


## Tenable Nessus Security Report


**Start Time:** Tue Jun 20 23:08:53 2006


**Finish Time:** Tue Jun 20 23:21:56 2006

### 192.168.10.0/24

 [192.168.10.1](#) 4 Open Ports, 12 Notes, 1 Warnings, 0 Holes.

 [192.168.10.3](#) 0 Open Ports, 2 Notes, 0 Warnings, 0 Holes.


 [192.168.10.130](#) 0 Open Ports, 2 Notes, 0 Warnings, 0 Holes.


 [192.168.10.145](#) 0 Open Ports, 3 Notes, 0 Warnings, 0 Holes.

### 192.168.10.1

[\[Return to top\]](#)

**domain**  
(53/tcp)

 Port is open  
Plugin ID : [11219](#)

 A DNS server is running on this port. If you do not use it, disable it.

**Risk Factor :** Low  
Plugin ID : [11002](#)

 **Synopsis :**

It is possible to obtain the version number of the remote DNS server.

**Description :**

The remote host is running BIND, an open-source DNS server. It is possible to extract the version number of the remote installation by sending a special DNS request for the text 'version.bind' in the domain 'chaos'.

**Solution:**

It is possible to hide the version number of bind by using the 'version' directive in the 'options' section in named.conf

**Risk Factor :**

None

**Plugin output:**

The version of the remote BIND server is : dnsmasq-2.27  
Plugin ID : [10028](#)

**domain**  
(53/udp)



**Synopsis :**

The remote name server allows recursive queries to be performed by the host running nssud.

**Description :**

It is possible to query the remote name server for third party names.

If this is your internal nameserver, then forget this warning.

If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as [www.nessus.org](http://www.nessus.org)). This allows hackers to do cache poisoning attacks against this nameserver.

If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.

**See Also :**

<http://www.cert.org/advisories/CA-1997-22.html>

**Solution:**

Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).

If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf

If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command

Then, within the options block, you can explicitly state:  
'allow-recursion { hosts\_defined\_in\_acl }'

For more info on Bind 9 administration (to include recursion), see:  
<http://www.nominum.com/content/documents/bind9arm.pdf>

If you are using another name server, consult its documentation.

**Risk Factor :**

Medium / CVSS Base Score : 4  
(AV:R/AC:L/Au:NR/C:N/A:N/I:P/B:I)  
CVE : CVE-1999-0024  
BID : 136, 678  
Plugin ID : [10539](#)


be able to use this attack to build a statistical model regarding company usage of aforementioned financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more...

For a much more detailed discussion of the potential risks of allowing DNS cache information to be queried anonymously, please see:

[http://community.sidestep.pt/~luis/DNS-Cache-Snooping/DNS\\_Cache\\_Snooping\\_1.1.pdf](http://community.sidestep.pt/~luis/DNS-Cache-Snooping/DNS_Cache_Snooping_1.1.pdf)


**Risk Factor :**

Low / CVSS Base Score : 2  
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)  
Plugin ID : [12217](#)

 A DNS server is running on this port. If you do not use it, disable it.

**Risk Factor :** Low

Plugin ID : [11002](#)

 Nessus was not able to reliable identify the remote DNS server type.

It might be :

Microsoft Windows 2000 Name Server


ISC BIND 8.4

The fingerprint differs from these known signatures on 2 points.

If you know which DNS server this host is actually running, please send this signature to [dns-signatures@nessus.org](mailto:dns-signatures@nessus.org) :


1q:2:2:1q:2:1q:1q:1q:1q:0TC:0AAXD:0X:0X:0Z0X:0X:0Z2X:4q:4q:4q:0X:0X:2:0AAXD:  
Plugin ID : [11951](#)

**general/udp**

 For your information, here is the traceroute from 192.168.182.122 to 192.168.10.1  
:  
192.168.182.122  
192.168.10.1


Plugin ID : [10287](#)

**ssh (22/tcp)**

 Remote SSH version : SSH-2.0-dropbear\_0.48

Remote SSH supported authentication : publickey,password


Plugin ID : [10267](#)

 The remote SSH daemon supports the following versions of the SSH protocol :

. 1.99  
. 2.0

Plugin ID : [10881](#)

**general/tcp**


 Nessus was not able to reliably identify the remote operating system. It might be:  
Netilla Service Platform 4.0

The fingerprint differs from these known signatures on 2 points.

If you know what operating system this host is running, please send this signature to [os-signatures@nessus.org](mailto:os-signatures@nessus.org) :


:0:1:0:64:1:64:1:0:64:1:0:64:1:>64:64:0:1:1:2:1:1:1:1:0:64:5840:MNNSNW:0:N:N  
(\$Revision: 1.132 \$)

Plugin ID : [11936](#)

 Information about this scan :

Nessus version : 3.0.3 Beta  
 Plugin feed version : 200606201415  
 Type of plugin feed : Registered (7 days delay)  
 Scanner IP : 192.168.182.122  
 Port scanner(s) : synscan  
 Port range : default  
 Thorough tests : no  
 Experimental tests : no  
 Paranoia level : 1  
 Report Verbosity : 1  
 Safe checks : yes  
 Max hosts : 20  
 Max checks : 4  
 Scan Start Date : 2006/6/20 23:09  
 Scan duration : 233 sec

Plugin ID : [19506](#)

**http (80/tcp)**  The following directories were discovered:  
/cgi-bin


While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

Other references : OWASP:OWASP-CM-006  
 Plugin ID : [11032](#)

**192.168.10.3**

[\[Return to top\]](#)

**general/udp**


 For your information, here is the traceroute from 192.168.182.122 to 192.168.10.3 :

```

192.168.182.122
192.168.182.1
?
```

Plugin ID : [10287](#)

**general/tcp**

 Information about this scan :

Nessus version : 3.0.3 Beta  
 Plugin feed version : 200606201415  
 Type of plugin feed : Registered (7 days delay)  
 Scanner IP : 192.168.182.122  
 Port scanner(s) : synscan  
 Port range : default  
 Thorough tests : no  
 Experimental tests : no  
 Paranoia level : 1  
 Report Verbosity : 1  
 Safe checks : yes


Max hosts : 20  
Max checks : 4  
Scan Start Date : 2006/6/20 23:09  
Scan duration : 657 sec

Plugin ID : [19506](#)

### 192.168.10.130


[\[Return to top\]](#)

#### general/udp

 For your information, here is the traceroute from 192.168.182.122 to 192.168.10.130 :  
192.168.182.122  
192.168.182.1  
?

Plugin ID : [10287](#)

#### general/tcp

 Information about this scan :


Nessus version : 3.0.3 Beta  
Plugin feed version : 200606201415  
Type of plugin feed : Registered (7 days delay)  
Scanner IP : 192.168.182.122  
Port scanner(s) : synscan  
Port range : default  
Thorough tests : no  
Experimental tests : no  
Paranoia level : 1  
Report Verbosity : 1  
Safe checks : yes  
Max hosts : 20  
Max checks : 4  
Scan Start Date : 2006/6/20 23:10  
Scan duration : 656 sec

Plugin ID : [19506](#)



### 192.168.10.145

[\[Return to top\]](#)

#### general/udp

 For your information, here is the traceroute from 192.168.182.122 to 192.168.10.145 :  
192.168.182.122  
192.168.182.1  
?

Plugin ID : [10287](#)

<b>general/tcp</b>	<p> 192.168.10.145 resolves as Vinton.lan. Plugin ID : <a href="#">12053</a></p> <p> Information about this scan :</p> <p>Nessus version : 3.0.3 Beta Plugin feed version : 200606201415 Type of plugin feed : Registered (7 days delay) Scanner IP : 192.168.182.122 Port scanner(s) : synscan Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : yes Max hosts : 20 Max checks : 4 Scan Start Date : 2006/6/20 23:11 Scan duration : 655 sec</p> <p>Plugin ID : <a href="#">19506</a></p>
--------------------	---