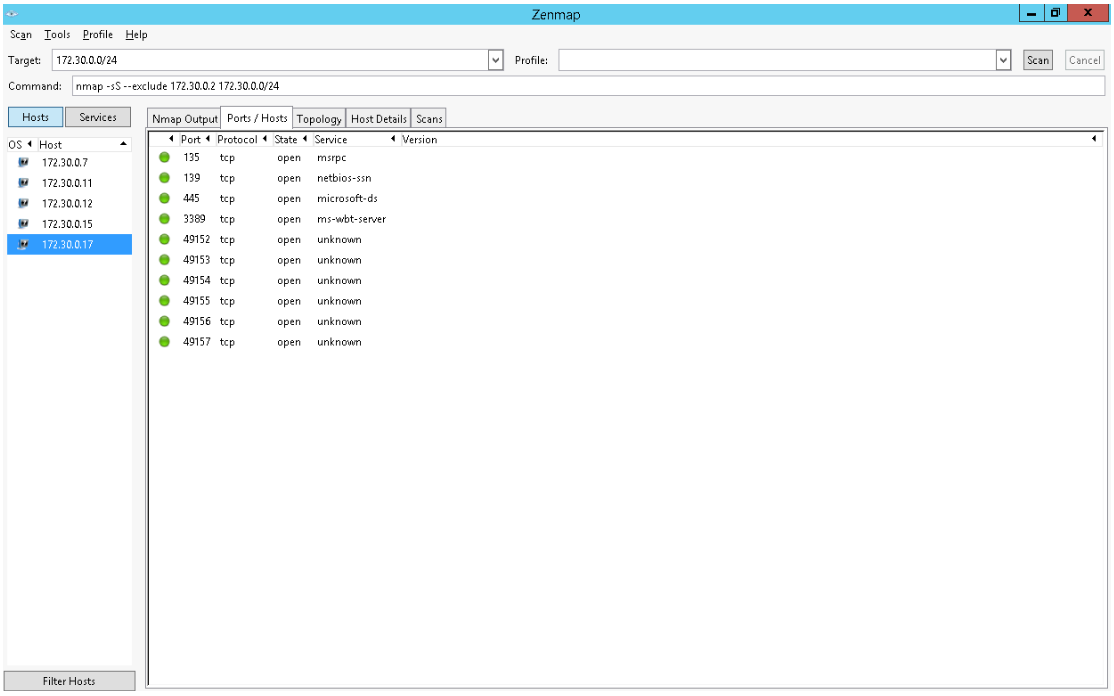
Lab Report

1. Nmap commands screenshot

1.1 Nmap -sS –exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.17 Ports/Hosts



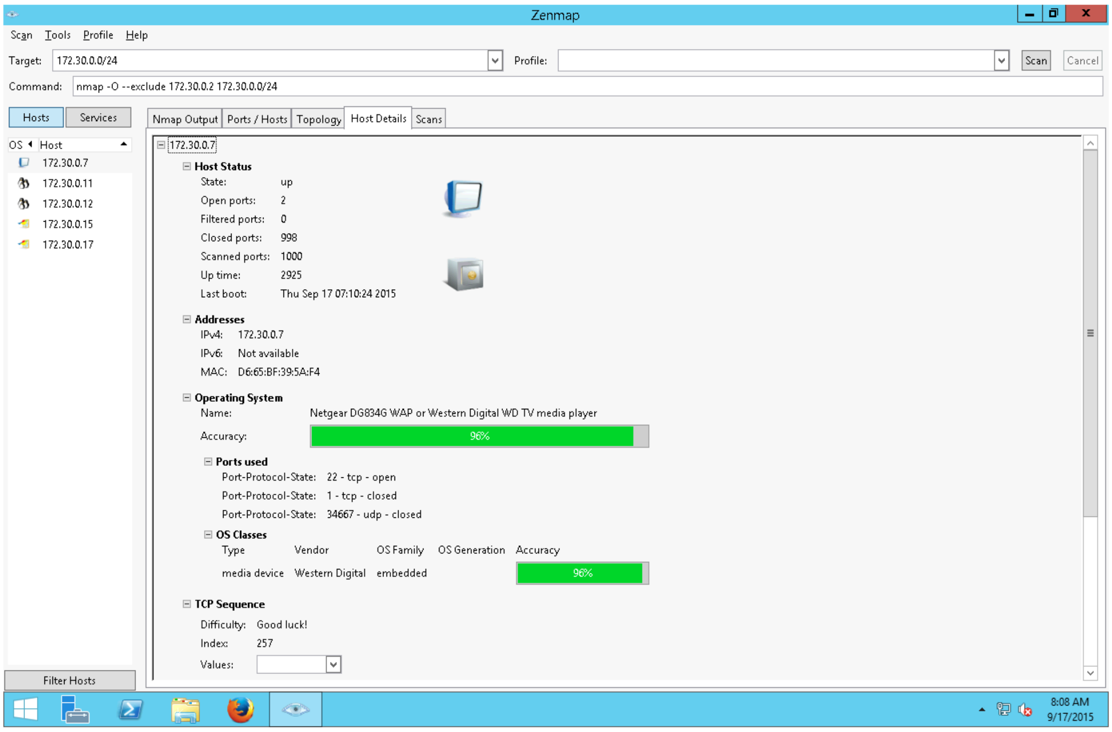
Target: 172.30.0.0/24

Command: nmap -sS --exclude 172.30.0.2 172.30.0.0/24

OS	Host
	172.30.0.7
	172.30.0.11
	172.30.0.12
	172.30.0.15
	172.30.0.17

	Port	Protocol	State	Service	Version
●	135	tcp	open	msrpc	
●	139	tcp	open	netbios-ssn	
●	445	tcp	open	microsoft-ds	
●	3389	tcp	open	ms-wbt-server	
●	49152	tcp	open	unknown	
●	49153	tcp	open	unknown	
●	49154	tcp	open	unknown	
●	49155	tcp	open	unknown	
●	49156	tcp	open	unknown	
●	49157	tcp	open	unknown	

1.2 Nmap -O -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.7 hostDetails

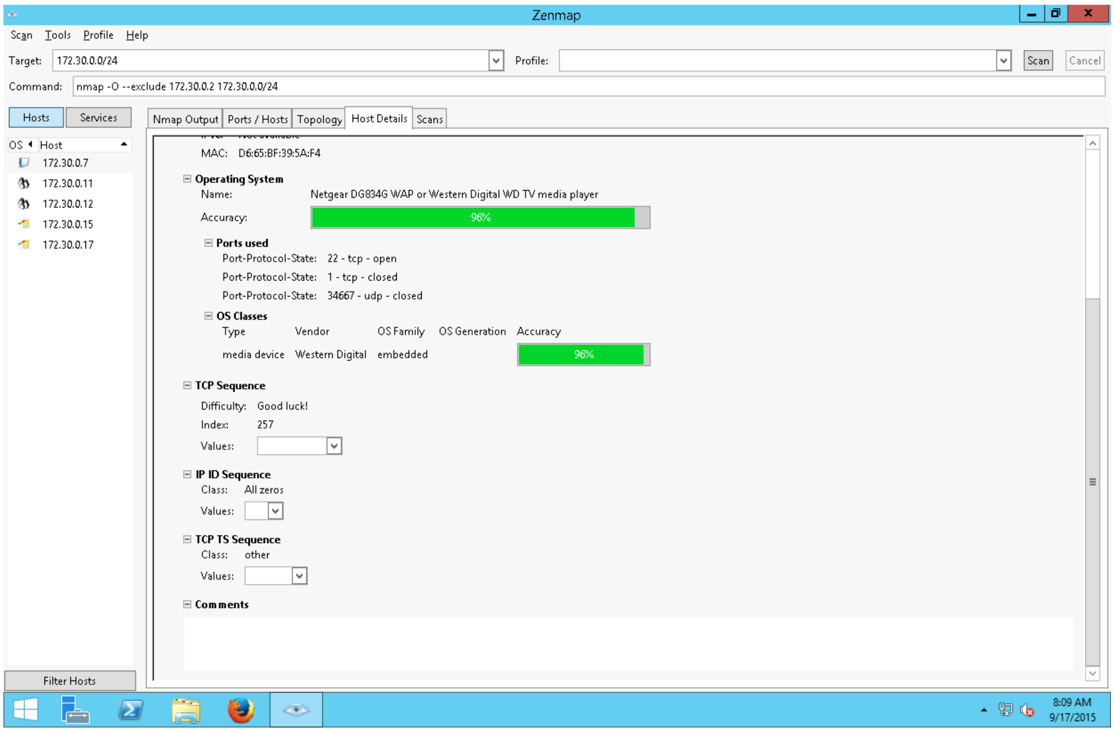


Target: 172.30.0.0/24
Profile:
Command: nmap -O --exclude 172.30.0.2 172.30.0.0/24

```
OS  Host
    172.30.0.7
    172.30.0.11
    172.30.0.12
    172.30.0.15
    172.30.0.17
```

```
172.30.0.7
  Host Status
    State:          up
    Open ports:     2
    Filtered ports: 0
    Closed ports:   998
    Scanned ports:  1000
    Up time:        2925
    Last boot:      Thu Sep 17 07:10:24 2015
  Addresses
    IPv4:  172.30.0.7
    IPv6:  Not available
    MAC:   D6:65:BF:39:5A:F4
  Operating System
    Name:      Netgear DG834G WAP or Western Digital WD TV media player
    Accuracy:  96%
    Ports used
      Port-Protocol-State:  22 - tcp - open
      Port-Protocol-State:  1 - tcp - closed
      Port-Protocol-State:  34667 - udp - closed
    OS Classes
      Type          Vendor           OS Family   OS Generation   Accuracy
      media device  Western Digital  embedded                    96%
  TCP Sequence
    Difficulty:  Good luck!
    Index:       257
    Values:
```

8:08 AM 9/17/2015



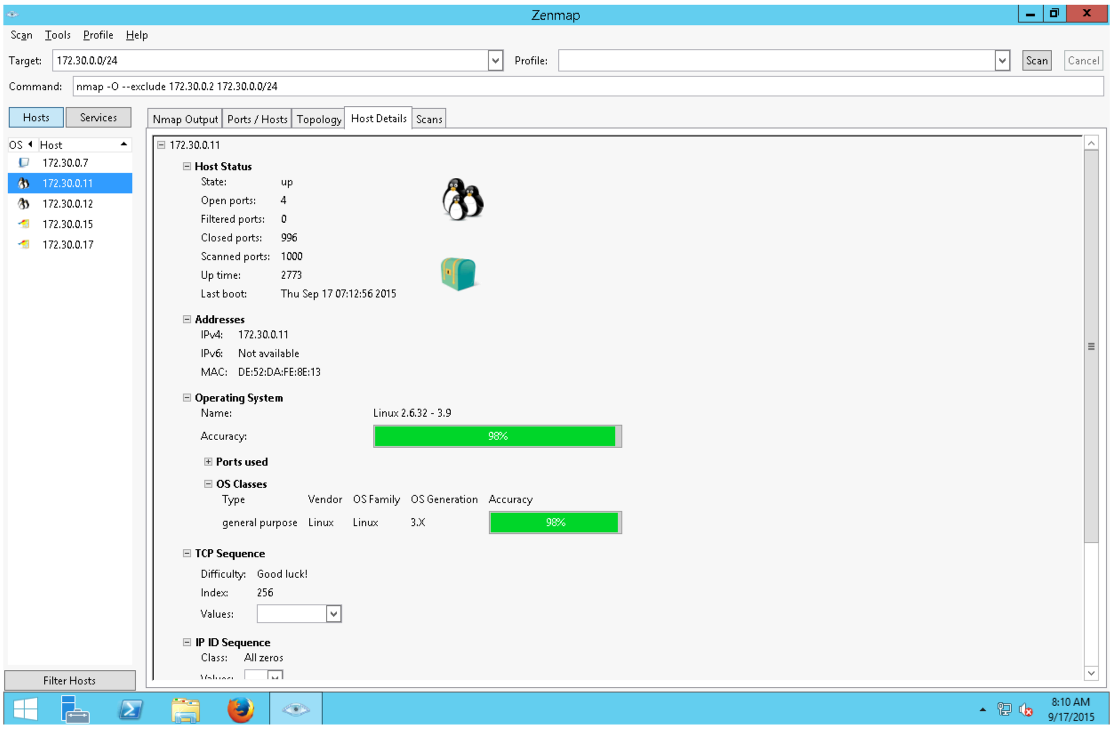
Target: 172.30.0.0/24
Profile:
Command: nmap -O --exclude 172.30.0.2 172.30.0.0/24

```
OS  Host
    172.30.0.7
    172.30.0.11
    172.30.0.12
    172.30.0.15
    172.30.0.17
```

```
    MAC:   D6:65:BF:39:5A:F4
  Operating System
    Name:      Netgear DG834G WAP or Western Digital WD TV media player
    Accuracy:  96%
    Ports used
      Port-Protocol-State:  22 - tcp - open
      Port-Protocol-State:  1 - tcp - closed
      Port-Protocol-State:  34667 - udp - closed
    OS Classes
      Type          Vendor           OS Family   OS Generation   Accuracy
      media device  Western Digital  embedded                    96%
  TCP Sequence
    Difficulty:  Good luck!
    Index:       257
    Values:
  IP ID Sequence
    Class:   All zeros
    Values:
  TCP TS Sequence
    Class:   other
    Values:
  Comments
```

8:09 AM 9/17/2015

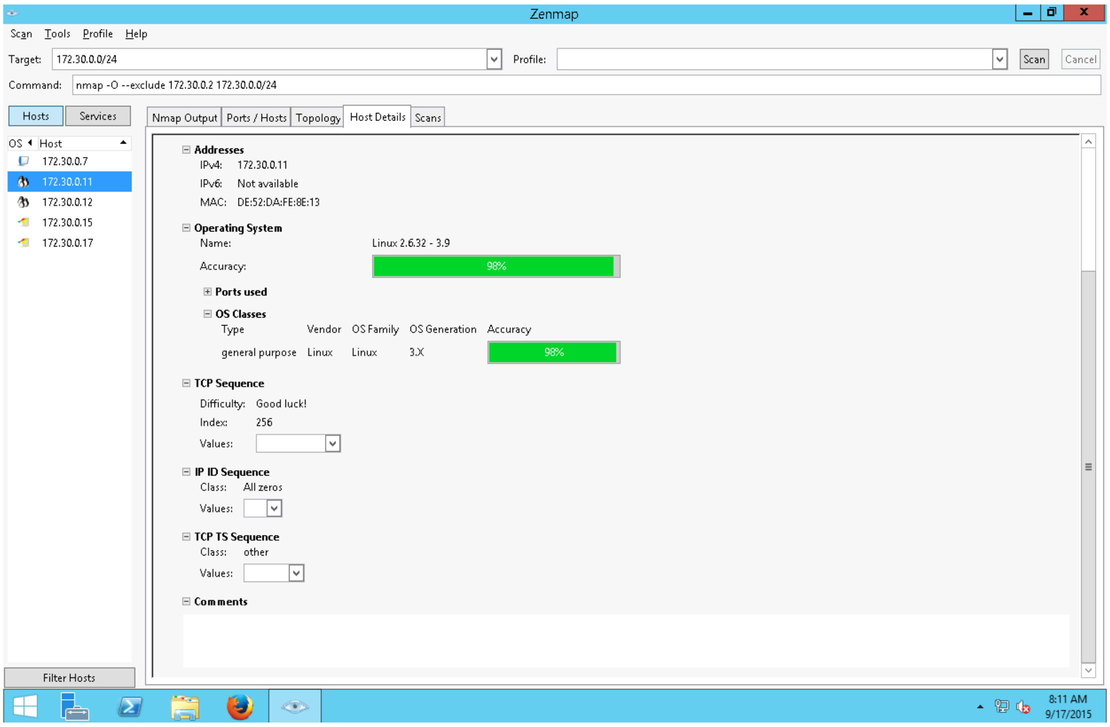
1.3 Nmap -O -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.11 hostDetails



Target: 172.30.0.0/24
Profile:
Command: nmap -O --exclude 172.30.0.2 172.30.0.0/24

172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17

```
⊟ 172.30.0.11
  ⊟ Host Status
     State:           up
     Open ports:      4
     Filtered ports:  0
     Closed ports:    996
     Scanned ports:   1000
     Up time:         2773
     Last boot:       Thu Sep 17 07:12:56 2015
  ⊟ Addresses
     IPv4:   172.30.0.11
     IPv6:   Not available
     MAC:    DE:52:DA:FE:8E:13
  ⊟ Operating System
     Name:                  Linux 2.6.32 - 3.9
     Accuracy:              98%
     ⊞ Ports used
     ⊟ OS Classes
        Type             Vendor   OS Family   OS Generation   Accuracy
        general purpose  Linux    Linux       3.X             98%
  ⊟ TCP Sequence
     Difficulty:  Good luck!
     Index:       256
     Values:
  ⊟ IP ID Sequence
     Class:   All zeros
     Values:
```

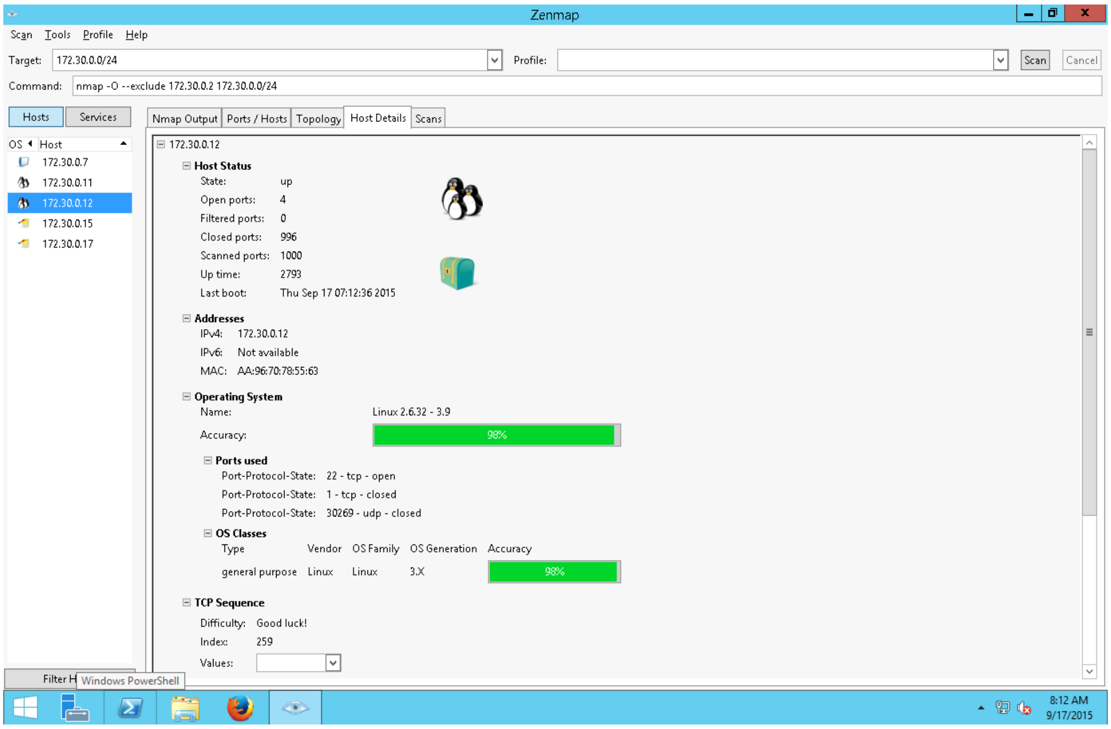


Target: 172.30.0.0/24
Profile:
Command: nmap -O --exclude 172.30.0.2 172.30.0.0/24

172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17

```
  ⊟ Addresses
     IPv4:   172.30.0.11
     IPv6:   Not available
     MAC:    DE:52:DA:FE:8E:13
  ⊟ Operating System
     Name:                  Linux 2.6.32 - 3.9
     Accuracy:              98%
     ⊞ Ports used
     ⊟ OS Classes
        Type             Vendor   OS Family   OS Generation   Accuracy
        general purpose  Linux    Linux       3.X             98%
  ⊟ TCP Sequence
     Difficulty:  Good luck!
     Index:       256
     Values:
  ⊟ IP ID Sequence
     Class:   All zeros
     Values:
  ⊟ TCP TS Sequence
     Class:   other
     Values:
  ⊟ Comments
```

1.4 Nmap -O -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.12 hostDetails



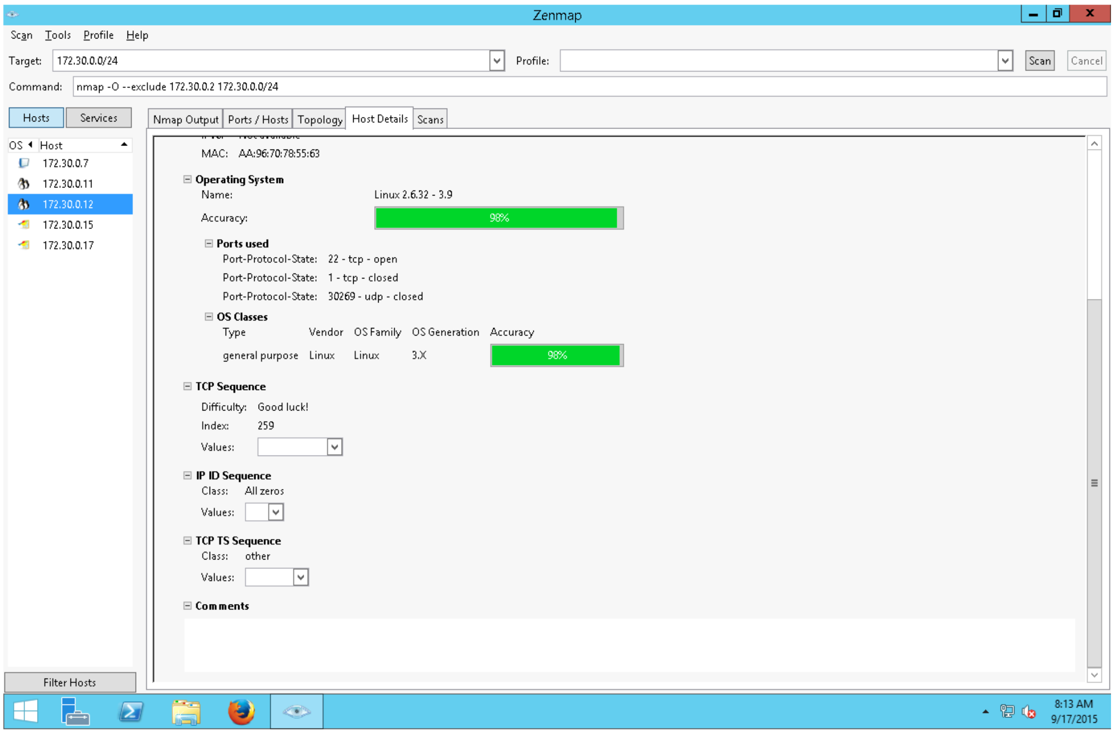
Target: 172.30.0.0/24

Profile:

Command: nmap -O --exclude 172.30.0.2 172.30.0.0/24

172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17

```
172.30.0.12
  Host Status
    State:          up
    Open ports:     4
    Filtered ports: 0
    Closed ports:   996
    Scanned ports:  1000
    Up time:        2793
    Last boot:      Thu Sep 17 07:12:36 2015
  Addresses
    IPv4:   172.30.0.12
    IPv6:   Not available
    MAC:    AA:96:70:78:55:63
  Operating System
    Name:                    Linux 2.6.32 - 3.9
    Accuracy:                98%
    Ports used
      Port-Protocol-State:  22 - tcp - open
      Port-Protocol-State:  1 - tcp - closed
      Port-Protocol-State:  30269 - udp - closed
    OS Classes
      Type             Vendor   OS Family   OS Generation   Accuracy
      general purpose  Linux    Linux       3.X             98%
  TCP Sequence
    Difficulty:  Good luck!
    Index:       259
    Values:
```



Target: 172.30.0.0/24

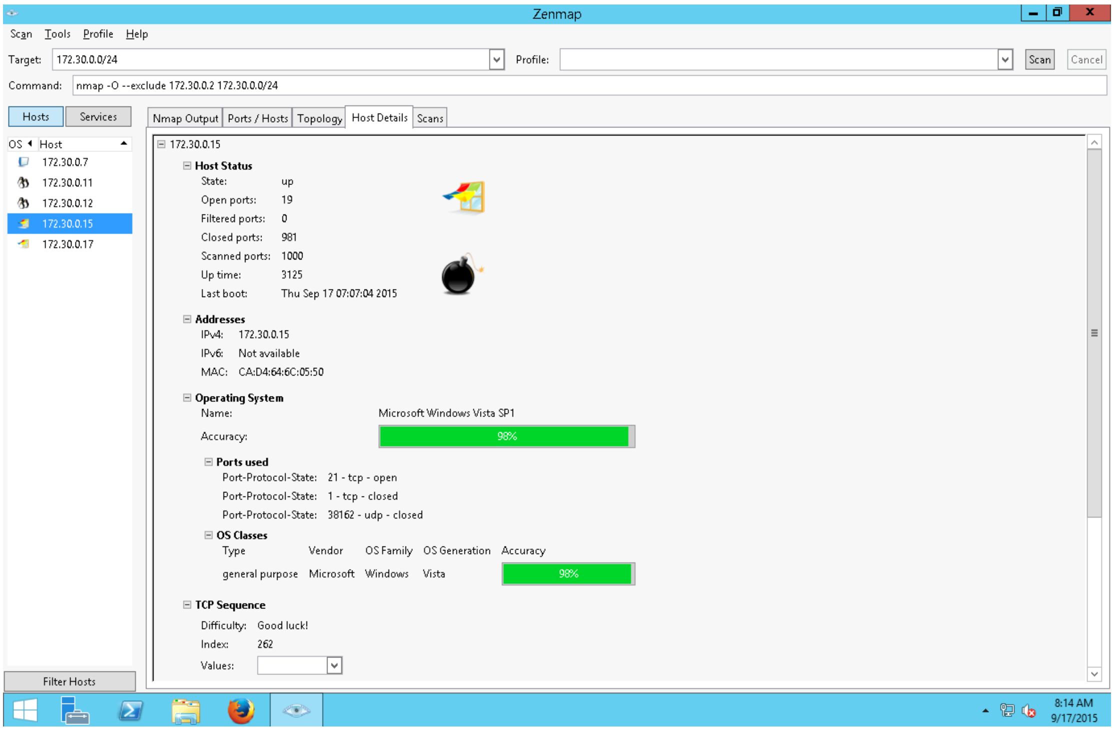
Profile:

Command: nmap -O --exclude 172.30.0.2 172.30.0.0/24

172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17

```
    MAC:    AA:96:70:78:55:63
  Operating System
    Name:                    Linux 2.6.32 - 3.9
    Accuracy:                98%
    Ports used
      Port-Protocol-State:  22 - tcp - open
      Port-Protocol-State:  1 - tcp - closed
      Port-Protocol-State:  30269 - udp - closed
    OS Classes
      Type             Vendor   OS Family   OS Generation   Accuracy
      general purpose  Linux    Linux       3.X             98%
  TCP Sequence
    Difficulty:  Good luck!
    Index:       259
    Values:
  IP ID Sequence
    Class:   All zeros
    Values:
  TCP TS Sequence
    Class:   other
    Values:
  Comments
```

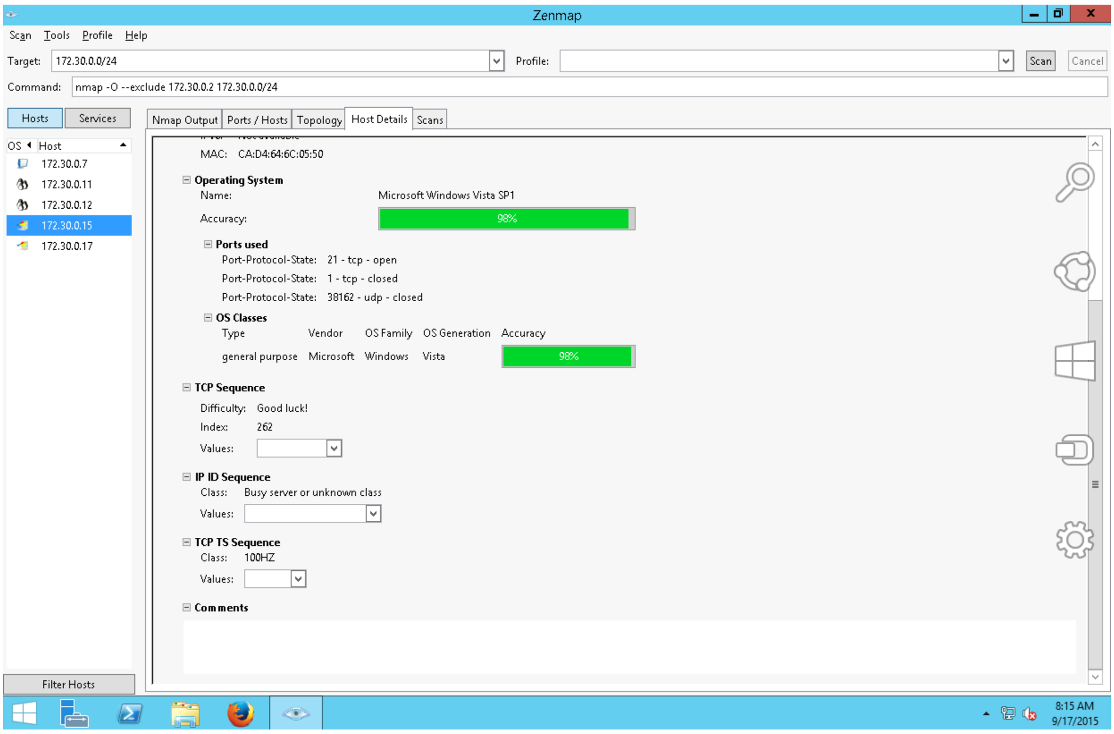
1.5 Nmap -O -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.15 hostDetails



Target: 172.30.0.0/24
Profile:
Command: nmap -O --exclude 172.30.0.2 172.30.0.0/24

172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17

```
⊟ 172.30.0.15
    ⊟ Host Status
        State:          up
        Open ports:     19
        Filtered ports: 0
        Closed ports:   981
        Scanned ports:  1000
        Up time:        3125
        Last boot:      Thu Sep 17 07:07:04 2015
    ⊟ Addresses
        IPv4:   172.30.0.15
        IPv6:   Not available
        MAC:    CA:D4:64:6C:05:50
    ⊟ Operating System
        Name:       Microsoft Windows Vista SP1
        Accuracy:   98%
        ⊟ Ports used
            Port-Protocol-State:  21 - tcp - open
            Port-Protocol-State:  1 - tcp - closed
            Port-Protocol-State:  38162 - udp - closed
        ⊟ OS Classes
            Type             Vendor     OS Family  OS Generation  Accuracy
            general purpose  Microsoft  Windows    Vista          98%
    ⊟ TCP Sequence
        Difficulty:  Good luck!
        Index:       262
        Values:
```

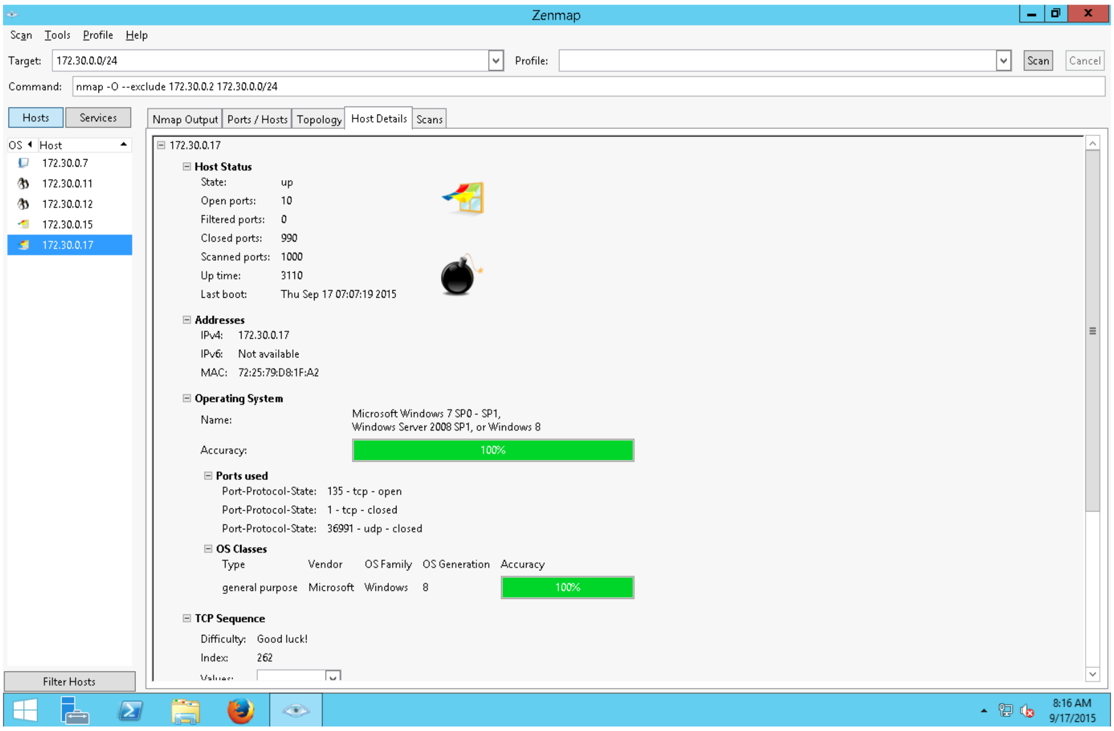


Target: 172.30.0.0/24
Profile:
Command: nmap -O --exclude 172.30.0.2 172.30.0.0/24

172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17

```
        MAC:    CA:D4:64:6C:05:50
    ⊟ Operating System
        Name:       Microsoft Windows Vista SP1
        Accuracy:   98%
        ⊟ Ports used
            Port-Protocol-State:  21 - tcp - open
            Port-Protocol-State:  1 - tcp - closed
            Port-Protocol-State:  38162 - udp - closed
        ⊟ OS Classes
            Type             Vendor     OS Family  OS Generation  Accuracy
            general purpose  Microsoft  Windows    Vista          98%
    ⊟ TCP Sequence
        Difficulty:  Good luck!
        Index:       262
        Values:
    ⊟ IP ID Sequence
        Class:   Busy server or unknown class
        Values:
    ⊟ TCP TS Sequence
        Class:   100HZ
        Values:
    ⊟ Comments
```

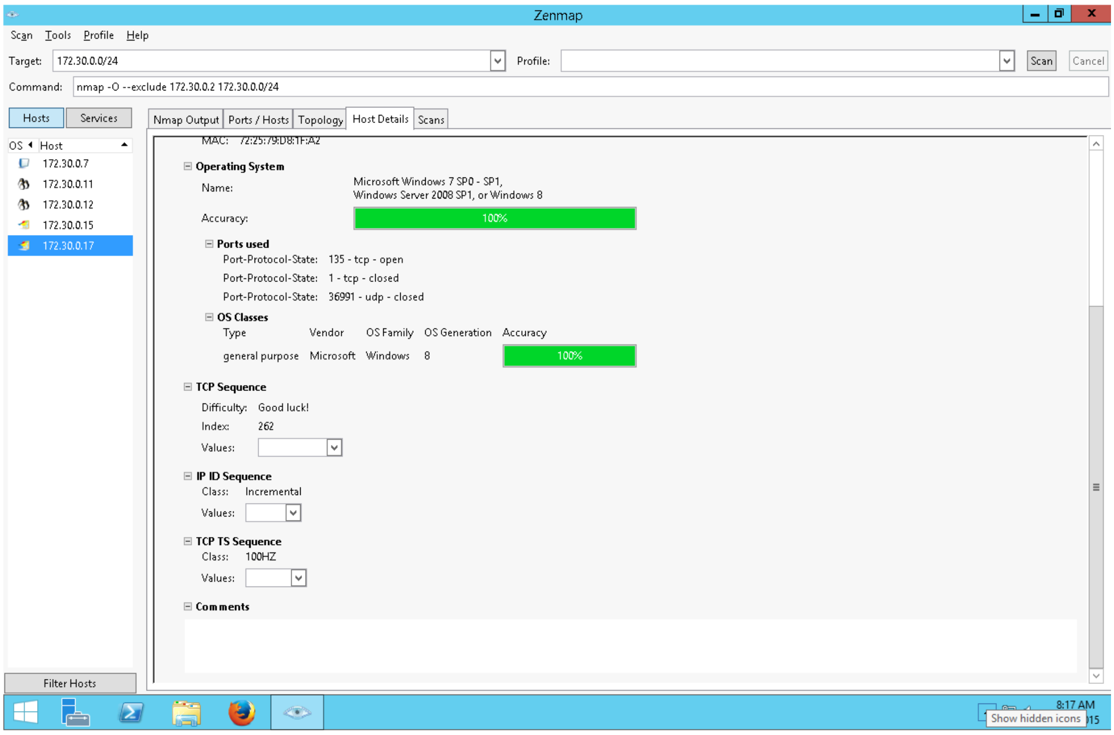
1.6 Nmap -O -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.17 hostDetails



Target: 172.30.0.0/24
Profile:
Command: nmap -O --exclude 172.30.0.2 172.30.0.0/24

172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17

```
⊟ 172.30.0.17
  ⊟ Host Status
     State:          up
     Open ports:     10
     Filtered ports: 0
     Closed ports:   990
     Scanned ports:  1000
     Up time:        3110
     Last boot:      Thu Sep 17 07:07:19 2015
  ⊟ Addresses
     IPv4:  172.30.0.17
     IPv6:  Not available
     MAC:   72:25:79:D8:1F:A2
  ⊟ Operating System
     Name:                   Microsoft Windows 7 SP0 - SP1,
                             Windows Server 2008 SP1, or Windows 8
     Accuracy:               100%
    ⊟ Ports used
       Port-Protocol-State:  135 - tcp - open
       Port-Protocol-State:  1 - tcp - closed
       Port-Protocol-State:  36991 - udp - closed
    ⊟ OS Classes
       Type             Vendor     OS Family  OS Generation  Accuracy
       general purpose  Microsoft  Windows    8              100%
  ⊟ TCP Sequence
     Difficulty:  Good luck!
     Index:       262
     Values:
```

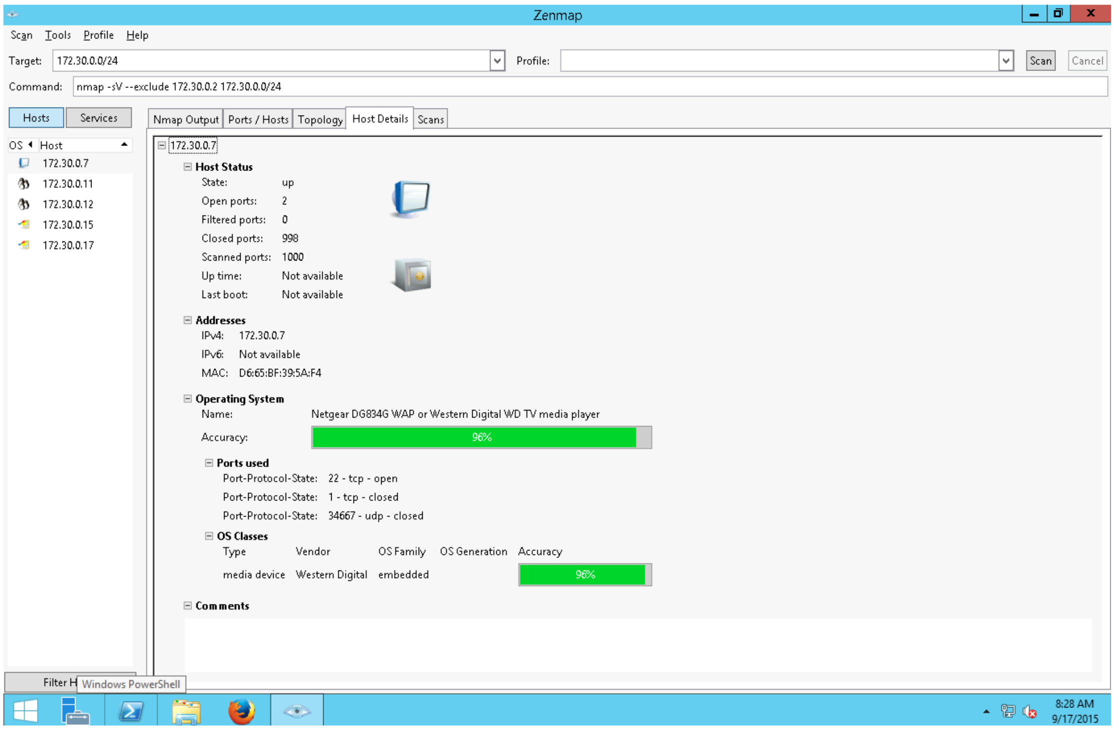


Target: 172.30.0.0/24
Profile:
Command: nmap -O --exclude 172.30.0.2 172.30.0.0/24

172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17

```
     MAC:   72:25:79:D8:1F:A2
  ⊟ Operating System
     Name:                   Microsoft Windows 7 SP0 - SP1,
                             Windows Server 2008 SP1, or Windows 8
     Accuracy:               100%
    ⊟ Ports used
       Port-Protocol-State:  135 - tcp - open
       Port-Protocol-State:  1 - tcp - closed
       Port-Protocol-State:  36991 - udp - closed
    ⊟ OS Classes
       Type             Vendor     OS Family  OS Generation  Accuracy
       general purpose  Microsoft  Windows    8              100%
  ⊟ TCP Sequence
     Difficulty:  Good luck!
     Index:       262
     Values:
  ⊟ IP ID Sequence
     Class:   Incremental
     Values:
  ⊟ TCP TS Sequence
     Class:   100HZ
     Values:
  ⊟ Comments
```

1.7 Nmap -sV -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.07 hostDetails



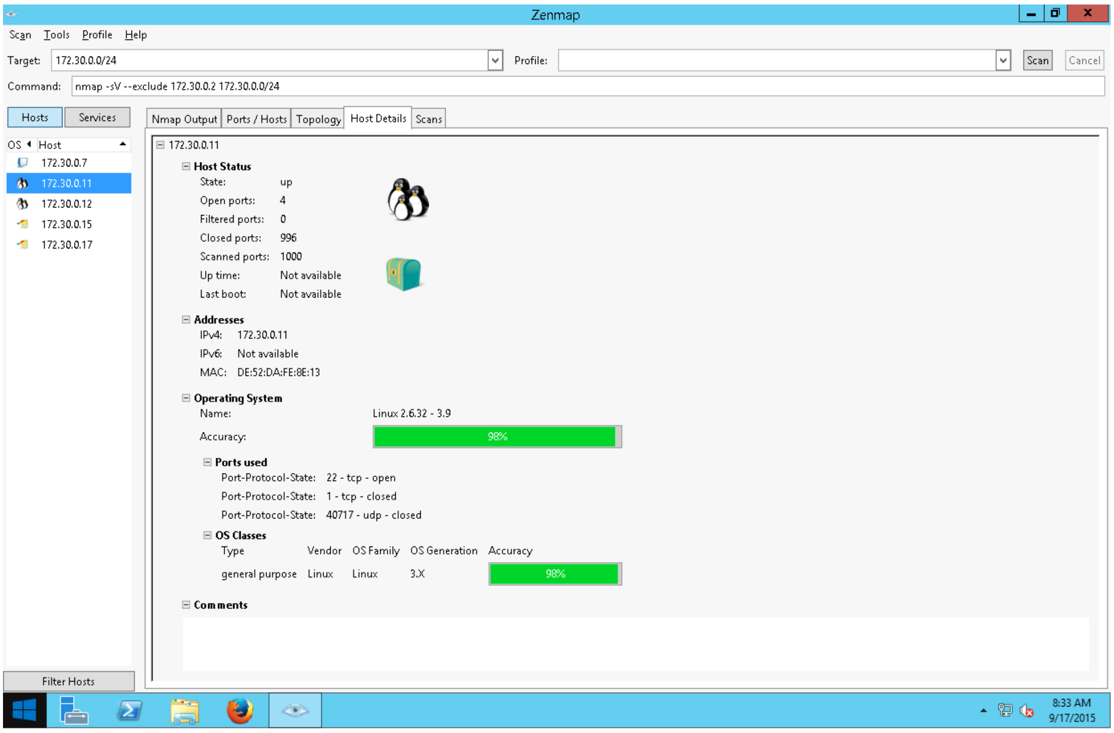
Target: 172.30.0.0/24

Command: nmap -sV --exclude 172.30.0.2 172.30.0.0/24

172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17

```
172.30.0.7
  Host Status
    State:          up
    Open ports:     2
    Filtered ports: 0
    Closed ports:   998
    Scanned ports:  1000
    Up time:        Not available
    Last boot:      Not available
  Addresses
    IPv4:   172.30.0.7
    IPv6:   Not available
    MAC:    D6:65:BF:39:5A:F4
  Operating System
    Name:      Netgear DG834G WAP or Western Digital WD TV media player
    Accuracy:  96%
    Ports used
      Port-Protocol-State:  22 - tcp - open
      Port-Protocol-State:  1 - tcp - closed
      Port-Protocol-State:  34667 - udp - closed
    OS Classes
      Type          Vendor           OS Family   OS Generation   Accuracy
      media device  Western Digital  embedded                    96%
  Comments
```

1.8 Nmap -sV -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.11 hostDetails



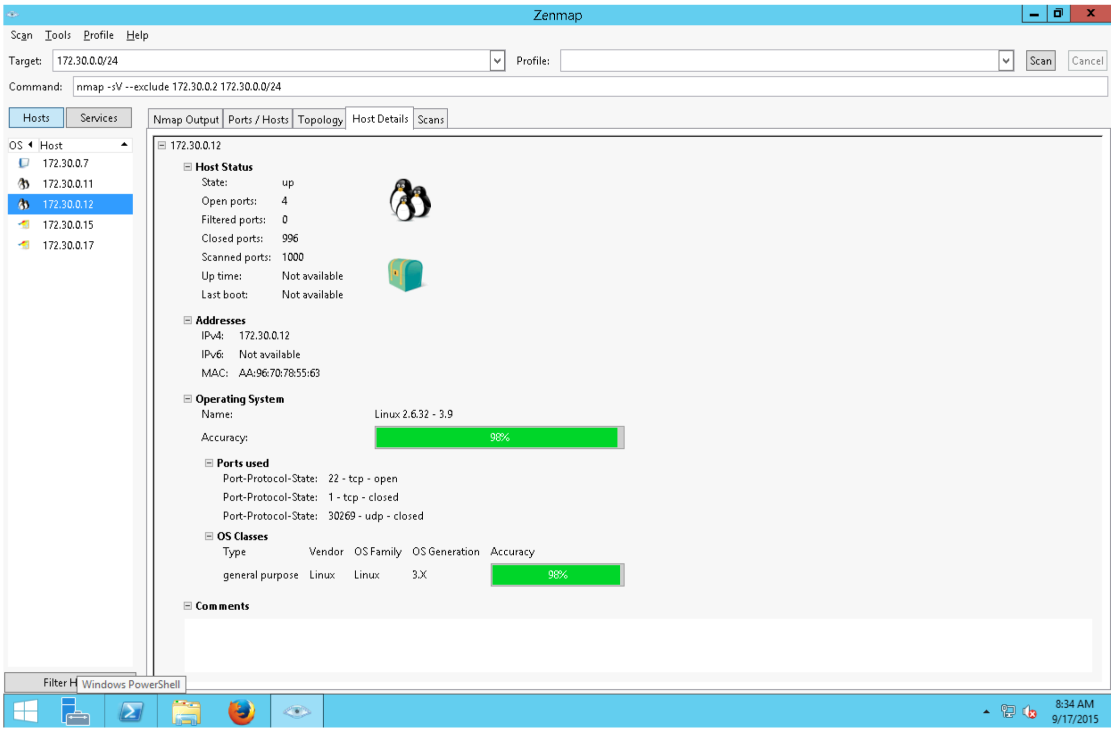
Target: 172.30.0.0/24

Command: nmap -sV --exclude 172.30.0.2 172.30.0.0/24

172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17

```
172.30.0.11
  Host Status
    State:          up
    Open ports:     4
    Filtered ports: 0
    Closed ports:   996
    Scanned ports:  1000
    Up time:        Not available
    Last boot:      Not available
  Addresses
    IPv4:   172.30.0.11
    IPv6:   Not available
    MAC:    DE:52:DA:FE:8E:13
  Operating System
    Name:      Linux 2.6.32 - 3.9
    Accuracy:  98%
    Ports used
      Port-Protocol-State:  22 - tcp - open
      Port-Protocol-State:  1 - tcp - closed
      Port-Protocol-State:  40717 - udp - closed
    OS Classes
      Type             Vendor  OS Family  OS Generation  Accuracy
      general purpose  Linux   Linux      3.X            98%
  Comments
```

1.9 Nmap -sV -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.12 hostDetails



Target: 172.30.0.0/24

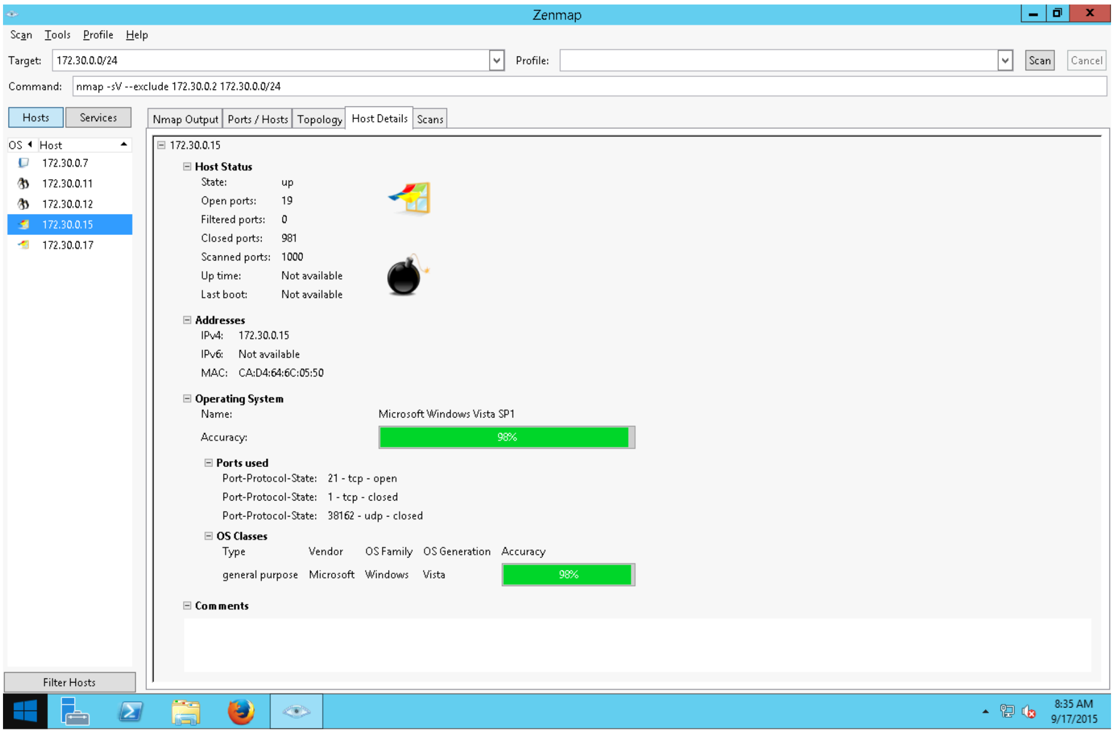
Profile:

Command: nmap -sV --exclude 172.30.0.2 172.30.0.0/24

```
172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17
```

```
172.30.0.12
  Host Status
    State:          up
    Open ports:     4
    Filtered ports: 0
    Closed ports:   996
    Scanned ports:  1000
    Up time:        Not available
    Last boot:      Not available
  Addresses
    IPv4:  172.30.0.12
    IPv6:  Not available
    MAC:   AA:96:70:78:55:63
  Operating System
    Name:      Linux 2.6.32 - 3.9
    Accuracy:  98%
    Ports used
      Port-Protocol-State:  22 - tcp - open
      Port-Protocol-State:  1 - tcp - closed
      Port-Protocol-State:  30269 - udp - closed
    OS Classes
      Type             Vendor  OS Family  OS Generation  Accuracy
      general purpose  Linux   Linux      3.X            98%
  Comments
```

1.10 Nmap -sV -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.15 hostDetails



Target: 172.30.0.0/24

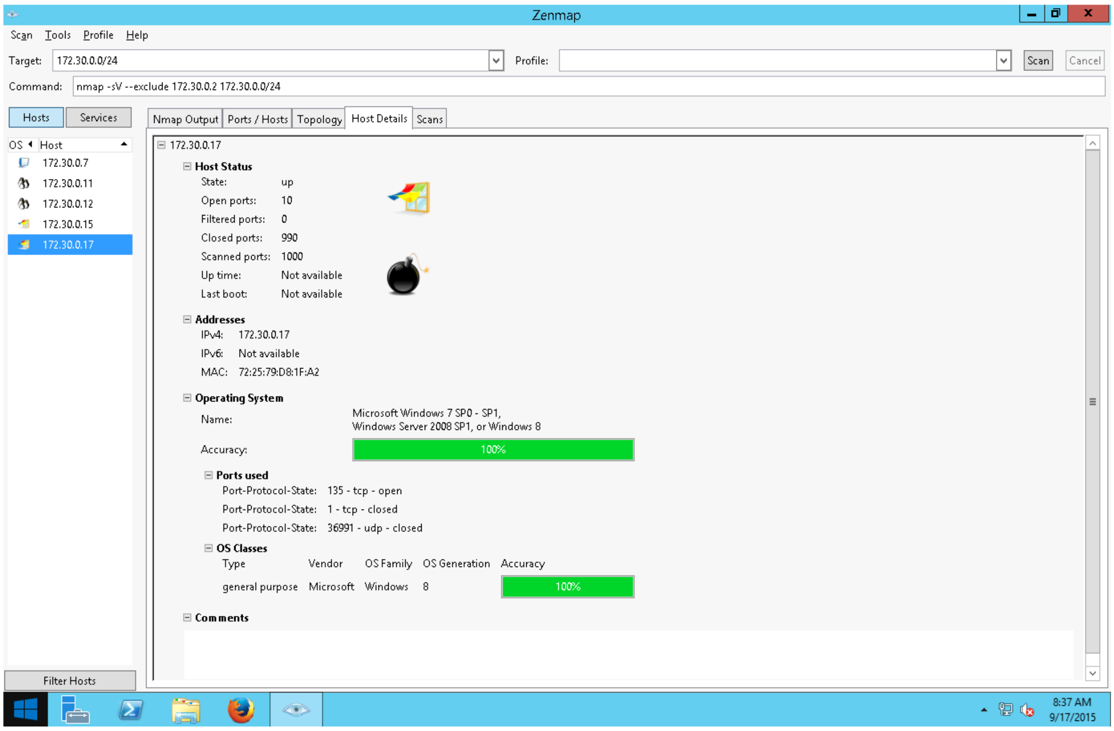
Profile:

Command: nmap -sV --exclude 172.30.0.2 172.30.0.0/24

```
172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17
```

```
172.30.0.15
  Host Status
    State:          up
    Open ports:     19
    Filtered ports: 0
    Closed ports:   981
    Scanned ports:  1000
    Up time:        Not available
    Last boot:      Not available
  Addresses
    IPv4:  172.30.0.15
    IPv6:  Not available
    MAC:   CA:D4:64:6C:05:50
  Operating System
    Name:      Microsoft Windows Vista SP1
    Accuracy:  98%
    Ports used
      Port-Protocol-State:  21 - tcp - open
      Port-Protocol-State:  1 - tcp - closed
      Port-Protocol-State:  38162 - udp - closed
    OS Classes
      Type             Vendor     OS Family  OS Generation  Accuracy
      general purpose  Microsoft  Windows    Vista          98%
  Comments
```

1.11 Nmap -sV -exclude 172.30.0.2 172.30.0.0/24 -> 172.30.0.17 hostDetails



Target: 172.30.0.0/24

Profile:

Command: nmap -sV --exclude 172.30.0.2 172.30.0.0/24

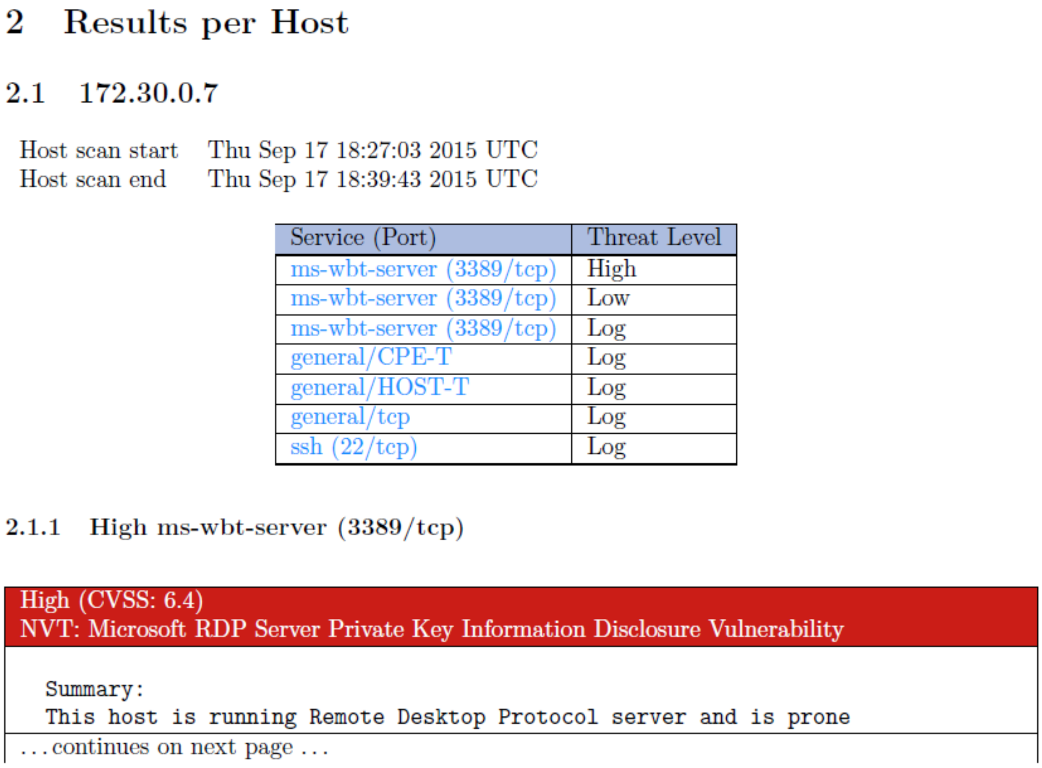
```
172.30.0.7
172.30.0.11
172.30.0.12
172.30.0.15
172.30.0.17
```

```
⊟ 172.30.0.17
    ⊟ Host Status
        State:           up
        Open ports:      10
        Filtered ports:  0
        Closed ports:    990
        Scanned ports:   1000
        Up time:         Not available
        Last boot:       Not available

    ⊟ Addresses
        IPv4:   172.30.0.17
        IPv6:   Not available
        MAC:    72:25:79:D8:1F:A2

    ⊟ Operating System
        Name:                       Microsoft Windows 7 SP0 - SP1,
                                    Windows Server 2008 SP1, or Windows 8
        Accuracy:                   100%

        ⊟ Ports used
            Port-Protocol-State:   135 - tcp - open
            Port-Protocol-State:   1 - tcp - closed
            Port-Protocol-State:   36991 - udp - closed
        ⊟ OS Classes
            Type             Vendor      OS Family   OS Generation   Accuracy
            general purpose  Microsoft   Windows     8               100%

    ⊟ Comments
```

2. OpenVAS high level vulnerability report analysis

2.1 Microsoft RDP Server Private Key Information Disclosure Vulnerability

2.1.1 172.30.0.7 High Vulnerability



2 Results per Host

2.1 172.30.0.7

Host scan start Thu Sep 17 18:27:03 2015 UTC
Host scan end Thu Sep 17 18:39:43 2015 UTC

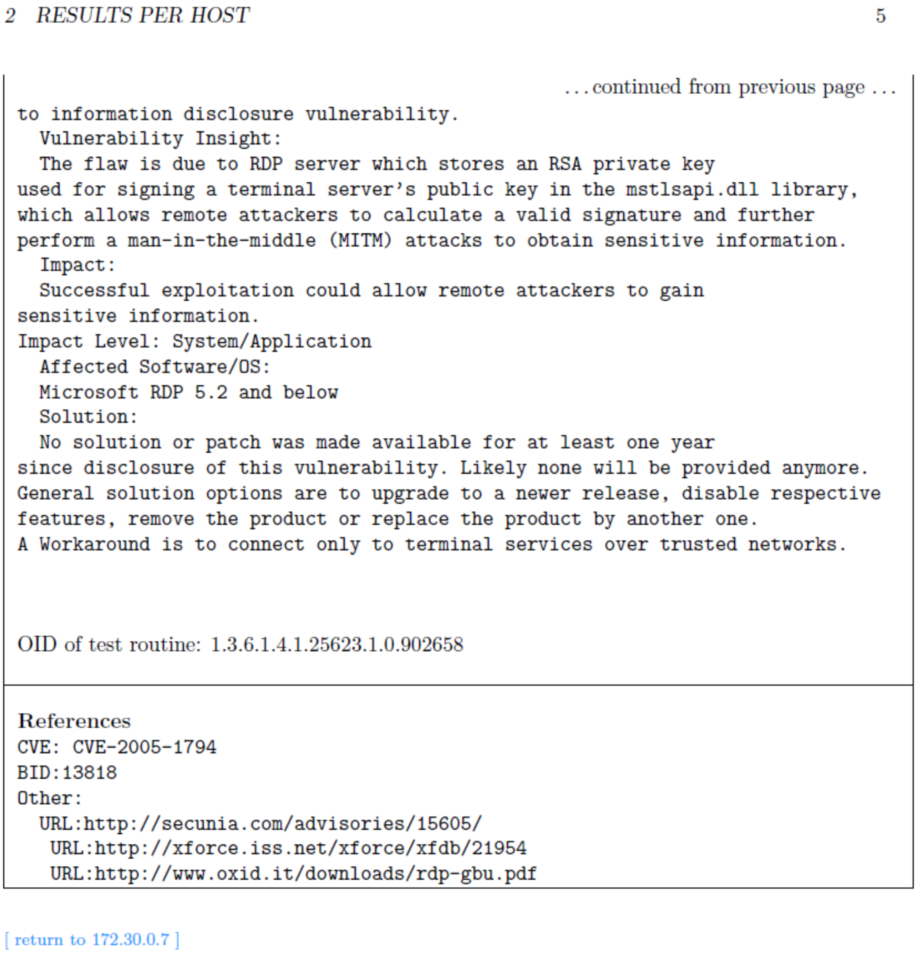
Service (Port)	Threat Level
ms-wbt-server (3389/tcp)	High
ms-wbt-server (3389/tcp)	Low
ms-wbt-server (3389/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/tcp	Log
ssh (22/tcp)	Log

2.1.1 High ms-wbt-server (3389/tcp)

High (CVSS: 6.4)
NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability

```
Summary:
This host is running Remote Desktop Protocol server and is prone
```

. . . continues on next page . . .



2 RESULTS PER HOST 5

. . . continued from previous page . . .

```
to information disclosure vulnerability.
  Vulnerability Insight:
  The flaw is due to RDP server which stores an RSA private key
used for signing a terminal server's public key in the mstlsapi.dll library,
which allows remote attackers to calculate a valid signature and further
perform a man-in-the-middle (MITM) attacks to obtain sensitive information.
  Impact:
  Successful exploitation could allow remote attackers to gain
sensitive information.
Impact Level: System/Application
  Affected Software/OS:
  Microsoft RDP 5.2 and below
  Solution:
  No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.
A Workaround is to connect only to terminal services over trusted networks.
```

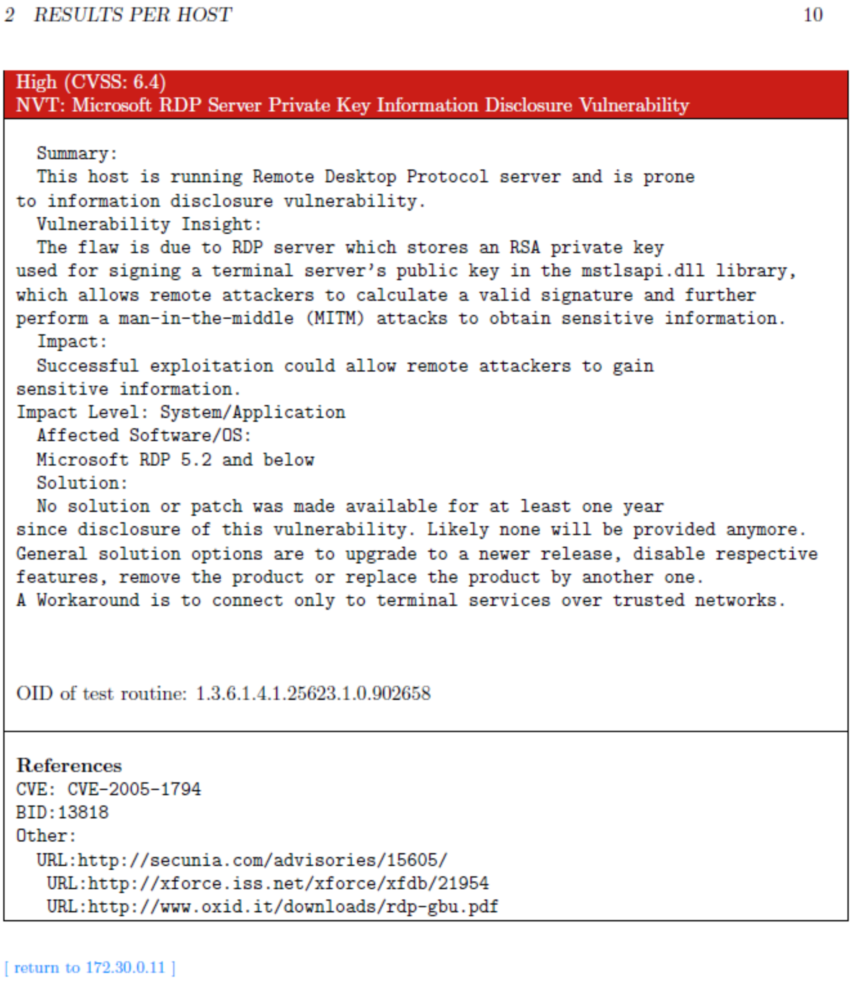
OID of test routine: 1.3.6.1.4.1.25623.1.0.902658

References

```
CVE: CVE-2005-1794
BID:13818
Other:
  URL:http://secunia.com/advisories/15605/
   URL:http://xforce.iss.net/xforce/xfdb/21954
   URL:http://www.oxid.it/downloads/rdp-gbu.pdf
```

[return to 172.30.0.7]

2.1.2 172.30.0.11 High Vulnerability



2 RESULTS PER HOST 10

High (CVSS: 6.4)
NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability

```
  Summary:
  This host is running Remote Desktop Protocol server and is prone
to information disclosure vulnerability.
  Vulnerability Insight:
  The flaw is due to RDP server which stores an RSA private key
used for signing a terminal server's public key in the mstlsapi.dll library,
which allows remote attackers to calculate a valid signature and further
perform a man-in-the-middle (MITM) attacks to obtain sensitive information.
  Impact:
  Successful exploitation could allow remote attackers to gain
sensitive information.
Impact Level: System/Application
  Affected Software/OS:
  Microsoft RDP 5.2 and below
  Solution:
  No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.
A Workaround is to connect only to terminal services over trusted networks.
```

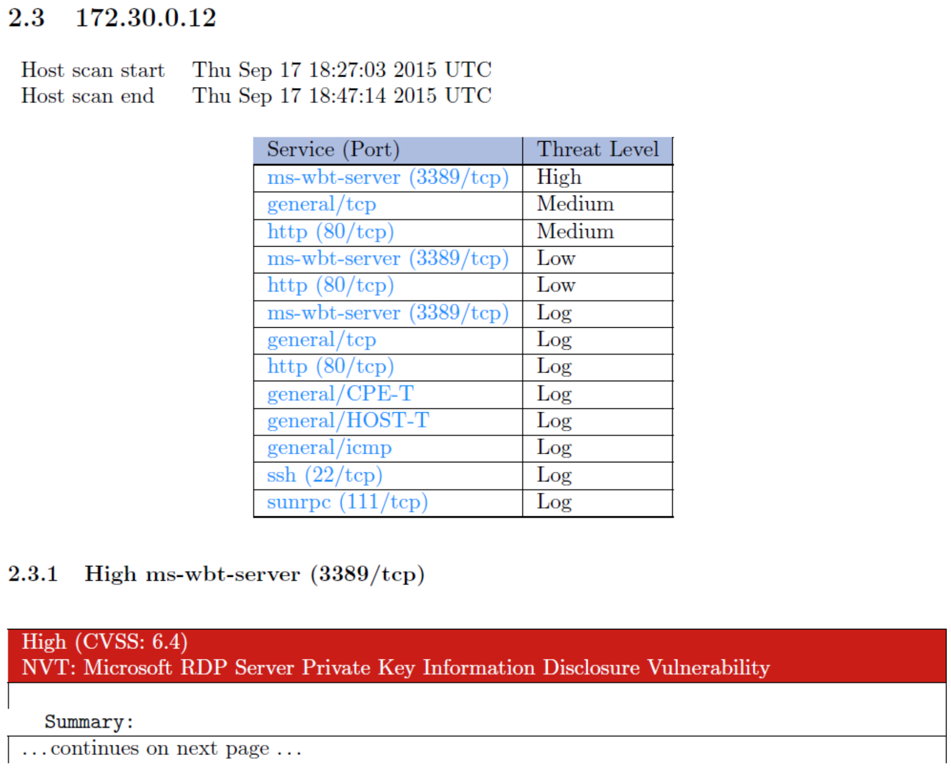
OID of test routine: 1.3.6.1.4.1.25623.1.0.902658

References

```
CVE: CVE-2005-1794
BID:13818
Other:
  URL:http://secunia.com/advisories/15605/
   URL:http://xforce.iss.net/xforce/xfdb/21954
   URL:http://www.oxid.it/downloads/rdp-gbu.pdf
```

[return to 172.30.0.11]

2.1.3 172.30.0.12 High Vulnerability



2.3 172.30.0.12

Host scan start	Thu Sep 17 18:27:03 2015 UTC
Host scan end	Thu Sep 17 18:47:14 2015 UTC

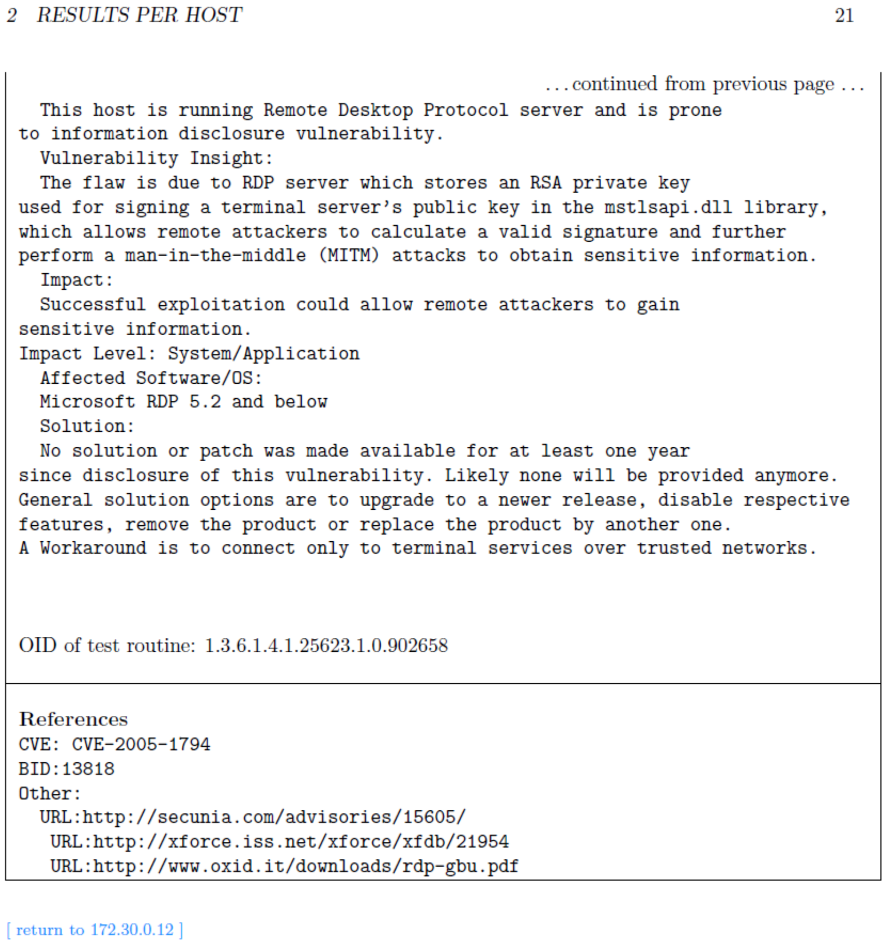
Service (Port)	Threat Level
ms-wbt-server (3389/tcp)	High
general/tcp	Medium
http (80/tcp)	Medium
ms-wbt-server (3389/tcp)	Low
http (80/tcp)	Low
ms-wbt-server (3389/tcp)	Log
general/tcp	Log
http (80/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log
ssh (22/tcp)	Log
sunrpc (111/tcp)	Log

2.3.1 High ms-wbt-server (3389/tcp)

High (CVSS: 6.4)
NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability

```
  Summary:
```

. . . continues on next page . . .



2 RESULTS PER HOST 21

...continued from previous page ...

```
  This host is running Remote Desktop Protocol server and is prone
to information disclosure vulnerability.
  Vulnerability Insight:
  The flaw is due to RDP server which stores an RSA private key
used for signing a terminal server's public key in the mstlsapi.dll library,
which allows remote attackers to calculate a valid signature and further
perform a man-in-the-middle (MITM) attacks to obtain sensitive information.
  Impact:
  Successful exploitation could allow remote attackers to gain
sensitive information.
Impact Level: System/Application
  Affected Software/OS:
  Microsoft RDP 5.2 and below
  Solution:
  No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.
A Workaround is to connect only to terminal services over trusted networks.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902658

References

```
CVE: CVE-2005-1794
BID:13818
Other:
  URL:http://secunia.com/advisories/15605/
   URL:http://xforce.iss.net/xforce/xfdb/21954
   URL:http://www.oxid.it/downloads/rdp-gbu.pdf
```

[return to 172.30.0.12]

2.1.4 Description and Recommendation

Vulnerabilities descriptions summary:

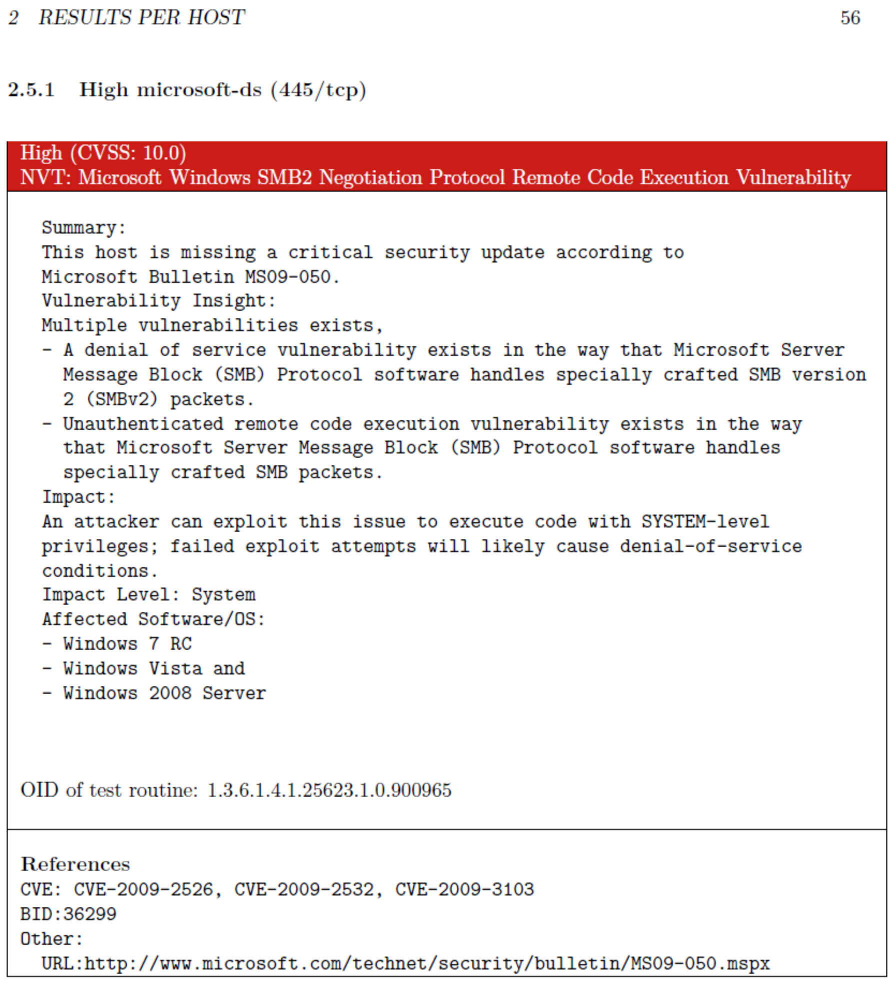
The type of the discovered vulnerabilities of the three hosts, 172.30.0.7, 172.30.0.11, 172.30.0.12 is the same – Microsoft RDP Server Private Key Information Disclosure Vulnerability. And, this kind of vulnerability happens at port 3389 which is using TCP protocol to communicate. The major danger of 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.

2.2 Microsoft Windows SMB2 Negotiation Protocol Remote code Execution

2.2.1 172.30.0.17 High Vulnerability



2 RESULTS PER HOST 56

2.5.1 High microsoft-ds (445/tcp)

High (CVSS: 10.0)
NVT: Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability

```
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS09-050.
Vulnerability Insight:
Multiple vulnerabilities exists,
- A denial of service vulnerability exists in the way that Microsoft Server
  Message Block (SMB) Protocol software handles specially crafted SMB version
  2 (SMBv2) packets.
- Unauthenticated remote code execution vulnerability exists in the way
  that Microsoft Server Message Block (SMB) Protocol software handles
  specially crafted SMB packets.
Impact:
An attacker can exploit this issue to execute code with SYSTEM-level
privileges; failed exploit attempts will likely cause denial-of-service
conditions.
Impact Level: System
Affected Software/OS:
- Windows 7 RC
- Windows Vista and
- Windows 2008 Server
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900965

References

```
CVE: CVE-2009-2526, CVE-2009-2532, CVE-2009-3103
BID:36299
Other:
  URL:http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx
```

2.2.2 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.

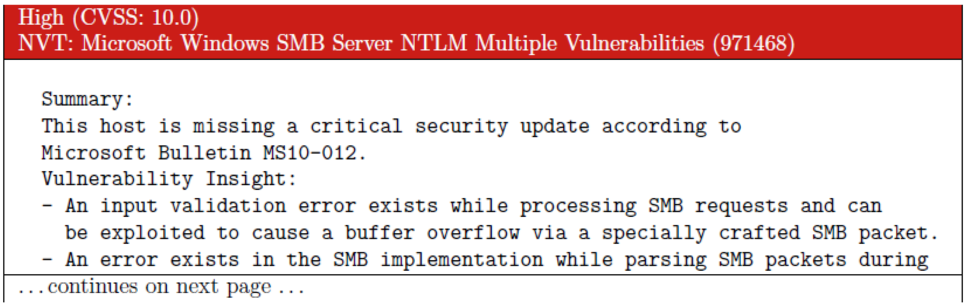
Recommendation:

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

2.3 Microsoft Windows SMB Server NTLM Multiple Vulnerability

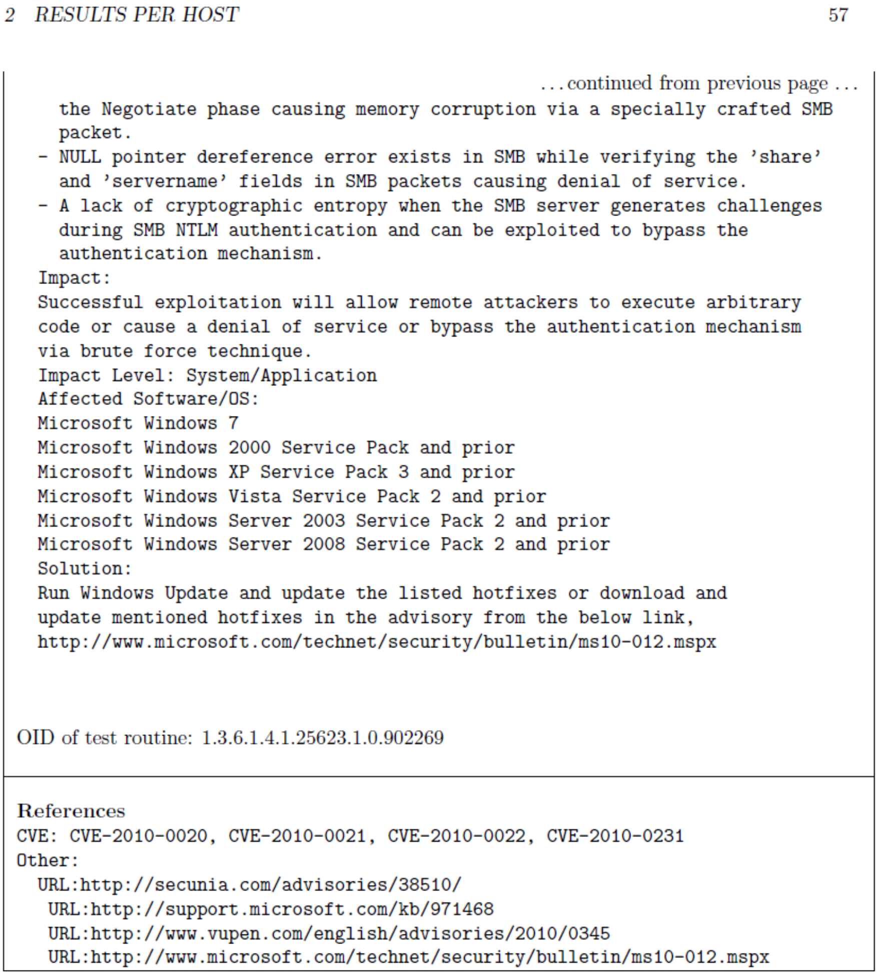
2.3.1 172.30.0.17 High Vulnerability



High (CVSS: 10.0)
NVT: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

```
Summary:
This host is missing a critical security update according to
Microsoft Bulletin MS10-012.
Vulnerability Insight:
- An input validation error exists while processing SMB requests and can
  be exploited to cause a buffer overflow via a specially crafted SMB packet.
- An error exists in the SMB implementation while parsing SMB packets during
```

. . . continues on next page . . .



2 RESULTS PER HOST 57

. . . continued from previous page . . .

```
  the Negotiate phase causing memory corruption via a specially crafted SMB
  packet.
- NULL pointer dereference error exists in SMB while verifying the 'share'
  and 'servername' fields in SMB packets causing denial of service.
- A lack of cryptographic entropy when the SMB server generates challenges
  during SMB NTLM authentication and can be exploited to bypass the
  authentication mechanism.
Impact:
Successful exploitation will allow remote attackers to execute arbitrary
code or cause a denial of service or bypass the authentication mechanism
via brute force technique.
Impact Level: System/Application
Affected Software/OS:
Microsoft Windows 7
Microsoft Windows 2000 Service Pack and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2003 Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior
Solution:
Run Windows Update and update the listed hotfixes or download and
update mentioned hotfixes in the advisory from the below link,
http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902269

References

```
CVE: CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231
Other:
  URL:http://secunia.com/advisories/38510/
   URL:http://support.microsoft.com/kb/971468
   URL:http://www.vupen.com/english/advisories/2010/0345
   URL:http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx
```

2.3.2 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.

3. 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