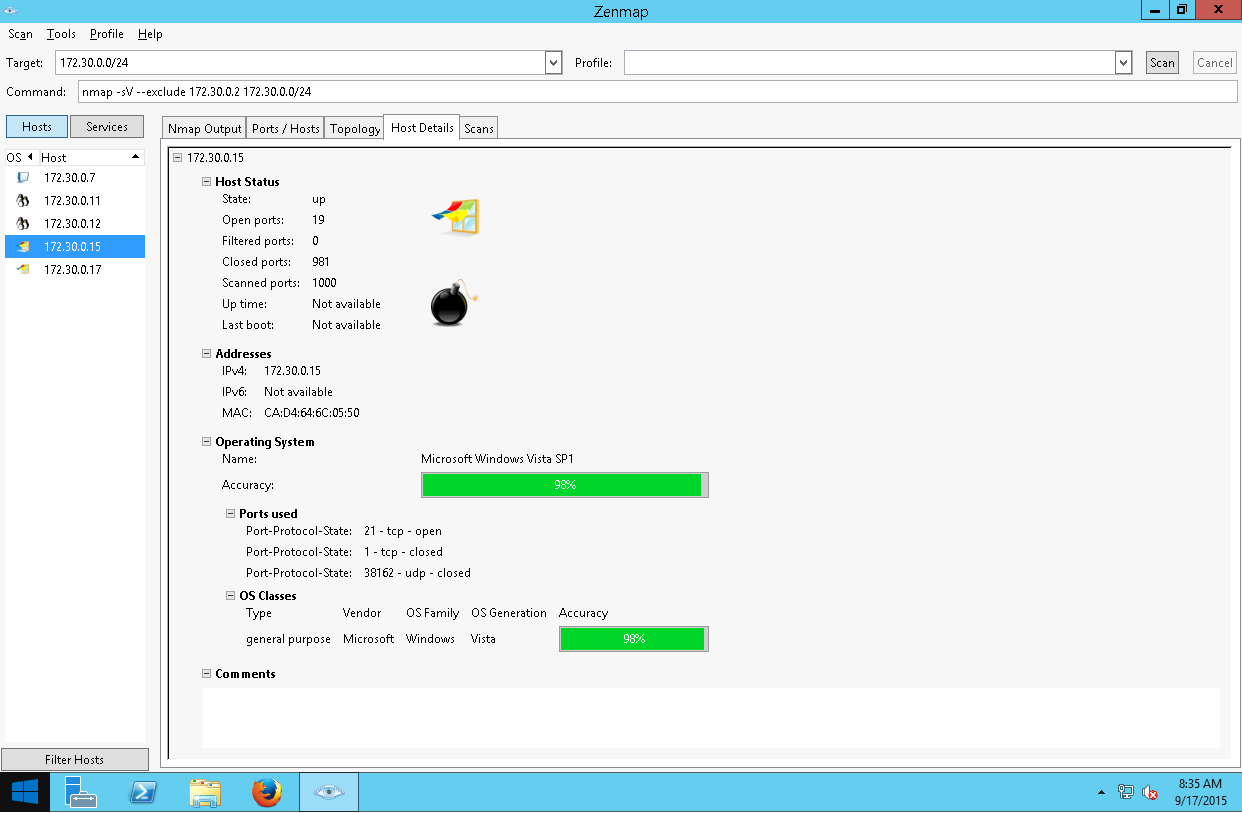
1. **Nmap -sV -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.11 hostDetails**



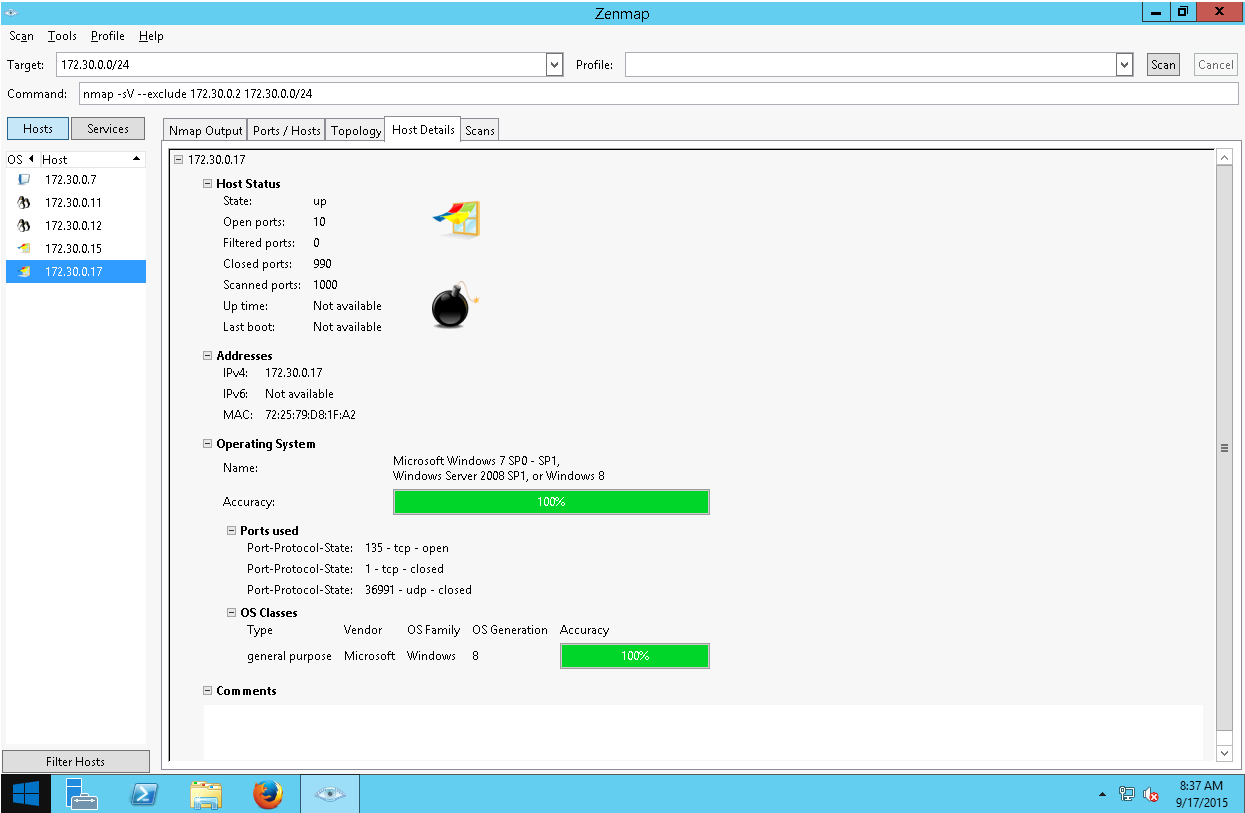
1. **Nmap -sV -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.12 hostDetails**



1. **Nmap -sV -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.15 hostDetails**

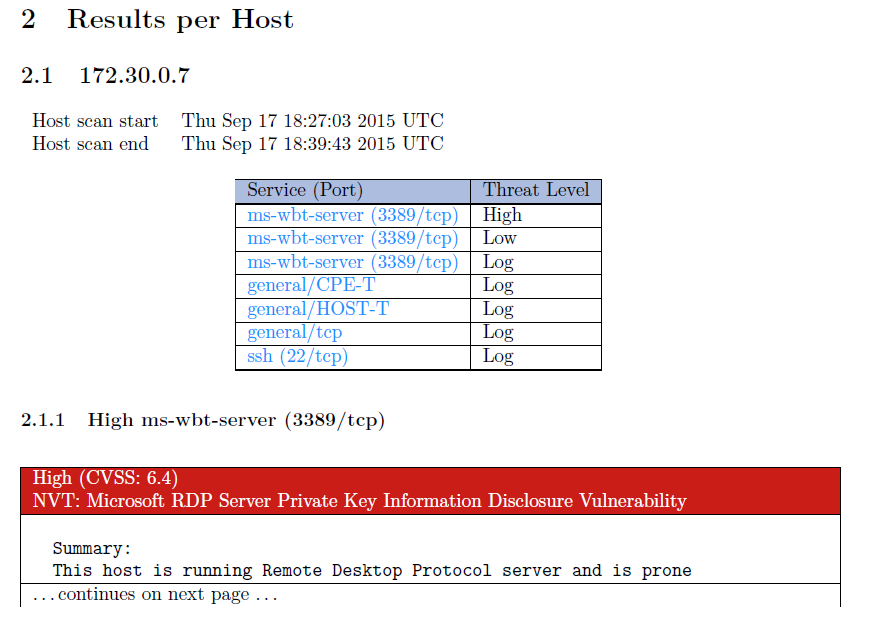


1. **Nmap -sV -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.17 hostDetails**

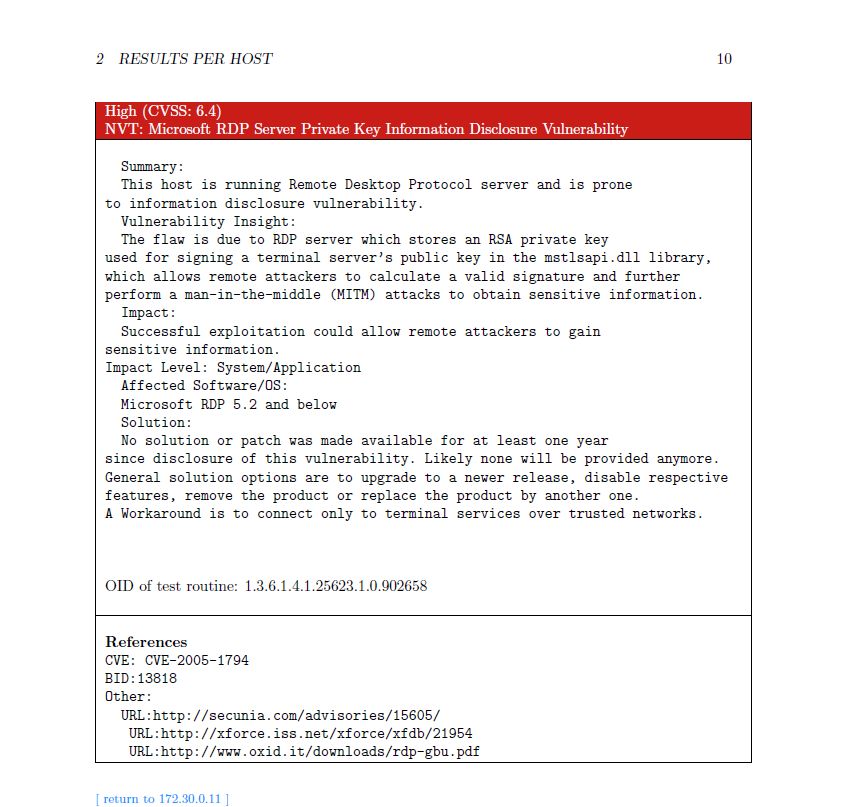


# OpenVAS high level vulnerability report analysis

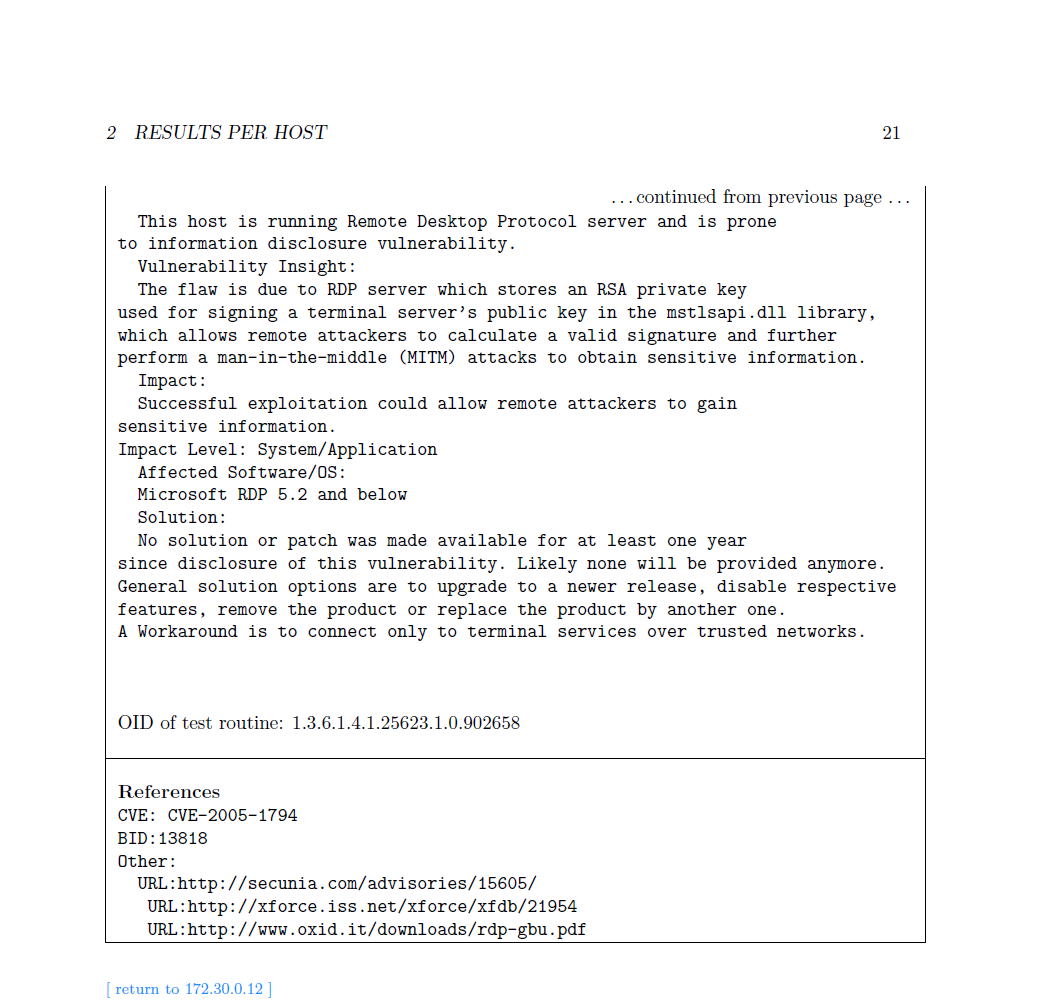
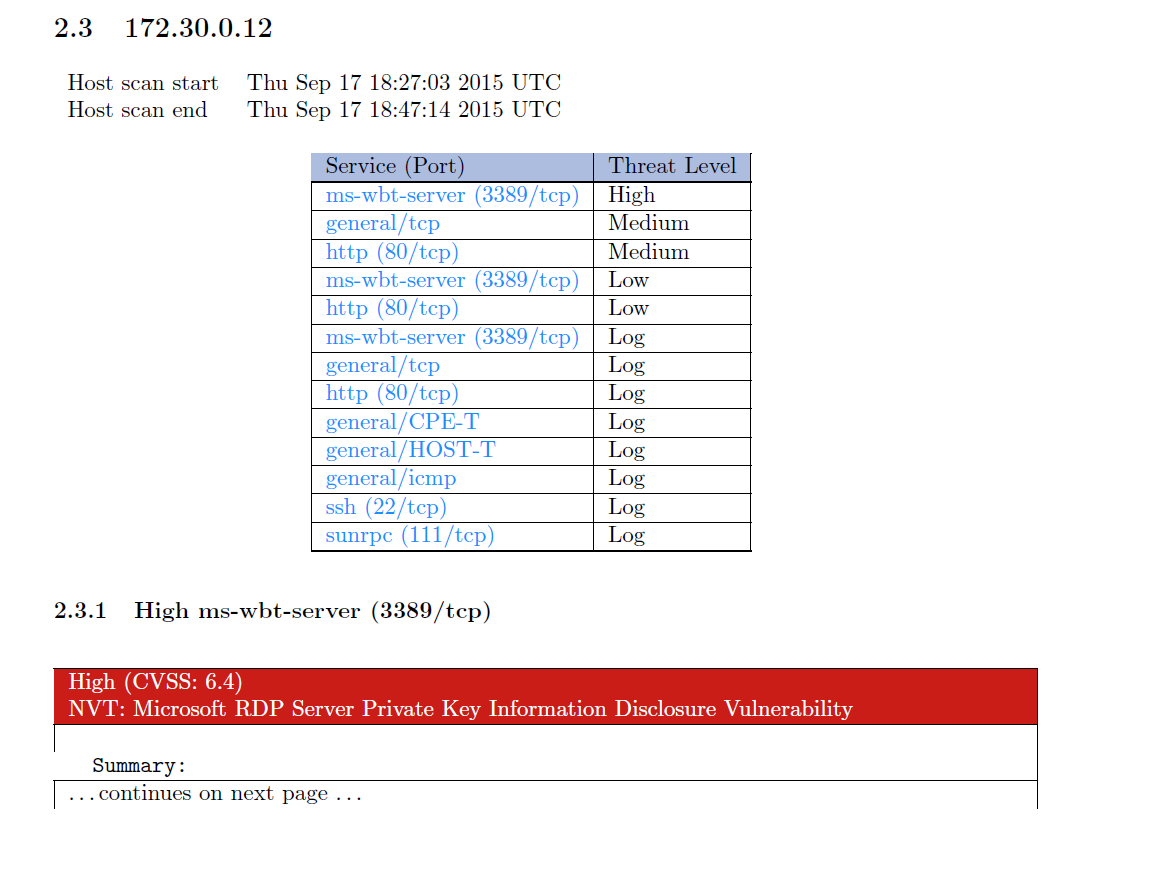
1. **Microsoft RDP Server Private Key Information Disclosure Vulnerability**
2. **172.30.0.7 High Vulnerability**

****

1. **172.30.0.11 High Vulnerability**

****

1. **172.30.0.12 High Vulnerability**

****

1. **Description and Recommendation**

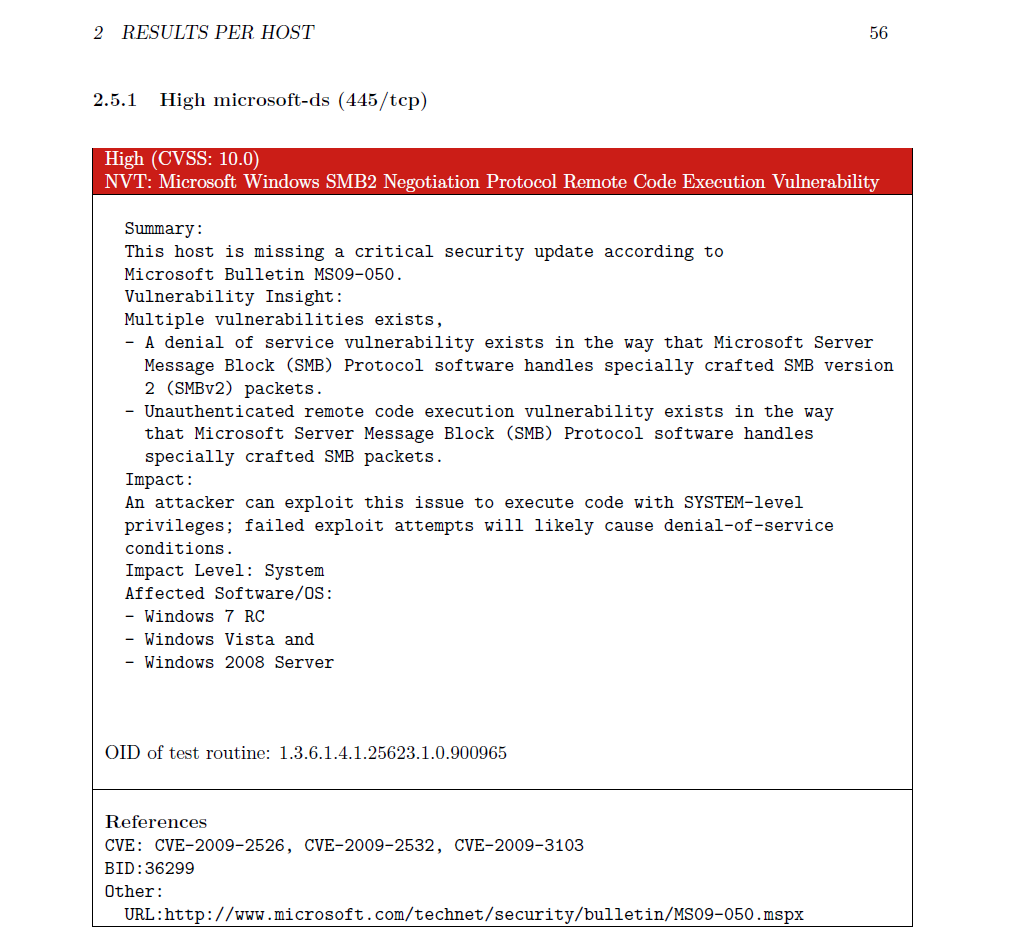
**Vulnerabilities descriptions summary:**

The type of the discovered vulnerabilities of the three hosts, 172.30.0.7, 172.30.0.11, 172.30.0.12 is the same – Microsoft RDP Server Private Key Information Disclosure Vulnerability. And, this kind of vulnerability happens at port 3389 which is using TCP protocol to communicate. The major danger of this vulnerability is that it allows potential attackers to act as a man-in-the-middle, which may cause serious sensitive information breach.

**Recommendation summary:**

Firstly, the vulnerability appears only on Microsoft RDP 5.2 and below. So, the first method is to upgrade the Microsoft RDP to higher versions. If the update is not available, I recommend turning down the features of RDP or just using other similar tools like TeamViewer or remote utilities … etc. The last way is to give up the graphic desktop and just use the terminal instead.

1. **Microsoft Windows SMB2 Negotiation Protocol Remote code Execution**
2. **172.30.0.17 High Vulnerability**

****

1. **Description and Recommendation:**

**Description:**

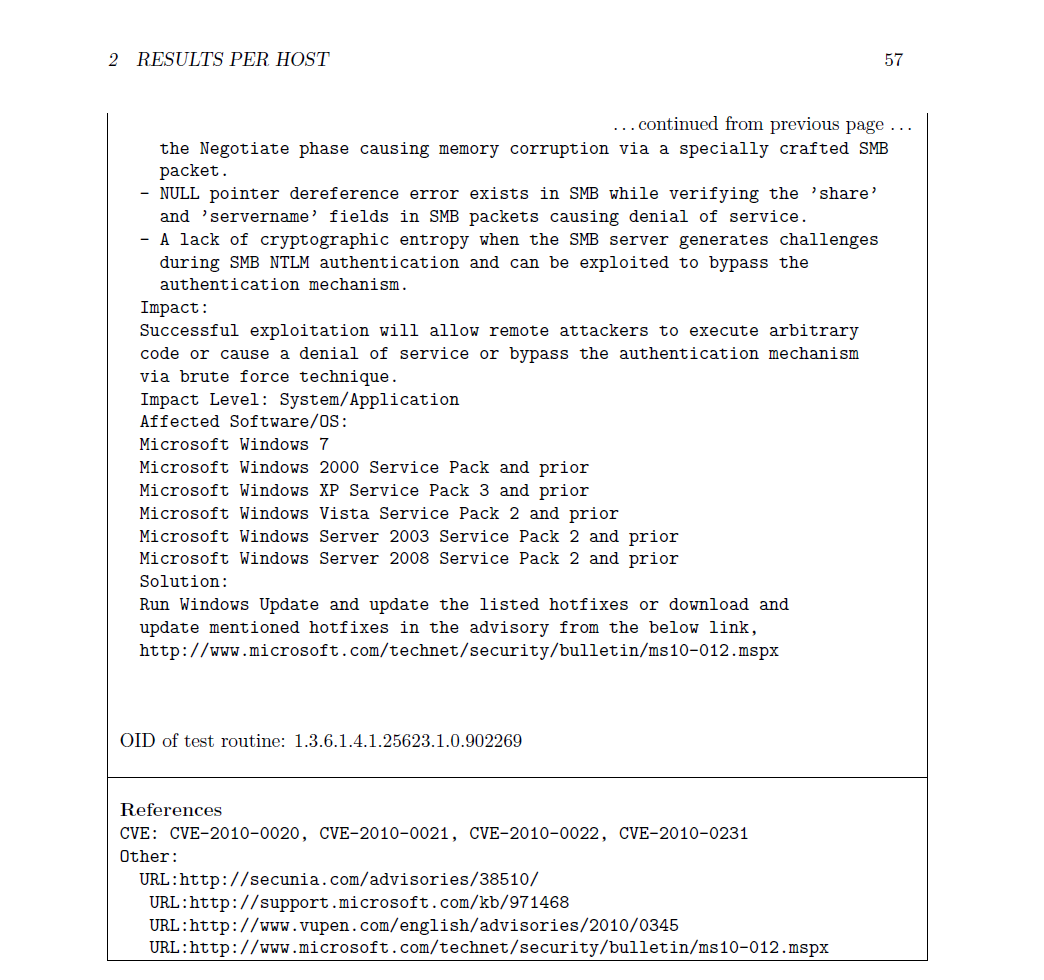
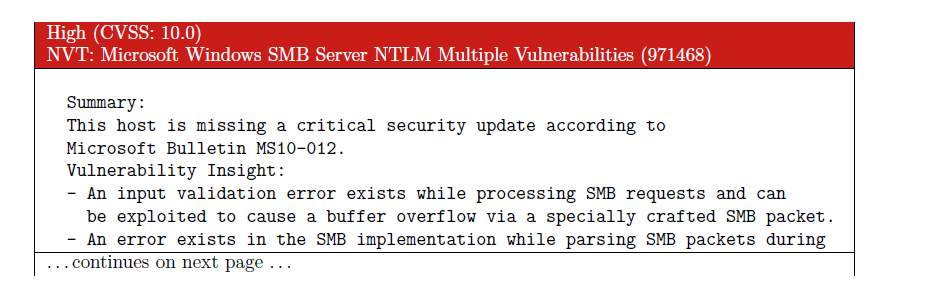
This vulnerability is caused by SMB communication functionality of Windows and it appears in many Windows versions at the port of 445 which use TCP as communication protocol. There are two major potential threats to user system – Denial of Services attack and modify SMB packets without authentication. Thus, attackers can obtain system-level privilege through this vulnerability.

**Recommendation:**

I recommend enabling the windows automatic update function and the patch will automatically installed. If the windows automatic update function is not available, users can download this patch on Microsoft official site to install it by themselves. If the patch still cannot be available, administrator should isolate the assaulted server, that is, restricting the access to that server. In addition, user still can download a Microsoft utility at the following URL to disable the SMBv2 function.

<https://support.microsoft.com/en-us/kb/975517>

1. **Microsoft Windows SMB Server NTLM Multiple Vulnerability**
2. **172.30.0.17 High Vulnerability**

****

1. **Description and Recommendation**

**Description:**

This vulnerability is also caused by SMB communication functionality of Windows and it appears in many Windows versions at the port of 445 which use TCP as communication protocol. It has four major threats to a system – causing buffer overflow, memory corruption, denial of service and bypass the system authentication mechanism. The attackers can take advantage of this vulnerability to steal sensitive data, sabotage data, and prevent user from using this service properly.

**Recommendation:**

For CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231, they are all belongs to SMB Server Could Allow Remote Code Execution and I recommend to use the Windows Update Services to automatically fix these vulnerabilities. If Windows auto update functionality is not available, just go to Microsoft official site to download the patch MS-09-050 and install them. Otherwise, if possible, administer could shut down the SMBv2 services.

# References

Microsoft. (2009, 10 13). *Microsoft Security Bulletin MS09-050 - Critical*. Retrieved 9 21, 2005, from technet.microsoft.com: https://technet.microsoft.com/en-us/library/security/ms09-050