VPN Penetration Test

Network Intelligence (I) Pvt. Ltd.

Penetration Testing Team

Document Information

Company	<CLIENT NAME>
Document Title	Report on Penetration Testing of VPN for <CLIENT>
Date	22nd June 2004
Ref	<REP/CLIENT/NII/03152004>
Classification	○ Public ○ Internal ● Confidential ○ Secret
Document Type	REPORT

Recipients

Name	Title	Company

Document History

Date	Version	Author	Comments

TABLE OF CONTENTS

Executive Summary

According to the discussions with the client, NII undertook to carry out a penetration test of the VPN setup at the client's head office at ___________. The project was started on the 11th of June and was completed on the 22nd June as per the schedule.

Objective

The purpose of the test was to determine any security vulnerabilities in the VPN configuration of <CLIENT>. The test was carried out from assuming various levels of information as described in the section below.

Methodology

The entire project was divided into four parts as shown below:

1. Black Box Testing of 10.0.0.1, which is the IP address of the main VPN Server
2. White Box Testing of 10.0.0.1
3. Configuration and Architecture Review

The first part of the test was an attempt to try and discover the vulnerabilities in the system that an attacker would try. This was a zero-knowledge test, and we only knew the IP address of the system. The test consisted of the following:

1. Determining the Authentication Mode and Algorithm used
2. Determining any default user accounts
3. Determining vulnerabilities in PSK authentication
4. Determining open ports

The second part of the test was to connect using an ID specially created for this test, and try and discover the vulnerabilities in the system. For a VPN test, this is usually the most crucial phase, and most of the vulnerabilities are discovered at this stage.

The third part of the test was the black box test of a second IP address, which represented another Nortel Contivity VPN system with a default configuration. We carried out the same range of tests against this IP address as well.

The final part of the test consisted of an architecture and configuration review. The client submitted to us the architecture of the network, clearly showing the position of the VPN Contivity Firewall. Also, relevant parts of the firewall configuration were shared with us in order for us to evaluate the security of the configuration.

Findings

In this section, we would like to highlight some of the critical problems for the review of senior management.

As is to be expected in any VPN or Firewall penetration test, the crucial vulnerabilities are exploitable primarily by authenticated users. An unauthenticated attacker will usually find it very difficult to find and exploit any vulnerabilities in the system externally. The only noteworthy problem we were able to determine during the zero-knowledge black-box testing was that the Contivity system displays different error messages for failed authentication when the user exists, and when the user does not exist. This allowed us to discover three other users that may exist on the system: **‘london’, ‘john’**, and **‘test’**.

During the white box test we discovered some critical problems that would allow an attacker to penetrate further into various system. These are highlighted below:

- The first issue was the presence of a blank password for the Administrator account on one of the Windows servers. This represents a **critical** lapse in the Password Policy implementation within the network. We recommend implementing the policy more stringently, and regularly carrying out an internal penetration test exercise to determine any other such instances.

- The second issue was a default authentication access to Baystack switches/routers. Using the default username of ‘User’ and no password we were able to successfully get complete read-only access to the entire configuration. From one switch we were then able to authenticate to various other switches, and were also able to determine the internal IP addressing scheme. This in our opinion is a **critical** issue, and must be addressed immediately. We recommend configuring access control lists on the switch/router to prevent telnet access, except from authorized terminals; disallowing telnet access through the firewall, disabling the default ‘User’ account.

- The third issue was the access allowed to FTP and Telnet ports on various Windows servers as well as two mainframes. We recommend this access be restricted unless absolutely necessary.

From the fourth part of the exercise – the architecture and configuration review – we would like to note the following points for the management:

- **Absence of an Intrusion Detection System:** There is no Intrusion Detection System (IDS) present within the architecture. An IDS has the ability to detect attacks much before they become serious. For any attacker, including ethical attackers like us, the first stage is to carry out a port-scan to determine which servers are accessible over the Internet. An IDS has the ability to detect the port-scan and flag a possible intrusion attempt. In this way, the administrators can be alerted to an attack even before the attacker can attempt to exploit any other vulnerabilities.

- **Absence of two-factor authentication:** The industry-standard practice is to combine the username/password standard authentication of the VPN with a dynamically changing authentication key. This enables two-factor authentication: something the user **knows** (his username and password), and something he **has** (the dynamic authentication generating token).

Full Security Audit
The final and most important recommendation we would like to make is for a full-fledged security review to be carried out against all the critical systems, not just the VPN. From our limited view of the network during the white-box testing, we were able to determine critical vulnerabilities in the system configurations of the servers as well as network devices. We have a strong reason to believe that there may be other more severe vulnerabilities in the systems, which will only come to light once a full-fledged security audit is carried out.

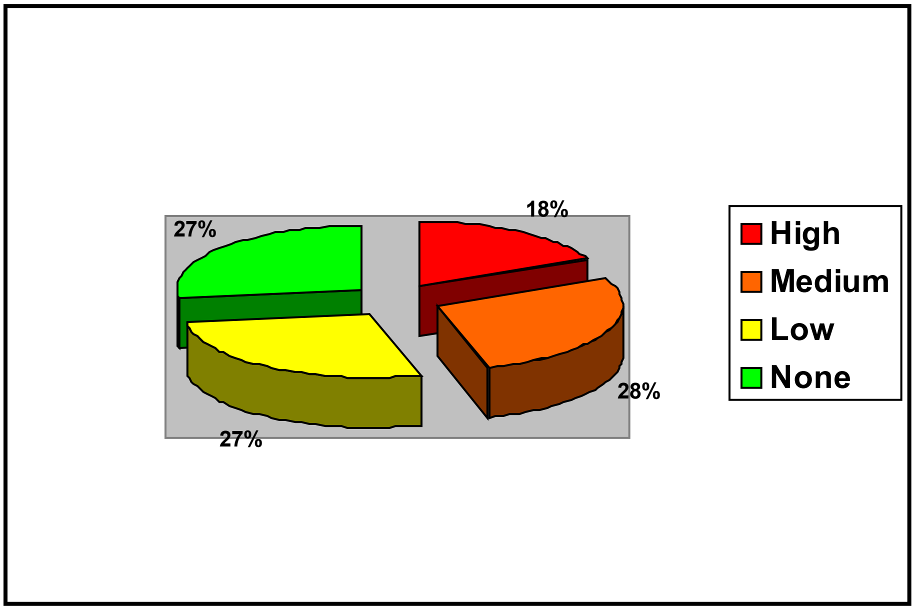
Summary of results

The table below summarizes our tests and the results:

Test Carried Out	Result	Criticality
Whois Information	Some critical information is revealed.	Low
Default Contivity Accounts	Not Present	None
Fingerprinting VPN Server – ikescan	PSK Authentication with MD5 and SHA1	None
Probing PSK Vulnerabilities	None found	None
Port scan	Some ports open, that may not be necessary	Low
TCP SYN Packets with FIN Flag	Firewall allows the packets through	Low
Username enumeration	User accounts could be guessed	Medium-High
FTP and Telnet security	Anonymous FTP allowed FTP and Telnet banners reveal critical information	Medium-High
Weak Windows Password	One system had a blank password for the super-user 'administrator' account	High
Telnet access to Baystack ARN and ASN	Using the 'User' default account we were able to get read-only access to the entire configuration	High
FTP and Telnet access can be restricted	Contivity Firewall allows authenticated users to access FTP and Telnet on any internal server	Medium

Graphical Summary

The pie chart below summarizes the number of vulnerabilities categorized as follows:
Low: Risk that has very low probability and low impact of being exploited. Recommendations do not require immediate consideration.
Medium: Risk that in conjunction with other vulnerabilities or unforeseen circumstances may result in system compromise. Suggestions must be considered seriously and acted upon in the immediate future
High: Risk that will eventually lead to a system compromise and must be acted upon immediately
Very High: Highest possible risk rating having a very high probability of being exploited. Also, can be exploited with low level of skills and must be acted upon immediately.



The following report presents the detailed technical findings and results from each of the tests that we carried out against the VPN systems. It also contains recommendations for vulnerabilities that were discovered.

Black Box Testing - 10.0.0.1

WHOIS Information

Severity Level: Low

Summary:

With the target IP addresses given we queried the Whois database and got the information related to internet address range assigned to the organization, domain names, contacts information (administrators) etc.

Results:

Truncated for Confidentiality

Risk:

The Whois database reveals information such as the name of the administrator, his actual email address and phone number. With this information an attacker may try to use social engineering technique to get further information from the email ids mentioned in the database or even by directly calling the person whose contact info is mentioned.

Recommendations:

The organization should use generic email ids. An email sent to this generic email ID will be forwarded to the system administrator. The actual names of the administrators must not be revealed. It is also not necessary to reveal the phone numbers of the organization. Also the organization must train their employees to adopt security policies and awareness of social engineering attacks.

Default accounts absent

Severity Level: None

Summary:

One of the common vulnerabilities in the implementation of any system is the presence of default system accounts with their passwords unchanged. In the case of the Nortel Contivity VPN server, there exists a default account of ‘admin’ with a password of ‘setup’.

Results:

We tried to connect with various easily guessable passwords for the ‘admin’ account, but were not able to authenticate to the system. Other username attempts such as ‘nortel’, ‘setup’, ‘vpn’, ‘client’, ‘widget’, ‘widget2’, ‘user’, ‘contivity’, ‘firewall’, etc. also did not yield any results.

Risk: None

Recommendation: None

Fingerprinting the VPN Server – IKE-SCAN

Severity Level: None

Summary:

This tool is used to discover and fingerprint IKE hosts (IPsec VPN Servers) using IKE (Internet Key Exchange). The ike-scan uses the retransmission and backoff strategy / fingerprint to determine which vendors implementation is being used.

Although just being able to discover an IPSec VPN system running IKE and determining which IKE implementation it is using is not a vulnerability in itself, this information can be valuable to a potential attacker. For example knowing that there is an XYZ brand of VPN server at a given address could prompt an attacker to download the appropriate VPN client and try some username/password guessing. Alternatively, the attacker could search for known vulnerabilities associated with the XYZ VPN server.

Results:

IKE-Scan against the target IP gave following results.

```
G:\ike-VPN-test>ike-scan 10.0.0.1
Starting ike-scan 1.6 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
10.0.0.1 Main Mode Handshake returned SA=(Enc=3DES Hash=SHA1 Auth=PSK
Group=1:modp768 LifeT
ype=Seconds LifeDuration(4)=0x00007080)

Ending ike-scan 1.6: 1 hosts scanned in 0.979 seconds (1.02 hosts/sec).  1 returned handshake; 0
returned notify
```

This showed us that the remote VPN system is using PSK for authentication. We then used the ike-probe tool shown below to try and crack the PSK keys.

Risk: None

Recommendation: None

Secure PSK Authentication

Severity Level: None

Summary:

IKEProbe is a tool to determine vulnerabilities in the PSK implementation of the VPN server. We ran this tool against the system, and it did not reveal any critical vulnerabilities.

Results:

The output given by this tool is as shown below:

```
IKEProbe 0.1beta   (c) 2003 Michael Thumann (www.ernw.de)
Portions Copyright (c) 2003 Cipherica Labs (www.cipherica.com)
Read license-cipherica.txt for LibIKE License Information
IKE Aggressive Mode PSK Vulnerability Scanner (Bugtraq ID 7423)

Supported Attributes
Ciphers              : DES, 3DES, AES-128, CAST
Hashes               : MD5, SHA1
Diffie Hellman Groups: DH Groups 1,2 and 5

IKE Proposal for Peer: 10.0.0.2
Aggressive Mode activated ...

[Output truncated for brevity]
Cipher AES
Hash MD5
Diffie Hellman Group 2

841.890 3: ph1_initiated(00443ee0, 007d23c8)
841.950 3: << ph1 (00443ee0, 276)
843.963 3: << ph1 (00443ee0, 276)
846.967 3: << ph1 (00443ee0, 276)
849.961 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher AES
Hash MD5
Diffie Hellman Group 5

849.961 3: ph1_initiated(00443ee0, 007d5010)
849.141 3: << ph1 (00443ee0, 340)
851.644 3: << ph1 (00443ee0, 340)
854.648 3: << ph1 (00443ee0, 340)
857.652 3: ph1_disposed(00443ee0)
```

```
Attribute Settings:
Cipher CAST
Hash SHA1
Diffie Hellman Group 1

857.652 3: ph1_initiated(00443ee0, 007d23c8)
857.682 3: << ph1 (00443ee0, 244)
859.685 3: << ph1 (00443ee0, 244)
862.680 3: << ph1 (00443ee0, 244)
865.684 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash SHA1
Diffie Hellman Group 2

865.684 3: ph1_initiated(00443ee0, 007d5010)
865.754 3: << ph1 (00443ee0, 276)
867.757 3: << ph1 (00443ee0, 276)
870.761 3: << ph1 (00443ee0, 276)
873.765 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash SHA1
Diffie Hellman Group 5

873.765 3: ph1_initiated(00443ee0, 007d23c8)
873.936 3: << ph1 (00443ee0, 340)
875.939 3: << ph1 (00443ee0, 340)
878.943 3: << ph1 (00443ee0, 340)
881.947 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash MD5
Diffie Hellman Group 1

881.947 3: ph1_initiated(00443ee0, 007d5010)
881.977 3: << ph1 (00443ee0, 244)
883.980 3: << ph1 (00443ee0, 244)
886.984 3: << ph1 (00443ee0, 244)
889.989 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
```

```
Hash MD5
Diffie Hellman Group 2

889.989 3: ph1_initiated(00443ee0, 007d23c8)
889.049 3: << ph1 (00443ee0, 276)
891.052 3: << ph1 (00443ee0, 276)
894.066 3: << ph1 (00443ee0, 276)
897.070 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash MD5
Diffie Hellman Group 5

897.070 3: ph1_initiated(00443ee0, 007d5010)
897.261 3: << ph1 (00443ee0, 340)
899.763 3: << ph1 (00443ee0, 340)
902.767 3: << ph1 (00443ee0, 340)
905.771 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash MD5
Diffie Hellman Group 5

905.771 3: ph1_initiated(00443ee0, 007d23c8)
905.942 3: << ph1 (00443ee0, 340)
```

System not vulnerable.

After probing to the VPN box with the IKEProbe tool we got the results that showed that the system is not vulnerable to such an attack. This means that the Nortel VPN box is not vulnerable to brute-force /dictionary attack on PSK ISK Authentication mechanism.

Risk: None

Recommendation: None

Port Scan

Severity Level: Low

Summary

Port scanning on a system gives the information of the services running on the target system. Also it gives useful information about the Operating System running on the server/system with the versions of services installed.

Results

The following ports appeared to be open on the server. Alongside the port number, we also show the service that usually runs on those ports as well as the banner displayed by the service.

Target IP Address: 10.0.0.1

Ports	Service Running
TCP 389	LDAP
TCP 1002	windows-icfw
TCP 1720	H.323/Q.931/H32hostcall
TCP 1723	PPTP
TCP 47624	Unknown service
UDP 500	ISAKMP

The result shown above may be the false positives. If a firewall is blocking access to the device, then it is quite likely that these ports may not really be open on the server. The only port that is definitely open is UDP 500. On port 47624 some unknown service is running. We were unable to find out the type of service running.

Risk:

Getting information from the port scanning attempt, an attacker can determine the known vulnerabilities and exploits for the specific services running in the system and try to compromise the system remotely.

Recommendation:

Any unnecessary service running on the system should be shutdown/stopped. If these ports are not open, then this recommendation can be ignored. We also recommend checking the service running on port 47624 (if any), and disabling it if required or blocking it at the firewall.

TCP SYN Packets with FIN flag allowed

Severity Level: Low

Description:

The remote host does not discard TCP SYN packets, which have the FIN flag set.

Risk:

The SYN-FIN combination of TCP flags is illegal, and should ideally be dropped by the firewall. Allowing these packets through, could potentially allow an attacker to bypass the rule-set.

Recommendation

Block all illegal combinations of TCP packets and allow only legal packets through.

References:

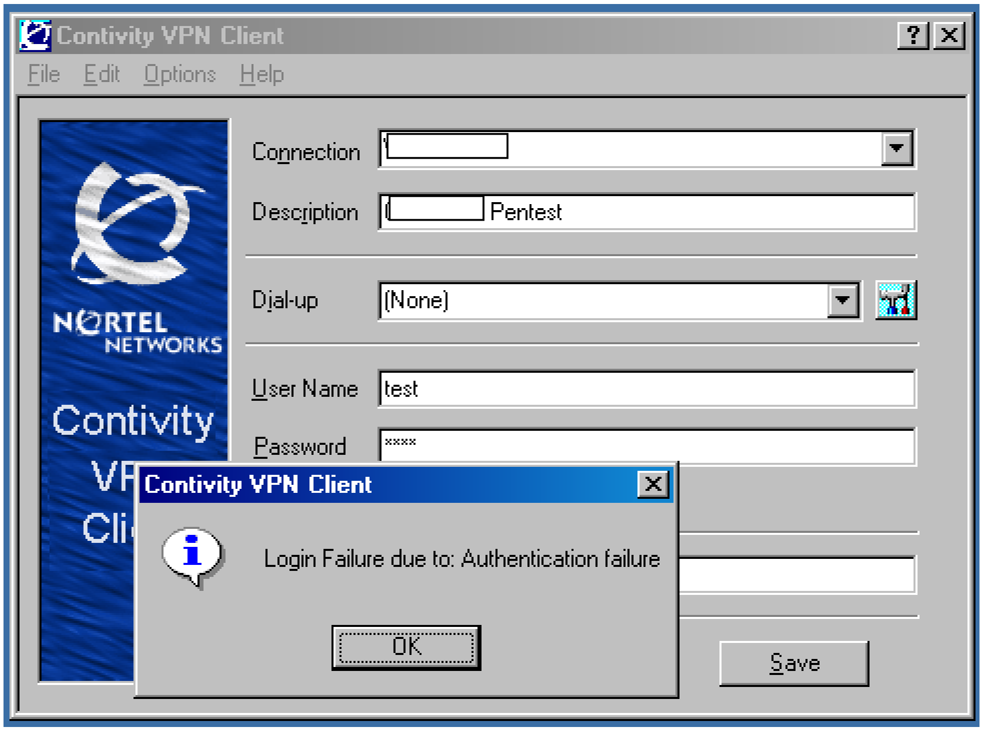
http://www.securityfocus.com/bid/7487
http://www.kb.cert.org/vuls/id/464113,
http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html

User Name Enumeration

Severity Level: Medium-High

Summary:
With the VPN client when we tried to connect with different username and password combinations we found that the VPN authentication mechanism gives different error messages for existing users present on the system and for non-existing accounts.

Results:
Below shown are the snaps for these error messages.
First snap showed that for the username 'test' if an incorrect password is entered, the error message is **"Login Failure due to: Authentication failure"**.



Connection [redacted]

Description [redacted] Pentest

Dial-up (None)

User Name test

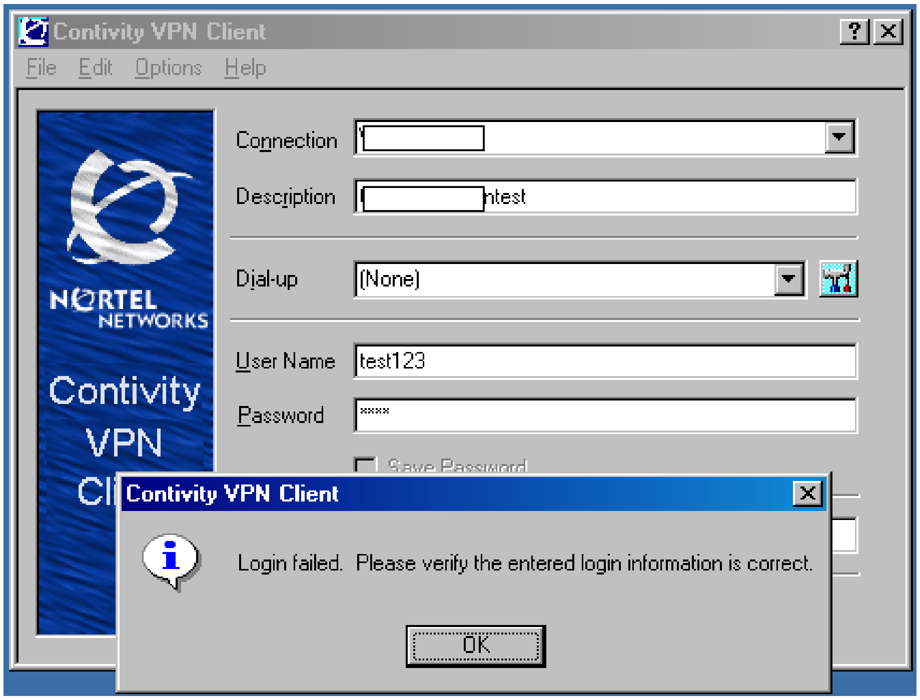
Password ****

Contivity VPN Client

Login Failure due to: Authentication failure

OK

However, if we use an account such as 'test123', with any password, the error message shown is: **"Login Failed: Please verify the entered login information is correct"**:



Connection [redacted]

Description [redacted]ntest

Dial-up (None)

User Name test123

Password ****

□ Save Password

Contivity VPN Client

Login failed. Please verify the entered login information is correct.

Thus the error messages for user accounts that exist, and for those that do not exist is different. This allows us to enumerate which user accounts may be present on the system. We found the following users present on the system using this flaw:

User – test
User – london
User – john

We were however, unable to guess the passwords for these accounts.

Risk:

From this behavior it is easier to find out the actual users present on the system without using a tool. This will simplify the attackers' attempts to get the actual username and passwords and connect to the VPN box, which eventually give access to the system. He can first enumerate typical usernames, and then try and guess passwords only for those user accounts.

Recommendation:

Use specific usernames that are hard to guess and contain numbers as well. Do not use generic user names such as 'test', and 'london'. Also use a good combination of alphabets, digits and special characters for passwords to make them difficult to guess/detect. Secondly, this might be a flaw in Nortel's implementation of the product[1], and unless there is a patch issued for it, there is not much the organization may be able to do. We have informed the security contact at Nortel,

[1] This did turn out to be a flaw in Nortel Contivity VPN client, and was subsequently patched by Nortel Networks. See our advisory on this issue at http://www.nii.co.in/vuln/contivity.html

and are awaiting confirmation from them, whether this is a known flaw, a configuration mistake, or they would need to issue a patch for it.

White Box Testing - 10.0.0.1

FTP and Telnet Security Issues

Severity Level: Medium-High

Summary:
FTP is a potentially dangerous service because anyone who gain access to remote system can download or upload illegal data/files. Also, FTP communication is in plain-text and an internal attacker can flood the ARP cache of a user to sniff his FTP authentication details, or compromise the switch. The same applies to Telnet access as well.

Results:
After connecting with the test user id and password we have got assigned an IP **(192.168.10.244)**. The next step after this was to carry out a port-scan of the IP range 192.168.10.X to check for open Telnet (TCP 23) and FTP (Telnet 21) ports. The port scan is followed by a banner-grabbing attempt, which tries to login to the FTP services with anonymous access. The results of the port-scan are shown below:

IP 192.168.10.1

```
TCP Port                 Banner

21                       220 datacenter Microsoft FTP Service (Version 5.0).
File Transfer [Control]  --> USER anonymous
                         331 Anonymous access allowed, send identity (e-mail name) as
                         password.
                         --> PASS anon@anon.com
                         230 Anonymous user logged in.
                         --> SYST
                         215 Windows_NT version 5.0
                         --> QUIT
                         221
```

IP 192.168.10.4

```
TCP Port                  Banner

21                        220 server1 Microsoft FTP Service (Version 5.0).
File Transfer [Control]   --> USER anonymous
                          331 Password required for anonymous.
                          --> PASS anon@anon.com
```

```
530 User anonymous cannot log in.
--> SYST
530 Please login with USER and PASS.
--> QUIT
221
```

IP 192.168.10.7

TCP Port	Banner
21 File Transfer [Control]	220 domino Microsoft FTP Service (Version 5.0). --> USER anonymous 331 Anonymous access allowed, send identity (e-mail name) as password. --> PASS anon@anon.com 230 Anonymous user logged in. --> SYST 215 Windows_NT version 5.0 --> QUIT 221

IP 192.168.10.8

TCP Port	Banner
21 File Transfer [Control]	220 ras Microsoft FTP Service (Version 5.0). --> USER anonymous 331 Anonymous access allowed, send identity (e-mail name) as password. --> PASS anon@anon.com 530 User anon@anon.com cannot log in. --> SYST 530 Please login with USER and PASS. --> QUIT 221

IP 192.168.10.11

File Transfer [Control]	--> USER anonymous 220 Connection will close if idle more than 5 minutes. --> PASS anon@anon.com 331 Enter password. --> SYST 530 Log on attempt by user ANONYMOUS rejected. --> QUIT 215 OS/400 is the remote operating system.
23 Telnet	[No Banner]

IP 192.168.10.12

TCP Port	Banner
21 File Transfer [Control]	220-OS21 at AS400. --> USER anonymous 220 Connection will close if idle more than 5 minutes. --> PASS anon@anon.com 331 Enter password. --> SYST 530 Log on attempt by user ANONYMOUS rejected. --> QUIT 215 OS/400 is the remote operating system.
23 Telnet	[No Banner]

IP   192.168.10.26

TCP Port	Banner
23 Telnet	Bay Networks, Inc. and its Licensors. Copyright 1992,1993,1994,1995,1996,1997,1998. All rights reserved. Login: ...

IP   192.168.10.28

TCP Port	Banner

TCP Port	Banner
21 File Transfer [Control]	220 WuFTP server(x13.10) ready. --> USER anonymous 331 Password required for anonymous. --> PASS anon@anon.com 530 Login incorrect. --> SYST 502 Unknown command SYST. --> QUIT 221 Goodbye.
23 Telnet	Bay Networks, Inc. and its Licensors. Copyright 1992,1993,1994,1995,1996,1997,1998. All rights reserved. Login: ...

IP 192.168.10.127

TCP Port	Banner
21 File Transfer [Control]	220 ras2 Microsoft FTP Service (Version 5.0). --> USER anonymous 331 Anonymous access allowed, send identity (e-mail name) as password. --> PASS anon@anon.com 530 User anon@anon.com cannot log in. --> SYST 530 Please login with USER and PASS. --> QUIT 221

IP 192.168.10.166

23 Telnet	[No Banner]

Risks Associated

FTP and Telnet Banners

The FTP and Telnet banners reveal the following pieces of information:

1. **System or Hostname**

For instance, in the cases above you can see that various hostnames are revealed such as 'domino', 'ras', 'ras2', etc. The knowledge of these hostnames gives the attacker an idea of what the system is used for. More importantly, it may also give him a clue as to possible passwords

2. **Operating System Version**

In almost all cases, the operating systems have been correctly identified. Most of the systems are running Microsoft FTP Version 5.0. This indicates the operating system is Windows 2000 Server or Windows 2000 Advanced Server or Windows 2000 Professional. In some cases, it reveals the system as an IBM Mainframe server running the OS/400 operating system. And finally, two of the devices are revealed as Nortel Baystack ASN or ARN boxes.

3. **FTP Version**

The FTP Version lets the attacker know if there might be any possible security issues existing in that version of FTP. For instance, as per the industry-standard vulnerability databases, FTP version 5.0 is vulnerable to a connection status request denial of service vulnerability. This is because of the way the server handles the request for transfer status. This allows a client to issue a command with a large number of file globbing characters as the argument, which may cause the service to crash. If the patch for this has been applied, then the server may not be vulnerable to this attack. However, in the future if a new vulnerability is discovered, for which a patch has not yet been applied, then the attacker would exploit that vulnerability with his previous knowledge of the FTP service version

Recommendation

Disable the banner or modify it using your FTP software's configuration. On IIS this can be done using the Internet Services Manager.

4. **Anonymous FTP**

On most of the Windows systems, anonymous FTP access is allowed. This enables an attacker to supply the username 'anonymous' with any email address as a password and log in to the FTP service. In the default configuration of Microsoft's FTP Service, the anonymous logged in user has read-only rights. However, if there is any critical data uploaded on to the FTP service, then the anonymous user may be able to download and compromise the confidentiality of the data.

Recommendation

Disable anonymous FTP using the Internet Services Manager applet, if not required. If FTP is required, then restrict the FTP access to only those servers that remote users need to connect to. In the current setup, FTP and Telnet access is allowed to the entire range of internal systems.

Weak Windows Passwords

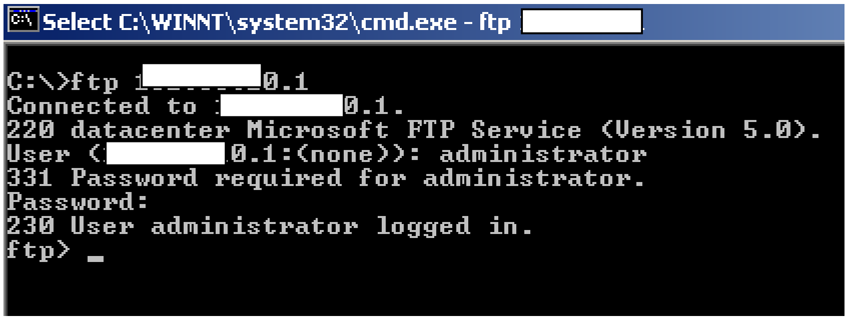
Severity Level: High

Summary

On the Windows FTP prompts we tried various username/password combinations to try and find out if any weak passwords were configured on the systems.

Results

On the main Windows server: 192.168.10.1 (datacenter), we were able to successfully login with a username of 'administrator', and a blank password.



Select C:\WINNT\system32\cmd.exe - ftp [redacted]

```
C:\>ftp [redacted]0.1
Connected to [redacted]0.1.
220 datacenter Microsoft FTP Service (Version 5.0).
User ([redacted]0.1:(none)): administrator
331 Password required for administrator.
Password:
230 User administrator logged in.
ftp> _
```

Risk Associated

The risks associated with weak passwords do not need to be enumerated. In all our experience we have seen that one of the most common mistakes made by system administrators is to not enforce password complexity on their systems. Without the enforcement of such a policy, users and system administrators will always have a tendency to choose weak passwords.

Recommendations:

Enable Password Complexity on the Windows system using the Local Security Policy settings, or if it is part of the domain, then enable Group Policy Security Object settings. Implement a corporate security policy, which ensures that users choose complex passwords.

Nortel Telnet Access

Severity Level: High

Summary

The telnet service was found to be open on the Nortel Baystack routers. More critically, the default access with username of ‘User’, and no password, was still enabled. As a result, we were able to connect to the routers and view the entire configuration. Moreover, from one router we were able to telnet into multiple other routers and access these as well.

Results:

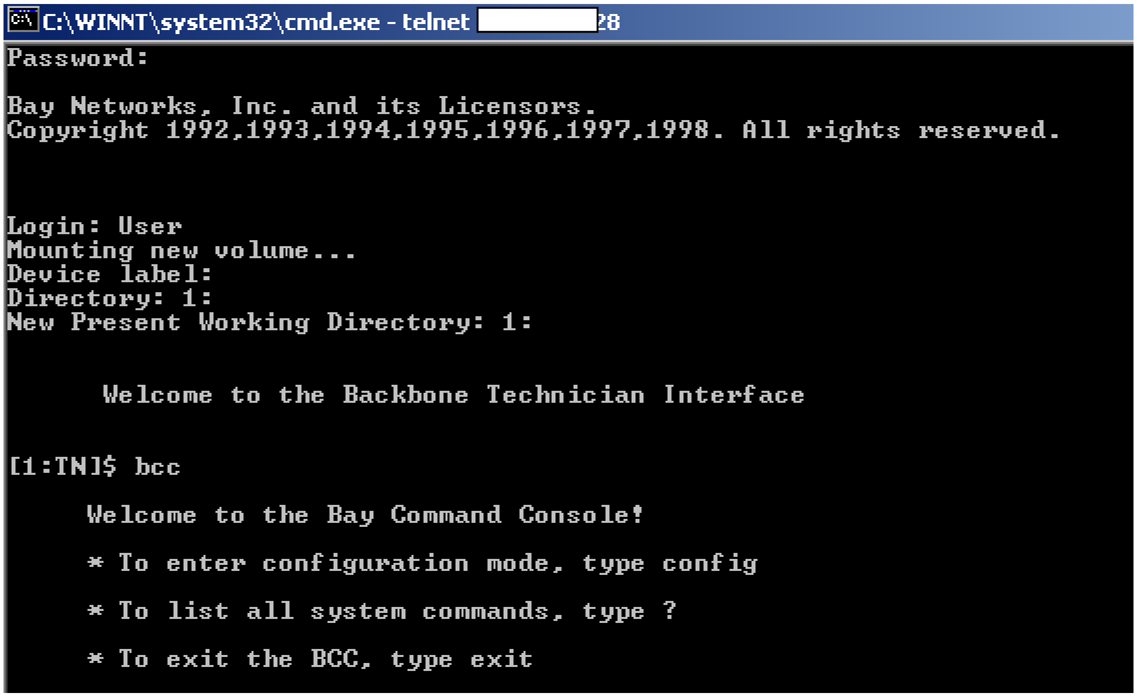
We have found Telnet service running on some systems. 192.168.10.11, 12, 26, 28,166, etc.

Banners grabbing as shown in the earlier sections revealed useful information about the network. From the banners displayed it was very easy to find out that the telnet service was running for the Bay Network Router/Switch.

As it revealed that this is a Bay Network it simplified our task further to get into the network. Using telnet to 192.168.10.28 we got in to the Bay Network Console Interface as shown below.

With Default username with password we got the access into the router. **‘User ‘** account gives us access to the bcc console prompt where anybody could give system commands to get more information about the configuration.

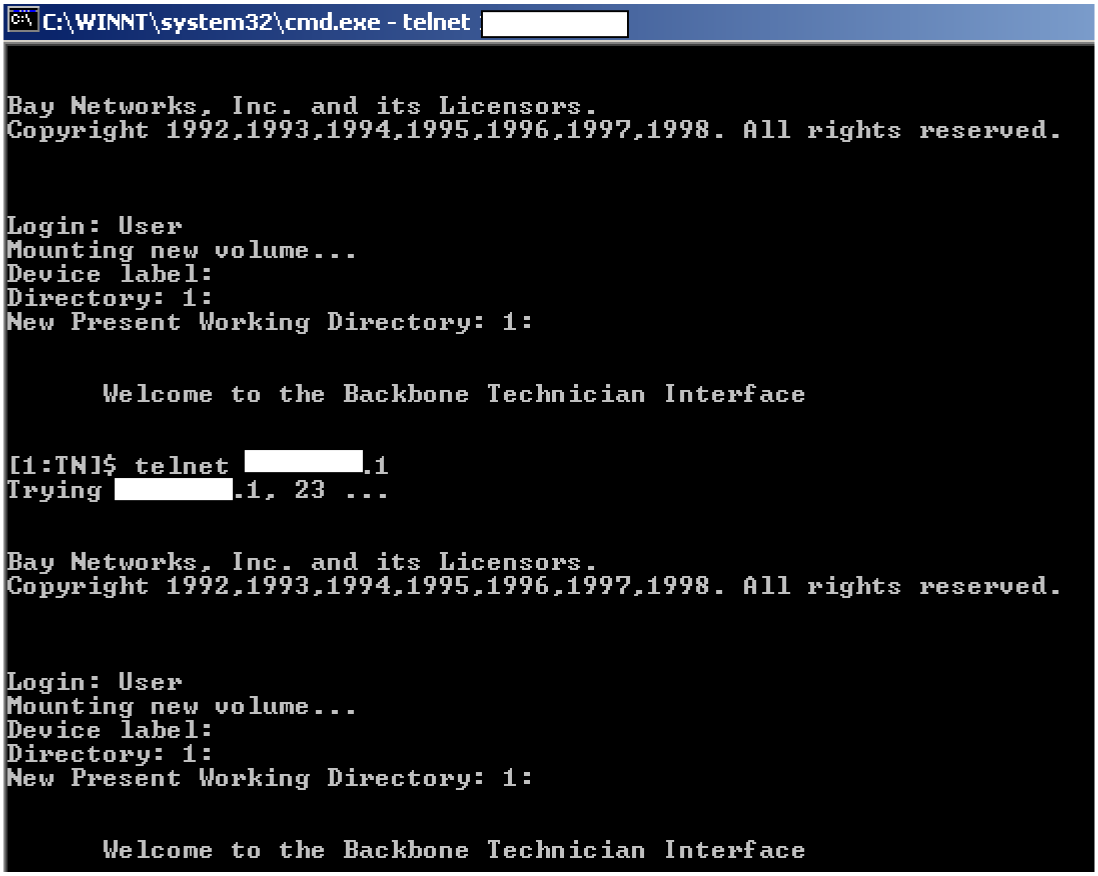
Picture below shows that we actually got bcc configuration access to bay network router.



```
Password:

Bay Networks, Inc. and its Licensors.
Copyright 1992,1993,1994,1995,1996,1997,1998. All rights reserved.


Login: User
Mounting new volume...
Device label:
Directory: 1:
New Present Working Directory: 1:


      Welcome to the Backbone Technician Interface


[1:TN]$ bcc

     Welcome to the Bay Command Console!

     * To enter configuration mode, type config

     * To list all system commands, type ?

     * To exit the BCC, type exit
```

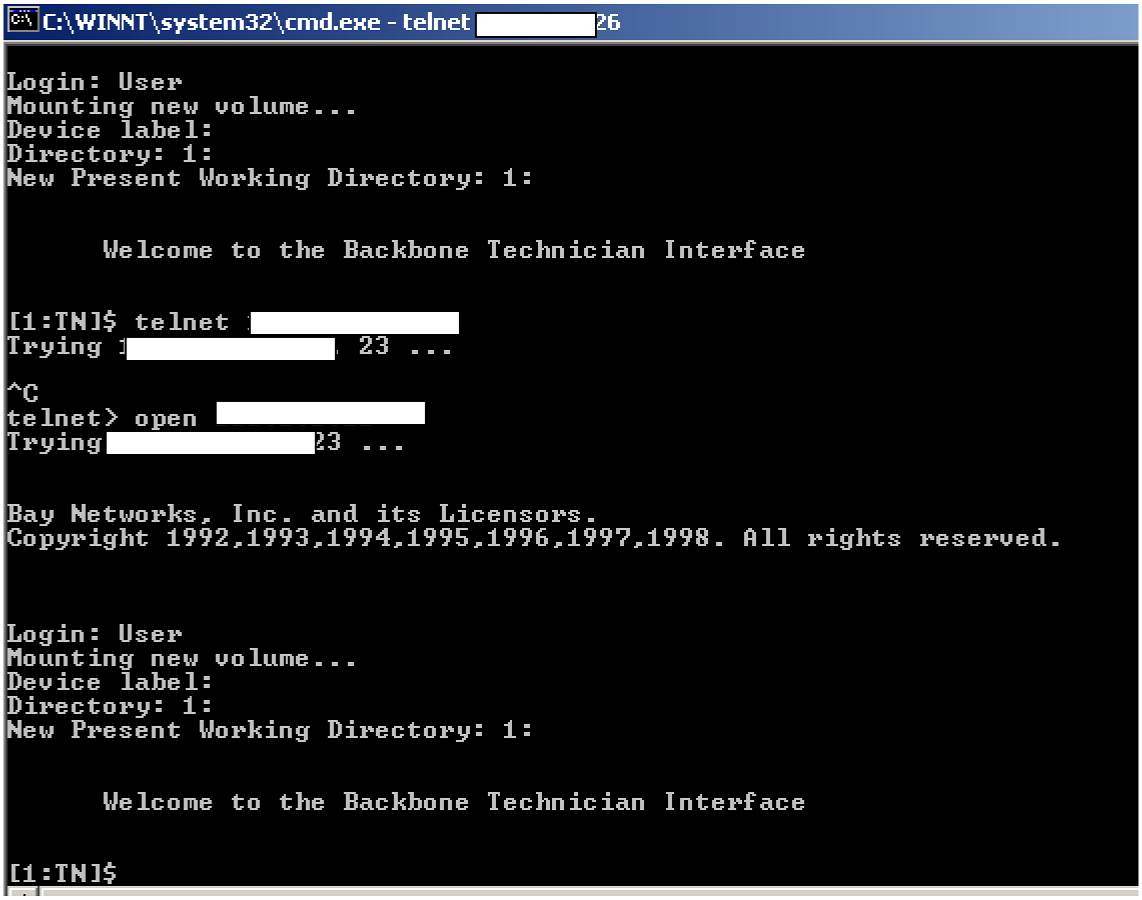
This was happening on 192.168.10.26 also. We were also able to get the whole configuration of the router. See the Appendix A to see the configuration we got. This revealed all the network setup.

Further drilled down gives critical network IP address allocation information and telnet access to the internal network. As the snapshot below shows, we were able to telnet into the other internal devices, such as 10.1.1.1 as shown below:



```
Bay Networks, Inc. and its Licensors.
Copyright 1992,1993,1994,1995,1996,1997,1998. All rights reserved.



Login: User
Mounting new volume...
Device label:
Directory: 1:
New Present Working Directory: 1:


      Welcome to the Backbone Technician Interface


[1:TN]$ telnet [redacted].1
Trying [redacted].1, 23 ...


Bay Networks, Inc. and its Licensors.
Copyright 1992,1993,1994,1995,1996,1997,1998. All rights reserved.



Login: User
Mounting new volume...
Device label:
Directory: 1:
New Present Working Directory: 1:


      Welcome to the Backbone Technician Interface
```

The snapshot below shows, that we were able to telnet to the router at 10.1.1.11 also.



```
Login: User
Mounting new volume...
Device label:
Directory: 1:
New Present Working Directory: 1:


      Welcome to the Backbone Technician Interface


[1:TN]$ telnet [redacted]
Trying [redacted] 23 ...

^C
telnet> open [redacted]
Trying [redacted]23 ...


Bay Networks, Inc. and its Licensors.
Copyright 1992,1993,1994,1995,1996,1997,1998. All rights reserved.



Login: User
Mounting new volume...
Device label:
Directory: 1:
New Present Working Directory: 1:


      Welcome to the Backbone Technician Interface


[1:TN]$
```

Recommendations:

- Only if required give telnet access to the remote systems. This can be done with the use of Access Control Lists. If possible simply stop the service from running.
- Hide banner information displayed after a user connects via telnet to the system. This gives the attacker critical information about the network.
- But the most important task is to remove the default user accounts and blank or weak passwords.

Nortel VPN Architecture and Configuration Review

Summary:

We were submitted snapshots of the Nortel Contivity Firewall configuration for a review. The document submitted to us also contained the network topology diagram showing the position of the VPN server as shown below:

[Removed for confidentiality]

Recommendations:

From the snapshots submitted to us, we would recommend the following:

1. **Restrict access only to the specific destination IP addresses**

   Currently, the rule set allows the authenticated users to access the allowed services, such as FTP, Telnet, NortelClient, Lotus Notes, etc. on any of the internal servers. This rule allowed us to connect to the Baystack switches, although under normal circumstances users would never need to access the configuration of the switches and routers. Furthermore, FTP access was mis-configured on some of the internal servers, and it needs to be evaluated whether the FTP rule can be configured to allow access only to specific FTP servers.

   The risk associated is that an internal server may have FTP or Telnet configured on it by mistake, and it would suddenly become accessibly to remote users.

2. **Sorting of rules for faster performance**

   This suggestion is not strictly linked to security, but performance of the firewall can be enhanced by moving the rules that are accessed frequently towards the top of the list. For instance, the rule that allows connections from NortelClient and NortelClient1 can be moved to the top of the list as this has the possibility of being a frequently used rule. When the Contivity firewall finds a first match, it will process the packet accordingly. The earlier the match, the faster the packet is processed.

Appendix A: Bay Networks Configuration

The listing below gives the configuration of one of the Baystack Routers that were accessible to an authenticated VPN user. Furthermore, once successfully authenticated to this box, we were able to telnet into the other Baystack routers as well. We have highlighted the important configuration information that would allow us to map the network.

REMOVED FOR CONFIDENTIALITY