A Security Audit of a 3COM OfficeConnect Remote 812 ADSL Router

GIAC Systems and Network Auditor (GSNA)

Practical Assignment (v3.0, option 1)

David Pérez Conde

March 2004

ABSTRACT

This paper constitutes the practical assignment (v3.0, option 1) that I submitted as one of the requirements to obtain the GSNA certification (GIAC Systems and Network Auditor).

The document, which describes a security audit of a 3COM OfficeConnect Remote 812 ADSL Router, is divided in four parts. Part 1 shows some preliminary research performed in preparation for the audit. Part 2 contains a checklist that can be used to conduct an audit of a router of the specified model or similar. Part 3 shows the evidence and findings obtained when performing a selection of the items of the checklist to the audited system. Finally, Part 4 is the audit report, including an executive summary, the findings and a set of recommendations.

Table of Contents

1 Preliminary Research

1.1 Description of the system to be audited

The system that will be audited is the border router of the home office network of Susan Smith[1], a freelance network consultant.

The network consists of a single Ethernet segment, where three PCs are permanently connected. One of the PCs belongs to the consultant's husband, another to their only child and the third one acts as a web and file server (will be referred to as “the web server”). Occasionally, other devices, like a game console or the consultant's laptop, are also attached to the network. Table 1 shows a diagram of the network.

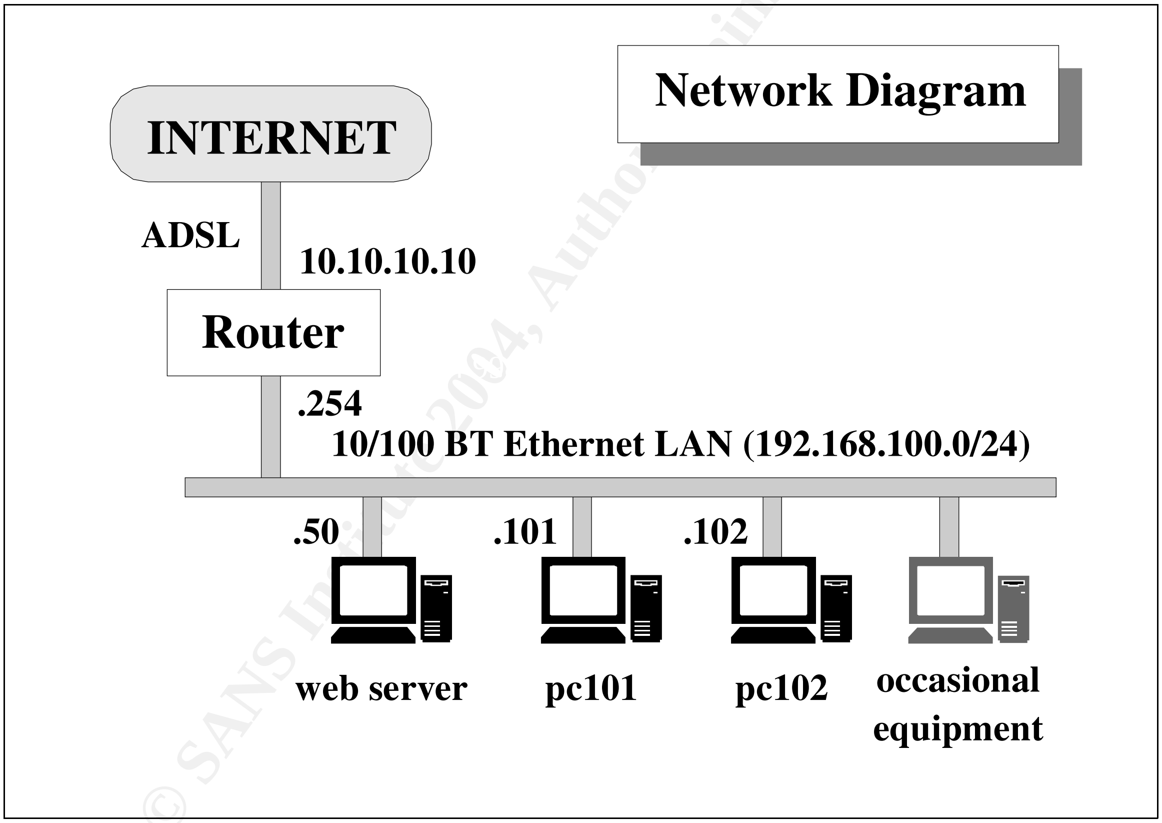

Table 1 Network diagram (public address changed to 10.10.10.10 for privacy reasons)

The border router, which is the system to be audited, is a "OfficeConnect Remote 812 ADSL Router", by 3COM [3CO01]. Its product number is "3CP204144" and its serial number is “HLY21XXXXXXX”.

[1] The name is fictitious, to preserve anonymity of the real character.

The OfficeConnect Remote 812 ADSL router is designed to provide network connectivity between a Local Area Network (LAN) and a Wide Area Network (WAN) to which it connects via an Asymmetric Digital Subscriber Line (ADSL).

Typically, and this is the case of the router being audited, the WAN connection goes to an Internet Service Provider (ISP), so the WAN is actually the Internet. Physically, the connection is established using the RJ11 socket provided in the unit. One end of a phone/modem cable is plugged to the router's RJ11 connector and the other end is plugged to the wall phone jack.

The LAN interface is implemented by four 10BT RJ45 Ethernet ports, internally connected in hub mode, meaning that all network traffic received at or sent to any port is broadcasted to all other ports.

In this particular case, only one of the Ethernet ports is used, and it is connected in cascade to a 8-port Ethernet hub, where all the devices are attached.

The IP addressing scheme is as follows. The LAN is assigned the private network 192.168.100.0/24. The router is configured as a DHCP server that provides internal network addresses (192.168.100.1 to 192.168.100.25) to dynamic clients in the LAN. The three stable PCs have their own fixed IP addresses above the DHCP range, as the network diagram on Table 1 shows. The WAN interface of the router holds the public Internet IP address assigned by the ISP, which will be substituted throughout all this report by the private address 10.10.10.10 for privacy reasons. The router is in charge of performing Network Address Translation (NAT) in order to hide all the internal addresses behind the public address[2] on outgoing traffic and do the reverse for the incoming replies. It is also in charge of performing Port Address Translation (PAT) in order to redirect any incoming connection to the appropriate internal server. In particular, only two ports should be mapped: 80/tcp (HTTP) and 22/tcp (SSH), both to the internal web server. These are the only two network services that need to be accessible from the Internet.

There is no formal security policy available, but there is the following informal policy that establishes what traffic should be allowed through, to and from the router:

- All internal hosts must be allowed to initiate any kind of connections to anywhere in the Internet, and to receive the replies.
- All traffic coming from the Internet other than replies to connections initiated from the LAN must be blocked at the router, with the following exceptions which must be forwarded to the web server:

[2] This kind of address translation is also known as IP masquerading.

  - HTTP connections from anywhere
  - SSH connections from anywhere

- The router itself must offer only the DHCP service, and only on the LAN interface. It must not offer any other service. The router must be managed exclusively through the console, which is accessed via an RS-232 cable from a serial port of the web server.
- Anything not explicitly allowed by this policy should be disallowed.

The web service is offered to the Internet because among other things it contains family pictures to be shared with distant relatives. The SSH service allows Susan to connect back to the system at any time, from wherever she may be working, and retrieve any files she may need.

1.2 Most significant risks to the system

The importance of the security of the system being audited comes from its role in the protection of important information assets. Table 2 enumerates and describes the major information assets whose security is affected by the security of the router being audited.

Information Asset	Description
Confidential files	The files that Susan stores in the web server contain information from previous works that is confidential. In particular, it contains documentation about network configuration of her customers. The confidentiality, integrity and availability of this information is vital for Susan's business.
Family Pictures	The web server publishes family pictures so that distant relatives can access them. The value of this information asset is not economical, but sentimental. Confidentiality is not an issue, but integrity and availability are: Susan would certainly not like their photos being modified or deleted by unauthorized persons.

Table 2 Information assets protected by the router

There are many different threats against the security of any information system in general and of the system being audited in particular, but they can be broken in three categories: natural, accidental or intentional[3] [PEL01]. Table 3 shows a

[3] [PEL01] p.7-15. Parts developed by John O'Leary, Director of the Education Resource Center

few examples of each kind of threats, with an explanation of the damage they may inflict.

Threat	Type	Description
Earthquake	Natural	A sudden movement of the earth's crust. It may cause the destruction of information processing facilities.
Tornado	Natural	A wide rotating column of air whirling at destructively high speeds. It may cause the destruction of information processing facilities.
Power failure	Accidental	A disruption in the the electrical power source. It may cause information processing equipment to be off during the outage.
Hardware failure	Accidental	Failure of some piece of information processing equipment. It may affect the ability of that equipment to continue operating.
Human error	Accidental	Mistake made by a user of an information processing system. It may cause the unwanted deletion, alteration or disclosure of data.
Alteration of data	Intentional	Intentional modification, insertion or deletion of data. It may affect the integrity or the availability of the data.
Alteration of software	Intentional	Intentional modification, insertion or deletion of computer programs. It may affect the integrity or the availability of the system.
Unauthorized disclosure	Intentional	Unauthorized disclosure of proprietary information by authorized or unauthorized users. It may affect the confidentiality of the information.

Table 3 Threats

The system being audited (the border router) is involved in protecting the aforementioned information assets from the last three (intentional) threats listed

of the Computer Security Institute.

on Table 3. Its main role is therefore preventing unauthorized access to the server, specially by outsiders since internal users can access the web server directly, without intervention of the router. Nevertheless, the router should be protected from unauthorized connections to itself even from the inside, in case an attacker managed to gain control of an internal system and from there he or she tried to modify the configuration of the router to his or her needs.

The major vulnerabilities that the router could present are listed on Table 4. The first column, "ID" contains an identifier for the vulnerability for future reference. The second and third columns, "Vulnerability" and "Description", enumerate and describe the different vulnerabilities. The next two columns, "Exposure" and "Impact", show the probability of the vulnerability being exploited, and the impact that its successful exploitation would have, respectively, represented by a numeric value between 1 and 5. The numerical values are assigned corresponding to the subjective values "very low" (1), "low", "medium", "high" and "very high" (5). The last column, "Risk" represents the overall risk that the vulnerability poses to the system, computed as the sum of exposure and impact. Its value therefore ranges from 2 (lowest risk) to 10 (highest risk).

ID	Vulnerability	Description	Exposure	Impact	Risk
VU#1	Unnecessary services offered to the Internet.	The router may run network services accessible from the Internet. Those services might be vulnerable to some present or future attacks. Not being required, they represent an unnecessary risk.	4	5	9
VU#2	Unnecessary services offered to the LAN.	Idem., but in this case a potential vulnerability on those services would have to be attacked from the local area network, making it more difficult for the attacker.	3	5	8
VU#3	Necessary network services offered to the Internet with known vulnerabilities.	If a network service offered by the router to the Internet has known vulnerabilities, then it may be successfully attacked. In the case of a needed service, switching it off would not be an option as it would in VU#1.	5	5	10
VU#4	Necessary network services offered to the LAN with known vulnerabilities.	Idem., but in this case the attack would have to be launched from the LAN, making it more difficult for the attacker.	3	5	8
VU#5	Traffic allowed that should not be.	If the router allows traffic in or out that should not be allowed according to the policy, it may be exposing the internal systems to unwanted risks.	5	4	9
VU#6	Single points of failure (power, LAN, WAN, HW).	If any element of the router is not redundant, then the service may be affected if any of those elements fail.	2	2	4
VU#7	Blank or weak administration passwords.	If the router has blank or weak administration passwords, then an attacker that achieved access to an administrative interface (telnet, web or console) might easily take control of the router.	3	5	8
VU#8	Obsolete firmware revision.	If the router runs an old version of the firmware, it is very probable that it has vulnerabilities that have been solved in later updates.	2	3	5

Table 4 Potential vulnerabilities of the system and associated risk

1.3 Current state of practice

To the best of my knowledge there is no specific document available covering the hardening or secure configuration of a 3COM OfficeConnect Remote 812 ADSL Router. At least, I could not find one in the 3COM site [3CO01], nor in the CERT/CC site [CER01], nor in the SANS site [SAN01], nor in previous practicals posted on the GIAC website [GIA01] nor using Google [GOO01] extensively.

However, documents on how to secure routers in general and home routers in particular certainly apply to the router being audited. Examples of such documents are [CER02] and [CER03], where CERT/CC gives recommendations for home users to secure their home network and systems.

Document [NSA01], from the National Security Agency, contains "principles and guidance for secure configuration of IP routers with detailed instructions for Cisco Systems routers". Also, document [GRA01] describes how to harden Cisco routers step by step. Although the 3COM is configured in a different way than Cisco routers, most of the concepts of the hardening process can be easily ported to the 3COM router.

For this task, and to learn about all the different options available to configure the 3COM router, the best reference by far is the product manual [3CO02], which describes in detail the command line interface to configure the system.

Document [3CO03] explains how to set up HTTP filtering to prevent denial of service attacks against the web server of the router. In this particular case it won't be needed since the web service of the router is not necessary and therefore should be turned off, but the reference is included in case the reader may need it in some other instance.

Finally, the "CIS Gold Standard Benchmark for Cisco IOS Routers" [CIS01], contains a list of detailed checks for Cisco routers. Again, most of these checks may be translated to the 3COM OfficeConnect Remote 812 ADSL router.

2 Audit Checklist

This section compiles a list a checks that should be performed to evaluate the security of any device of the same model as the one being audited. Actually, many of them are generic and could be applied to any other border router connecting a small LAN to a WAN.

For every check the following items are detailed:

• Check ID:	An alphanumeric identifier for the check (e.g. CK#01).
• Check Title:	Short description of the check.
• References:	Publications with further information about the check.
• Risk:	Vulnerabilities related to the check (See Table 4)
• Testing Procedure:	Step-by-step procedure to perform the check.
• Evidence:	Screen output obtained when performing the check.
• Findings:	Conclusions derived from the evidence.

2.1 Response to WAN Stimuli

2.1.1 Check #1: Response to TCP SYN scan from WAN

Check ID

CK#01

Check Title

Response to TCP SYN scan from WAN

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#1, VU#3, VU#5

Testing Procedure

From a system connected to the Internet, outside the LAN of the audited system, send a TCP SYN packet to each TCP port between 0 and 65535, while at the same time saving a full network audit trail of the traffic of the LAN and also in the system connected to the Internet.

Note that a simple laptop would suffice to perform all the described tasks. The system would need an Ethernet card connected to the LAN and a modem to dial up to an ISP account. It could sniff the traffic going through the LAN and, separately, the traffic going through the phone line, while sending the desired traffic through the ISP.

The scan should be broken into 750-port blocks so that the NAT/PAT table of the router doesn't get filled, since that would make it discard packets that could otherwise get through. After each block of 750 packets, the table should be emptied by momentarily disabling and re-enabling the WAN connection of the router, using the following two commands at the router console:

```
disable vc Internet
enable vc Internet
```

Additionally, the following command shows the number of entries occupied in the table:

```
list nat vc Internet address
```

Note that typing "CTRL-P" (that's holding the CTRL key down and then pressing the "P" key) several times allows to navigate through the command history, making it easier to repeat the above commands very fast after each 750-port block.

The TCP SYN packets could be generated using the tool "hping" [SFI01] as follows, where "$TARGET" is the IP address of the destination system, if the scan didn't need to be split in blocks of 750 ports:

```
hping2 --syn --count 65536 --destport ++0 --quiet --numeric \
       --interval u100 <PUBLIC-IP>
```

To automate the process of sending blocks of 750 packets and then waiting until the table has been cleared, the following shell script can be used. It sends 750 TCP SYN packets to 750 consecutive ports and then waits until the user types a carriage return to send the next 750 packets and repeat the process.

```
#!/bin/sh
TARGET=<PUBLIC-IP>
#Note: When the port number goes above 65535 it cycles to 0,
#      therefore some low ports will be repeated in the traces.
let p=0
while [ $p -lt 65536 ]
do
  date
  command="time hping2 --syn --count 750 --destport ++$p --quiet  \
                       --numeric --interval u100 $TARGET"
  echo $command
  $command
  read dummy
  let p=p+750
done
date
```

The network audit trail in the LAN can be acquired using the tool "tcpdump" [TCP01], as follows:

```
tcpdump -nn -i eth0 -w ck01_eth0.tcpdump
```

The network audit trail in the modem line of the system sending the traffic can be acquired using the tool "tcpdump" [TCP01], as follows:

```
tcpdump -nn -i ppp0 -w ck01_ppp0.tcpdump
```

After all the TCP SYN packets have been sent, stop tcpdump typing "CTRL-C" both in the system connected to the LAN and in the system connected to the Internet.

Note that using a normal 33Kbps modem connection, the whole scan for the 65536 ports can take around 30 minutes to complete, including the stops to reset the connection table of the router.

Then, obtain the list of TCP SYN packets that got through the router and were seen on the LAN (list #01-01), using the following command in the system connected to the LAN:

```
tcpdump -nn -r ck01_eth0.tcpdump 'ip src <DIAL-UP-IP> and
(tcp[tcpflags] & tcp-syn != 0)'
```

Then, obtain the list of replies received by the system connected to the Internet coming from the public IP address of the target system (list #2), as follows:

```
tcpdump -nn -r ck01_ppp0.tcpdump 'ip src <PUBLIC-IP> and ip dst <DIAL-
UP-IP>'
```

The result of the check is PASS if all of the following conditions are met:

- List #01-01 only shows SYN packets with the destination ports expected to be forwarded to a server, in this case, ports 22 and 80.
- List #01-02 only shows packets from those same ports (22 and 80).

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.1.2 Check #2: Response to UDP scan from WAN

Check ID

CK#02

Check Title

Response to UDP scan from WAN

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#1, VU#3, VU#5

Testing Procedure

Follow the same steps as in CK#01 to send the traffic, but send UDP packets instead of TCP SYN packets, using the following script:

```
#!/bin/sh
TARGET=<PUBLIC-IP>
#Note: When the port number goes above 65535 it cycles to 0,
#      therefore some low ports will be repeated in the traces.
let p=0
while [ $p -lt 65536 ]
do
  date
  command="time hping2 --udp --count 750 --destport ++$p --quiet  \
                       --numeric --interval u100 $TARGET"
  echo $command
  $command
  read dummy
  let p=p+750
done
date
```

Also follow the same steps as in CK#01 to capture the network trace in the LAN, but then use the following command to obtain the list "List #02-01" of packets seen on the LAN coming from your dial-up IP address:

```
tcpdump -nn -r ck02_eth0.tcpdump 'ip src <DIAL-UP-IP>'
```

Then, obtain the list of replies received by the system connected to the Internet coming from the public IP address of the target system (List #02-02), in the same way as in CK#01:

```
tcpdump -nn -r ck02_ppp0.tcpdump 'ip src <PUBLIC-IP> and ip dst <DIAL-
UP-IP>'
```

Note that this whole procedure will take approximately the same amount of time as CK#01 to complete.

The result of the check is PASS if all of the following conditions are met:

- List #02-01 is empty.
- List #02-02 is empty.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.1.3 Check #3: Response to ICMP requests from WAN

Check ID

CK#03

Check Title

Response to ICMP requests from WAN

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#1, VU#3, VU#5

Testing Procedure

Using the same setup as in CK#01 and CK#02, send a collection of ICMP requests, as indicated below, to the public IP address of the router and record the traffic at the LAN and the dial up connection.

The following commands send different ICMP requests, namely "Echo", "Timestamp" and "Address Mask Request":

```
hping2 --icmp --icmptype 8  --count 1 <PUBLIC-IP>
hping2 --icmp --icmptype 13 --count 1 <PUBLIC-IP>
hping2 --icmp --icmptype 17 --count 1 <PUBLIC-IP>
```

After sending these three packets, stop the network traces and obtain the list of ICMP packets seen on the LAN (List #03-01) and the ICMP replies seen on the dial up line (List #03-02), using these commands:

```
tcpdump -nn -r ck03_eth0.tcpdump 'ip src <DIAL-UP-IP> and icmp'
tcpdump -nn -r ck03_ppp0.tcpdump 'ip src <PUBLIC-IP> and ip dst <DIAL-
UP-IP>'
```

The result of the check is PASS if all of the following conditions are met:

- List #03-01 is empty.
- List #03-02 is empty.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.1.4 Check #4: WAN traffic originated within the router

Check ID

CK#04

Check Title

WAN traffic originated within the router

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#5

Testing Procedure

Use the same setup as in CK#01, CK#02, and CK#03, except that you will not need the LAN traces this time. Additionally, log into the router command line interface (CLI) using a serial cable (RS-232) to connect your laptop to the console port of the router. Authenticate with the appropriate password if necessary. More details on how to set up the connection can be found in CK#07 and in the router documentation [3CO02].

Then, execute the following two commands in the router:

```
ping <DIAL-UP-IP>
CTRL-C
telnet <DIAL-UP-IP>
CTRL-C
```

Stop the network traces and obtain the list, List #04-01, of packets that arrived to your dial up connection from the router (source address equal to the public IP address of the router), using the following command:

```
tcpdump -nn -r ck04_ppp0.tcpdump 'src <PUBLIC-IP>'
```

The result of the check is PASS if all of the following conditions are met:

- List #04-01 is empty.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.1.5 Check #5: WAN ingress filtering

Check ID

CK#05

Check Title

WAN ingress filtering

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#1, VU#3, VU#5

Testing Procedure

Log into the console of the router and execute the following command:

```
show interface atm:1 settings
```

Check the value of "Filter Access". If it is set to "OFF" then the filters being applied to the WAN connection are those indicated in the fields "Input Filter" and "Output Filter" on the output of the above command.

However, if "Filter Access" is set to "ON" then the filters being applied to the WAN connection are those indicated in the fields "Input Filter" and "Output Filter" on the output of the following command, where "Internet" is the name of the virtual circuit associated with the WAN connection of the router:

```
show vc Internet
```

Verify that an input filter is listed on the line "Input Filter:" (e.g. filter_wan_in.flt) on the output of the appropriate of the two previous commands.

Next, obtain a copy of that file using TFTP, as indicated in the product documentation [3CO02].

Then, compare the contents of the filter with the following example. Any packets with source IP address belonging the private IP address space defined in RFC-1918, and packets with the router's own public IP address as the source IP address, should be rejected. Note that the real public IP address in the example has been changed to "10.10.10.10".

```
#filter

# Input filter for WAN interface

IP:
1 REJECT src-addr=10.0.0.0/8;       # Reject private source IPs (RFC-1918)
2 REJECT src-addr=172.16.0.0/12;    # Reject private source IPs (RFC-1918)
3 REJECT src-addr=192.168.0.0/16;   # Reject private source IPs (RFC-1918)
4 REJECT src-addr=10.10.10.10;      # Reject source my public IP (spoofing)
5 ACCEPT dst-addr=192.168.100.0/24; # Accept destination LAN
999 DENY;                           # Reject everything else

IP-RIP:
999 DENY;

IPX:
999 DENY;

IPX-RIP:
999 DENY;

IPX-SAP:
999 DENY;

BR-ETH:
999 DENY;
```

The syntax of the filters is discussed in detail in the product documentation [3CO02].

The result of the check is PASS if all of the following conditions are met:

- There is an input filter applied to the WAN virtual circuit interface.
- The filter states that the router must reject packets with source IP address belonging to the private address space defined in RFC-1918 or equal to the public IP address of the router.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.1.6 Check #6: WAN egress filtering

Check ID

CK#06

Check Title

WAN egress filtering

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#1, VU#3, VU#5

Testing Procedure

Follow the same steps outlined on the WAN ingress filtering check, but look for an "Output Filter" and compare its contents with the following example. Only traffic with source IP address belonging to the internal LAN should be allowed. This would prevent any unwanted reply of the router or any traffic generated in it to reach the Internet.

```
#filter

# Output filter for WAN interface

IP:
1 ACCEPT src-addr=192.168.100.0/24; # Accept source LAN
999 DENY;                           # Reject everything else
                                    # (including traffic generated
                                    #  by the router itself)

IP-RIP:
999 DENY;

IPX:
999 DENY;

IPX-RIP:
999 DENY;

IPX-SAP:
999 DENY;

BR-ETH:
999 DENY;
```

Again, the syntax of the filters is discussed in detail in the product documentation [3CO02].

The result of the check is PASS if all of the following conditions are met:

- There is an output filter applied to the WAN virtual circuit interface.
- The filter states that the router must accept packets with source IP address belonging to the internal LAN and reject any other packets.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.1.7 Check #7: CAN-2002-0888

Check ID

CK#07

Check Title

CAN-2002-0888

References

[CVE01]

Risk

VU#5

Testing Procedure

Using the same setup of check CK#01, send a few packets to public IP address of the router from the system in the Internet, to different TCP and UDP ports, for example using the following commands:

```
# hping2 --syn --count 3 --destport ++0     --numeric --interval u100 <PUBLIC-IP>
# hping2 --syn --count 3 --destport ++1000  --numeric --interval u100 <PUBLIC-IP>
# hping2 --syn --count 3 --destport ++20000 --numeric --interval u100 <PUBLIC-IP>
# hping2 --udp --count 3 --destport ++0     --numeric --interval u100 <PUBLIC-IP>
# hping2 --udp --count 3 --destport ++1000  --numeric --interval u100 <PUBLIC-IP>
# hping2 --udp --count 3 --destport ++20000 --numeric --interval u100 <PUBLIC-IP>
```

Those commands send sets of three packets to consecutive ports starting with port 0, 1000, and 20000, respectively. The first three commands send TCP SYN packets and the last three send UDP packets.

Then, on a different window, establish and keep open a connection to a TCP port that is forwarded to the server and open, such as TCP port 22 in this case, using the tool netcat [HOB01] as follows:

```
nc <PUBLIC-IP> 22
```

This should get the OpenSSH banner from the server displayed on your window. If it does not, verify that the SSH server is running in the target system.

Alternatively, a TELNET client can be used to connect to that port. I suggest netcat because it is easier to drop the connection after the test, simply type CTRL-C, as opposed to "CTRL-]" and then typing "close" for the telnet client:

```
telnet <PUBLIC-IP> 22
```

Now send a the same packets again, repeating the previous commands:

```
# hping2 --syn --count 3 --destport ++0     --numeric --interval u100 <PUBLIC-IP>
# hping2 --syn --count 3 --destport ++1000  --numeric --interval u100 <PUBLIC-IP>
# hping2 --syn --count 3 --destport ++20000 --numeric --interval u100 <PUBLIC-IP>
# hping2 --udp --count 3 --destport ++0     --numeric --interval u100 <PUBLIC-IP>
# hping2 --udp --count 3 --destport ++1000  --numeric --interval u100 <PUBLIC-IP>
# hping2 --udp --count 3 --destport ++20000 --numeric --interval u100 <PUBLIC-IP>
```

Then, stop the network trace at the LAN and obtain the list (List #07-01) of packets coming from the Internet system that got through the router to the server, using the following command:

```
tcpdump -nn -r ck07_eth0.tcpdump 'ip src <DIAL-UP-IP>'
```

The result of the check is PASS if all of the following conditions are met:

- The List #07-01 only contains packets destined to TCP port 22 and at most a reply or set of replies from TCP port 113 (ident). These port 113 packets are normal if the SSH server is configured to query the identd daemon of the client asking for the username of the remote user.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.2 Response to LAN Stimuli

2.2.1 Check #8: Response to TCP SYN scan from LAN

Check ID

CK#08

Check Title

Response to TCP SYN scan from LAN

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#2, VU#4, VU#5

Testing Procedure

Use the same setup of CK#01 except that the system needs to be connected only to the LAN (no need for dial-up connection to the Internet anymore).

Send the same set of TCP SYN packets (ports 0 to 65535) against the LAN IP address of the router and also against the public IP address of the router, using the following commands:

```
hping2 --syn --count 65536 --destport ++0 --quiet --numeric --interval u100
     192.168.100.254

hping2 --syn --count 65536 --destport ++0 --quiet --numeric --interval u100
     10.10.10.10
```

This time there is no need to split the scan in blocks of 750 packets because there is no NAT/PAT involved and therefore there is no danger of the NAT/PAT table filling up. This clearly speeds up the process.

Obtain the list of response packets sent by the router (List #08-01) using the following command:

```
$ tcpdump -nn -r ck08_eth0.tcpdump '(src host <LAN-ROUTER-IP> or src host
     <PUBLIC-IP>) and dst host <LAN-AUDITING-SYSTEM-IP> and not arp'
```

The result of the check is PASS if all of the following conditions are met:

- List #08-01 is empty.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.2.2 Check #9: Response to UDP scan from LAN

Check ID

CK#09

Check Title

Response to UDP scan from LAN

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#2, VU#4, VU#5

Testing Procedure

Follow the same steps as in CK#05 but send UDP packets instead of TCP SYN packets, using the following commands:

```
hping2 --udp --count 65536 --destport ++0 --quiet --numeric --interval u100
     <LAN-ROUTER-IP>
hping2 --udp --count 65536 --destport ++0 --quiet --numeric --interval u100
     <PUBLIC-IP>
```

Obtain the list of response packets sent by the router (List #09-01) using the following command:

```
$ tcpdump -nn -r ck09_eth0.tcpdump '(src host <LAN-ROUTER-IP> or src host
     <PUBLIC-IP>) and dst host <LAN-AUDITING-SYSTEM-IP> and not arp'
```

The result of the check is PASS if all of the following conditions are met:

- List #09-01 is empty.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.2.3 Check #10: Response to ICMP requests from LAN

Check ID

CK#10

Check Title

Response to ICMP requests from LAN

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#2, VU#4, VU#5

Testing Procedure

Use the same setup of CK#01 except that the system needs to be connected only to the LAN (no need for dial-up connection to the Internet).

Send the same set of ICMP requests to the LAN IP address of the router and also to the public IP address of the router, as indicated below. The following commands send different ICMP requests, namely "Echo", "Timestamp" and "Address Mask Request":

```
hping2 --icmp --icmptype 8  --count 1 <LAN-ROUTER-IP>
hping2 --icmp --icmptype 13 --count 1 <LAN-ROUTER-IP>
hping2 --icmp --icmptype 17 --count 1 <LAN-ROUTER-IP>
hping2 --icmp --icmptype 8  --count 1 <PUBLIC-IP>
hping2 --icmp --icmptype 13 --count 1 <PUBLIC-IP>
hping2 --icmp --icmptype 17 --count 1 <PUBLIC-IP>
```

After sending these packets, stop the network traces and obtain the list of replies seen on the LAN (List #10-01), using these command:

```
$ tcpdump -nn -r ck10_eth0.tcpdump '(src host <LAN-ROUTER-IP> or src host
     <PUBLIC-IP>) and dst host <LAN-AUDITING-SYSTEM-IP> and not arp'
```

The result of the check is PASS if all of the following conditions are met:

- List #10-01 is empty

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.2.4 Check #11: LAN traffic originated within the router

Check ID

CK#11

Check Title

LAN traffic originated within the router

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#5

Testing Procedure

Use the same setup as in CK#05 and CK#06. Additionally, log into the router command line interface (CLI) using a serial cable (RS-232) to connect your laptop to the console port of the router. Authenticate with the appropriate password if necessary. More details on how to set up the connection can be found in CK#07 and in the router documentation [3CO02].

Then, execute the following two commands in the router:

```
ping <LAN-AUDITING-SYSTEM-IP>
CTRL-C
telnet <LAN-AUDITING-SYSTEM-IP>
CTRL-C
```

Stop the network traces and obtain the list, List #11-01, of packets that arrived to your LAN interface from the router (source address equal to the LAN IP address of the router), using the following command:

```
$ tcpdump -nn -r ck11_eth0.tcpdump 'src host <LAN-ROUTER-IP> and dst host <LAN-
    AUDITING-SYSTEM-IP> and not arp'
```

The result of the check is PASS if all of the following conditions are met:

- List #11-01 is empty.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.2.5 Check #12: LAN ingress filtering

Check ID

CK#12

Check Title

LAN ingress filtering

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#2, VU#4, VU#5

Testing Procedure

Log into the console and execute the following command on the router to see the configuration of the Ethernet interface:

```
show interface eth:1 settings
```

Verify that an input filter is listed on the line "Input Filter:" (e.g. filter_lan_in.flt).

Next, obtain a copy of that file using TFTP, as indicated in the product documentation [3CO02].

Then, compare the contents of the filter with the following example. All packets addressed to the router (LAN or WAN addresses) or to broadcast addresses must be rejected except DHCP queries and ICMP packets. The rest of the packets with source IP address belonging to the local LAN must be allowed and any other packets must be rejected. Note that the real public IP address in the example has been changed to "10.10.10.10".

```
#filter

# Input filter for LAN interface

IP:
1 ACCEPT udp-dst-port=67;          # Accept DHCP queries
2 ACCEPT protocol=ICMP;            # Accept ICMP
3 REJECT dst-addr=192.168.100.254;  # Reject destination router-LAN
4 REJECT dst-addr=10.10.10.10;      # Reject destination router-WAN
5 REJECT dst-addr=192.168.100.255;  # Reject destination broadcast LAN
6 REJECT dst-addr=255.255.255.255;  # Reject destination broadcast global
7 ACCEPT src-addr=192.168.100.0/24; # Accept source LAN
999 DENY;                           # Reject everything else

IP-RIP:
999 DENY;

IPX:
999 DENY;

IPX-RIP:
999 DENY;

IPX-SAP:
999 DENY;
```

```
BR-ETH:
999 DENY;
```

The syntax of the filters is discussed in detail in the product documentation [3CO02].

The result of the check is PASS if all of the following conditions are met:

- There is an input filter applied to the LAN interface.
- The filter states that the router must reject the packets with the criteria explained above.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.2.6 Check #13: LAN egress filtering

Check ID

CK#13

Check Title

LAN egress filtering

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#2, VU#4, VU#5

Testing Procedure

Follow the same steps outlined on the LAN ingress filtering check, but look for an "Output Filter" and compare its contents with the following example. Any packets with a source IP address of the router (LAN or WAN) must be rejected except DHCP replies and ICMP packets. Then, only traffic with destination IP address belonging to the internal LAN must be allowed and anything else must be rejected. This will prevent any unwanted reply of the router or any traffic generated in it to reach the LAN.

```
#filter

# Output filter for LAN interface

IP:
1 ACCEPT udp-src-port=67;           # Accept DHCP replies
2 ACCEPT protocol=ICMP;             # Accept ICMP
3 REJECT src-addr=192.168.100.254;  # Reject source router-LAN
4 REJECT src-addr=10.10.10.10;      # Reject source router-WAN
5 ACCEPT dst-addr=192.168.100.0/24; # Accept destination LAN
999 DENY;                           # Reject everything else

IP-RIP:
999 DENY;

IPX:
999 DENY;

IPX-RIP:
999 DENY;

IPX-SAP:
999 DENY;

BR-ETH:
999 DENY;
```

Again, the syntax of the filters is discussed in detail in the product documentation [3CO02].

The result of the check is PASS if all of the following conditions are met:

- There is an output filter applied to the LAN interface.
- The filter states that the router must reject the packets with the criteria explained above.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.3 Active Services

2.3.1 Check #14: TELNET & HTTP access

Check ID

CK#14

Check Title

TELNET & HTTP access

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#1, VU#2

Testing Procedure

Log into the console of the router and execute the following command:

```
list services
```

This displays the list of network services defined in the router. Note any services with the value "TELNETD" or "HTTPD" in the "Server Type" column and check whether they are enabled by looking at the corresponding value (ENABLED/DISABLED) in the "Admin Status" column.

The result of the check is PASS if all of the following conditions are met:

- There is no TELNETD service or it is DISABLED.
- There is no HTTPD service or it is DISABLED.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.3.2 Check #15: SNMP access

Check ID

CK#15

Check Title

SNMP access

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#1, VU#2

Testing Procedure

Log into the console of the router and execute the following command:

```
list snmp communities
```

This displays the list of SNMP community names that can be used to access the SNMP server of the router, together with the IP addresses from which this access can be exercised and the type of access (read-only or read-write) allowed. If no community name is defined, the router will not reply to any SNMP query.

The result of the check is PASS if all of the following conditions are met:

- The list of SNMP community names is empty.

Otherwise, the result of the check is FAIL.

Note that in the case of SNMP, it is irrelevant whether there is a network service listed ("list services") with server type "SNMPD" or if it is disabled: if an SNMP community has been defined, the router will honor those requests. That is true even if the security options are both set to "DISABLED"/"OFF" as in this example:

```
3Com-DSL>show security_option

SECURITY OPTION SETTINGS
SNMP User Access:                         DISABLED
Administration by Remote User:            OFF
3Com-DSL>
```

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.4 Console Protection

2.4.1 Check #16: Console password enabled

Check ID

CK#16

Check Title

Console password enabled

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#7

Testing Procedure

Connect your laptop to the console port of the router using a serial cable (RS-232). Connect a terminal to the serial port using the following settings: 9600 bps, 8 bits, parity none, 1 stop bit. More details on how to set up the connection can be found in the router documentation [3CO02].

Type a few carriage returns until a message appears. If no message is shown, re-check the cable and the connection settings.

Then, type a non-valid command (e.g. "foo") and press ENTER.

The result of the check is PASS if the following message is displayed by the router in response to the non-valid command:

The result of the check is PASS if all of the following conditions are met:

- The following message is displayed by the router in response to the non-valid command, asking for a password:

```
Password: ***

Login incorrect
Password:
```

Otherwise, the result of the check is FAIL.

Note that if the console didn't require a password, the following message would be displayed instead:

```
3Com-DSL>foo
CLI - Invalid Argument: foo

This field is a KEYWORD. The possible values are:
ADD                      HELP                     RESET
ARP                      HISTORY                  RESOLVE
[--other commands omitted---]
EXIT                     RECONFIGURE
HANGUP                   RENAME
3Com-DSL>
```

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.4.2 Check #17: Timeout for idle sessions

Check ID

CK#17

Check Title

Timeout for idle sessions

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#7

Testing Procedure

Log into the console as described in CK#07, providing the appropriate password if necessary.

Then, execute the following command on the router console:

```
show command settings
```

Record the value indicated at the right hand side of the line starting with "Console Idle Timeout:". Valid values range from 0 (no timeout) to 60 (60 minutes).

The following is an example of output from this command:

```
3Com-DSL>show command settings

COMMAND SETTINGS
History Depth:                          100
Current Prompt:                         3Com-DSL>
Local Prompt:                           3Com-DSL>
Console Login Required:                 YES
Console Idle Timeout:                   10
Current Idle Timeout:                   10
3Com-DSL>
```

The result of the check is PASS if all of the following conditions are met:

- The value of "Console Idle Timeout" is greater than zero.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.4.3 Check #18: Password strength

Check ID

CK#18

Check Title

Password strength

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#7

Testing Procedure

This check assumes that the result of check CK#07 was PASS and therefore a password is required to log into the console of the router. If that condition is not met, this check should automatically be considered FAIL.

Connect your laptop to the console port of the router using a serial cable (RS-232). Connect a terminal to the serial port using the following settings: 9600 bps, 8 bits, parity none, 1 stop bit. More details on how to set up the connection can be found in the router documentation [3CO02].

Type a few carriage returns until the message "Password:" appears. If no message is shown, re-check the cable and the connection settings.

Then, try to log in using trivial passwords like "" (blank password), "secret", "password", "3com", "susan" (name of the owner of the system), " " (blank space), "root", "admin", "adminttd", "tech" and "recovery". A script that could automate the password checking using a dictionary file would be preferred.

The result of the check is PASS if all of the following conditions are met:

- None of these passwords allows you in.

Otherwise, the result of the check is FAIL.

Note that if any of the passwords would allow you in, the prompt would change from "Password:" to something similar to (the prompt is configurable) "3Com-DSL> ".

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

2.5 Firmware

2.5.1 Check #19: Firmware version

Check ID

CK#19

Check Title

Firmware version

References

[CER02] [NSA01] [GRA01] [3CO02] [CIS01]

Risk

VU#8

Testing Procedure

Log into the console as described in CK#07, providing the appropriate password if necessary.

Then, execute the following command on the router console:

```
show system settings
```

Record the value indicated at the right hand side of the line starting with "System Version:".

The following is an example of output from this command:

```
3Com-DSL>show system settings
```

```
SYSTEM DESCRIPTION
System Descriptor:
        3Com OfficeConnect Remote ADSL 812 V1.1.9, Built on Jun  1 2001
at 14:22:58.
Object ID:                                ( 1.3.6.1.4.1.429.2.13 )
System UpTime:                            0d 10:23:48
System Contact:                           none
System Name:                              none
System Location:                          none
System Services:                          Internet EndToEnd
Applications
System Version:                           V1.1.9
3Com-DSL>
```

Check which is the most current version of firmware available for the OfficeConnect Remote 812 ADSL Router at the 3COM web site [3CO04]. At the time of this writing, the most current version available (for P/N 3CP204144) is 1.1.9.4, downloadable as a zip file named "bld_1_1_9_4.zip". Since the product is already discontinued it is very probable that this version remains the most current version of the firmware for ever.

However, note that the "show system command" does not specify which sub-version of 1.1.9 is installed. In order to be sure that the release installed is actually 1.1.9.4, the MD5 hash of the main executable file should be compared with the following value, which was obtained from a router running version 1.1.9.4 of the firmware:

File name:	mr010000.exe
MD5 hash:	6be97bd45216410b51f2730a4aa384bd

The existence of the file on the router can be confirmed typing the following command in the router console: "list files".

In order to calculate the file size and MD5 hash, the file will need to be copied to a workstation using tftp ("get mr010000.exe") as described in the product documentation [3CO02]. Once in the workstation, if it is a Linux system, the following command yields the MD5 hash of the file:

```
md5sum mr010000.exe
```

The result of the check is PASS if all of the following conditions are met:

- The value displayed under "System Version:" matches the most current version available of the firmware, in this case, V1.1.9.

- The MD5 hash of file "mr010000.exe" matches that of a copy of that file known to belong to the most current version (and sub-version) of the firmware. In this case (version 1.1.9.4) see the value in the table above.

Otherwise, the result of the check is FAIL.

Objectivity

This check is objective.

Evidence

[place marker]

Findings

[place marker]

3 Audit Completion: Tests, Evidence and Findings

This section contains the evidence and findings obtained for a selection of ten checks, the most critical, actually performed to the system being audited: CK#01, CK#02, CK#04, CK#07, CK#08, CK#09, CK#15, CK#16, CK#17, CK#19.

Please note that the dial-up (public) IP address of the auditing system has been replaced by 10.22.22.22 for privacy reasons. The internal (LAN) address of the auditing system is 192.168.100.100 (used when performing internal tests).

3.1 Response to WAN Stimuli

3.1.1 Check #1: Response to TCP SYN scan from WAN

Check ID

CK#01

Check Title

Response to TCP SYN scan from WAN

Evidence

List #01-01 (SYN packets seen in the LAN):

```
# tcpdump -nn -r ck01_eth0.tcpdump 'ip src 10.22.22.22 and (tcp[tcpflags] &
     tcp-syn != 0)'
11:08:38.714736 10.22.22.22.2569 > 192.168.100.50.22: S 817646005:817646005(0)
     win 512
11:08:38.715423 10.22.22.22.2571 > 192.168.100.50.24: S 504375473:504375473(0)
     win 512
11:08:38.727750 10.22.22.22.2572 > 192.168.100.50.25: S 306953006:306953006(0)
     win 512
11:08:38.729301 10.22.22.22.2573 > 192.168.100.50.26: S 209719522:209719522(0)
     win 512
[...SYN to consecutive ports omitted...]
11:08:38.947952 10.22.22.22.2586 > 192.168.100.50.39: S 758535991:758535991(0)
     win 512
11:08:38.951181 10.22.22.22.2585 > 192.168.100.50.38: S
     1916804715:1916804715(0) win 512
11:08:38.952876 10.22.22.22.2587 > 192.168.100.50.40: S
     2050648950:2050648950(0) win 512
11:08:39.476475 10.22.22.22.2627 > 192.168.100.50.80: S 262113781:262113781(0)
     win 512
11:08:39.480603 10.22.22.22.2628 > 192.168.100.50.81: S 248944763:248944763(0)
     win 512
11:08:39.482235 10.22.22.22.2629 > 192.168.100.50.82: S
     1047836880:1047836880(0) win 512
[...SYN to consecutive ports omitted...]
11:08:39.702490 10.22.22.22.2646 > 192.168.100.50.99: S
     1802900253:1802900253(0) win 512
11:08:39.704046 10.22.22.22.2647 > 192.168.100.50.100: S
```

```
     2066341870:2066341870(0) win 512
[...sequence repeated for ports 22 to 97...]
#
```

List #01-02 (responses from the target)

```
# tcpdump -nn -r ck01_ppp0.tcpdump 'ip src 10.10.10.10 and ip dst 10.22.22.22'
11:08:38.789130 10.10.10.10.23 > 10.22.22.22.2570: R 0:0(0) ack 1601316198 win
     0
11:08:38.799125 10.10.10.10.22 > 10.22.22.22.2569: S 1826664714:1826664714(0)
     ack 817646006 win 5840 <mss 1460> (DF)
11:08:38.809125 10.10.10.10.24 > 10.22.22.22.2571: R 0:0(0) ack 504375474 win 0
     (DF)
[...RST to consecutive ports omitted...]
11:08:39.049138 10.10.10.10.40 > 10.22.22.22.2587: R 0:0(0) ack 2050648951 win
     0 (DF)
11:08:39.559127 10.10.10.10.80 > 10.22.22.22.2627: S 1818340706:1818340706(0)
     ack 262113782 win 5840 <mss 1460> (DF)
11:08:39.609135 10.10.10.10.81 > 10.22.22.22.2628: R 0:0(0) ack 248944764 win 0
     (DF)
11:08:39.609139 10.10.10.10.82 > 10.22.22.22.2629: R 0:0(0) ack 1047836881 win
     0 (DF)
[...RST to consecutive ports omitted...]
11:08:39.819133 10.10.10.10.100 > 10.22.22.22.2647: R 0:0(0) ack 2066341871 win
     0 (DF)
11:09:08.499142 10.10.10.10.1214 > 10.22.22.22.2897: S 2093487455:2093487455(0)
     ack 345812910 win 5840 <mss 1460> (DF)
11:10:42.029127 10.10.10.10.4662 > 10.22.22.22.1693: S 836274891:836274891(0)
     ack 521915859 win 2920 <mss 1460> (DF)
11:11:23.589129 10.10.10.10.6346 > 10.22.22.22.1487: S 2220410185:2220410185(0)
     ack 294777444 win 5840 <mss 1460> (DF)
11:11:23.589136 10.10.10.10.6347 > 10.22.22.22.1488: S 866215771:866215771(0)
     ack 22936219 win 2920 <mss 1460> (DF)
11:11:23.589140 10.10.10.10.6348 > 10.22.22.22.1489: S 2229252894:2229252894(0)
     ack 880022489 win 5840 <mss 1460> (DF)
11:11:27.429133 10.10.10.10.6699 > 10.22.22.22.1840: S 2229281838:2229281838(0)
     ack 148291563 win 5840 <mss 1460> (DF)
[...sequence repeated for ports 22 to 97...]
#
```

Findings

In List #01-01 it can be seen that the first packet that crossed the router was the one with destination port 22 and it was redirected to the internal server 192.168.100.50 as expected. However, immediately after, packets sent to ports 24 to 40 were also redirected to the same internal server by the router. That wasn't expected. Note that the packet sent to port 23 was not redirected by the router.

The same happens again a moment later, when the packet directed to port 80 was redirected to the internal server as expected, and then packets sent to ports

81 to 100 were unexpectedly redirected to the same internal server by the router.

Finally, the same sequence is repeated for ports 22 to 97 because the script repeated the sending of the first packets. This doesn't add anything except that the facts are reproducible.

List #01-02 shows a reply (RST) from port 23. Given the fact that the packet destined to port 23 was not seen on the LAN (List #01-01), this reply must have been sent by the router itself or some kind of transparent proxy. It is a RST packet, meaning that the port is closed, which is good, but it means that if the TELNET server was started on the router at any time it would be accessible from the Internet, which is not good.

Then, List #2 shows positive responses (SYN/ACK) from ports 22 and 80, as expected, but also from ports 1214, 4662, 6346, 6347, 6348 and 6699. That could be worrying, because the SYN packets to those ports were not seen on the LAN, meaning that the router itself could be accepting connections on those ports. However, the most probable explanation for these replies is that the ISP is using some kind of transparent proxy for those ports. All these ports are commonly used by peer-to-peer (P2P) file sharing applications, like Kazaa (1214), e-mule/eDonkey (4662), Gnutella (6346, 6347, 6348) and Napster (6699). The test was repeated for these specific ports (including port 23, TELNET) from a different dial-up ISP and the only reply this time was a RST packet from port 23, confirming that the router was not listening on those P2P ports but it was indeed responding to connection attempts to the TELNET port.

Obviously, both lists show more packets than those corresponding to ports 22 and 80. Therefore, the result of this check is **FAIL**.

3.1.2 Check #2: Response to UDP scan from WAN

Check ID

CK#02

Check Title

Response to UDP scan from WAN

Evidence

List #02-01 (UDP packets seen in the LAN):

```
# tcpdump -nn -r ck02_eth0.tcpdump 'ip src 10.22.22.22'
#
```

List #02-02 (responses from the target)

```
# tcpdump -nn -r ck02_ppp0.tcpdump 'ip src 10.10.10.10 and ip dst 10.22.22.22'|
     less
11:43:04.729124 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 80
     unreachable
11:43:04.759128 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 81
     unreachable
11:43:04.779143 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 82
     unreachable
11:43:04.779149 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 83
     unreachable
11:43:04.779153 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 85
     unreachable
11:43:04.789131 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 84
     unreachable
[...consecutive ports omitted...]
11:43:05.619128 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 159
     unreachable
11:43:05.629126 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 160
     unreachable
11:43:05.639122 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 162
     unreachable
11:43:05.639129 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 163
     unreachable
[...consecutive ports omitted...]
11:43:12.759139 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 748
     unreachable
11:43:12.779126 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 747
     unreachable
11:43:12.779132 10.10.10.10 > 10.22.22.22: icmp: 10.10.10.10 udp port 749
     unreachable
[...sequence repeated for ports 80 to 463...]
```

Findings

List #02-01 is empty, as expected. No UDP packet was redirected by the router to any system in the LAN.

However, List #02-02 shows many ICMP "port unreachable" replies, sent by the router itself. The first reply corresponds to port 80. Then, replies are received for all consecutive ports included in the same set of 750 packets (up to port 749) except for port 161 (SNMP). This indicates that the router is listening on that UDP port. The fact that the router began to reply to the UDP packets when it received the packet destined to port 80 can be explained by the combination of the following two factors: the router does not forward packets destined to port 80 (both TCP or UDP) unless there are explicit rules in its configuration for those specific ports (regardless of the "Default NAT Address"), instead it sends the packet to its internal daemons and processes; then, the second factor is that the router must have the feature "INTELLIGENT NAT OPTION" enabled. This is explained in detail in CK#7 where the system is checked for the CAN-2002-0888 vulnerability.

NOTE: From my experience, the router does not forward the following ports *(regardless of the Default NAT Address) unless there is a explicit PAT rule for them in the configuration. Instead, it sends the packets destined to these ports to its internal daemons and processes (unless an input filter rejects them):*

TCP:	*23, 80, 1755, 64098*
UDP:	*69, 80, 161, 520, 1755*

The ports that did not provoke a response were either redirected by the router to the default NAT address and because that IP was not active they were silently dropped by the router, or processed by the router and there was a process listening on that port inside the router.

In any case, the safe bet is to put an input filter on the WAN interface that drops any packet that happens to be destined to the router after the PAT module has processed it. An example of this kind of filter is shown on CK#5.

List #02-01 was empty, as expected, but List #02-02 was not. Therefore, the result of this check is **FAIL**.

3.1.3 Check #4: WAN traffic originated within the router

Check ID

CK#04

Check Title

WAN traffic originated within the router

Evidence

Commands executed in the router:

```
3Com-DSL>ping 10.22.22.22
3Com-DSL>10.22.22.22 is alive
3Com-DSL>telnet 10.22.22.22
Trying 10.22.22.22 ...
3Com-DSL>
```

List #04-01 (packets arrived to the dial-up IP address from the router)

```
# tcpdump -nn -r ck04_ppp0.tcpdump 'src 10.10.10.10'
19:16:42.629137 10.10.10.10 > 10.22.22.22: icmp: echo request
19:16:58.709141 10.10.10.10.1025 > 10.22.22.22.23: S 2114024000:2114024000(0)
     win 1024 <mss 536>
19:17:01.719144 10.10.10.10.1025 > 10.22.22.22.23: S 2114024000:2114024000(0)
     win 1024 <mss 536>
19:17:07.719140 10.10.10.10.1025 > 10.22.22.22.23: S 2114024000:2114024000(0)
     win 1024 <mss 536>
#
```

Findings

In List #04-01 it can be seen that both the ICMP echo request (ping) and the telnet connection attempt (SYN packets to port 23) arrived to the system connected the Internet, indicating that there is no output filter preventing the traffic originated in the router to reach the Internet.

List #04-01 was not empty. Therefore, the result of this check is **FAIL**.

3.1.4 Check #7: CAN-2002-0888

Check ID

CK#07

Check Title

CAN-2002-0888

Evidence

List #07-01 (packets that made it to the LAN):

```
# tcpdump -nn -r ck07_eth0.tcpdump 'ip src 10.22.22.22'
21:34:25.230097 10.22.22.22.32783 > 192.168.100.50.22: S
     2225799746:2225799746(0) win 4452 <mss 1484,sackOK,timestamp 4271715
     0,nop,wscale 0> (DF)
21:34:25.409177 10.22.22.22.32783 > 192.168.100.50.22: . ack 860069442 win 4452
     <nop,nop,timestamp 4271736 7976932> (DF)
21:34:25.599219 10.22.22.22.113 > 192.168.100.50.32795: R 0:0(0) ack 853112857
     win 0 (DF)
21:34:25.809168 10.22.22.22.32783 > 192.168.100.50.22: . ack 45 win 4452
     <nop,nop,timestamp 4271776 7976955> (DF)
21:34:35.269166 10.22.22.22.1141 > 192.168.100.50.1: S 1020570770:1020570770(0)
     win 512
21:34:35.279206 10.22.22.22.1142 > 192.168.100.50.2: S 480670199:480670199(0)
     win 512
21:35:08.399300 10.22.22.22.1139 > 192.168.100.50.1000: S
     1810213719:1810213719(0) win 512
21:35:08.409231 10.22.22.22.1140 > 192.168.100.50.1001: S
     637685614:637685614(0) win 512
21:35:08.479389 10.22.22.22.1141 > 192.168.100.50.1002: S
     984427523:984427523(0) win 512
21:35:15.629233 10.22.22.22.1447 > 192.168.100.50.20000: S
     499260717:499260717(0) win 512
21:35:15.630453 10.22.22.22.1448 > 192.168.100.50.20001: S
     714014624:714014624(0) win 512
21:35:15.691765 10.22.22.22.1449 > 192.168.100.50.20002: S
     1116920029:1116920029(0) win 512
21:35:21.409301 10.22.22.22.2405 > 192.168.100.50.1: udp 0
21:35:21.480613 10.22.22.22.2406 > 192.168.100.50.2: udp 0
```

```
21:35:36.389317 10.22.22.22.2661 > 192.168.100.50.1000: udp 0
21:35:36.390540 10.22.22.22.2662 > 192.168.100.50.1001: udp 0
21:35:36.459169 10.22.22.22.2663 > 192.168.100.50.1002: udp 0
21:35:47.219703 10.22.22.22.2896 > 192.168.100.50.20000: udp 0
21:35:47.231900 10.22.22.22.2897 > 192.168.100.50.20001: udp 0
21:35:47.311830 10.22.22.22.2898 > 192.168.100.50.20002: udp 0
21:36:10.249237 10.22.22.22.32783 > 192.168.100.50.22: F 0:0(0) ack 45 win 4452
     <nop,nop,timestamp 4282220 7976955> (DF)
21:36:10.439397 10.22.22.22.32783 > 192.168.100.50.22: . ack 46 win 4452
     <nop,nop,timestamp 4282239 7982644> (DF)
#
```

Findings

List #07-01 shows that only the packets sent before the connection to port 22 were not forwarded by the router to the server (they don't appear on the list) and also that all packets sent after the connection to port 22, except those destined to port 0, were forwarded. This indicates that the router exhibits the vulnerability CAN-2002-0888: once a packet is forwarded by the router to a server because of a port address translation (PAT), then all subsequent packets with the same source IP will be forwarded to the same server, irrespective of the settings of the static PAT table or the default NAT address configured. This exposes the internal server to unwanted and potentially malicious traffic from the Internet.

List #07-01 contains more packets than those destined to port 22 or from port 113. Therefore, the result of this check is **FAIL**.

3.2 Response to LAN Stimuli

3.2.1 Check #8: Response to TCP SYN scan from LAN

Check ID

CK#08

Check Title

Response to TCP SYN scan from LAN

Evidence

List #08-01 (reply packets from the router):

```
$ tcpdump -nn -r ck08_eth0.tcpdump '(src host 192.168.100.254 or src host
     10.10.10.10) and dst host 192.168.100.100 and not arp'

22:25:47.697522 192.168.100.254.0 > 192.168.100.100.2469: R 0:0(0) ack
     395739139 win 0
22:25:47.703173 192.168.100.254.1 > 192.168.100.100.2470: R 0:0(0) ack
     1750813313 win 0
22:25:47.717197 192.168.100.254.2 > 192.168.100.100.2471: R 0:0(0) ack
```

```
     1165836288 win 0
22:25:47.737135 192.168.100.254.3 > 192.168.100.100.2472: R 0:0(0) ack
     1598762942 win 0
[...]
22:37:19.171254 10.10.10.10.0 > 192.168.100.100.2836: R 0:0(0) ack 1128728333
     win 0
22:37:19.173617 10.10.10.10.1 > 192.168.100.100.2837: R 0:0(0) ack 332473307
     win 0
22:37:19.185746 10.10.10.10.2 > 192.168.100.100.2838: R 0:0(0) ack 1481286841
     win 0
22:37:19.193780 10.10.10.10.3 > 192.168.100.100.2839: R 0:0(0) ack 613237314
     win 0
[...]
```

Findings

List #8 shows that the router responded to every SYN packet with a RST packet. This is good in part, because it means that all TCP ports were closed in the router. However, it is bad because it means that the router does process those TCP connection requests and responds to them. Should a TCP service be enabled in the router at any time, it would be accessible from the LAN, and it could be left like that, forgotten. The recommended setup includes setting up a filter to discard any TCP packets directed to the router, as it is suggested in CK#12 (LAN ingress filtering).

List #08-01 was not empty. Therefore, the result of this check is **FAIL**.

3.2.2 Check #9: Response to UDP scan from LAN

Check ID

CK#09

Check Title

Response to UDP scan from LAN

Evidence

List #09-01 (reply packets from the router):

```
$ tcpdump -nn -r ck09_eth0.tcpdump '(src host 192.168.100.254 or src host
     10.10.10.10) and dst host 192.168.100.100 and not arp'

22:51:05.702277 192.168.100.254 > 192.168.100.100: icmp: 192.168.100.254 udp
     port 0 unreachable
22:51:05.703634 192.168.100.254 > 192.168.100.100: icmp: 192.168.100.254 udp
     port 1 unreachable
22:51:05.718182 192.168.100.254 > 192.168.100.100: icmp: 192.168.100.254 udp
     port 2 unreachable
22:51:05.724363 192.168.100.254 > 192.168.100.100: icmp: 192.168.100.254 udp
     port 3 unreachable
```

```
[...]
22:51:06.353586 192.168.100.254 > 192.168.100.100: icmp: 192.168.100.254 udp
     port 66 unreachable
22:51:06.381873 192.168.100.254.2049 > 192.168.100.100.514: udp 91
22:51:06.383824 192.168.100.254 > 192.168.100.100: icmp: 192.168.100.254 udp
     port 69 unreachable
[...]
22:51:06.913565 192.168.100.254 > 192.168.100.100: icmp: 192.168.100.254 udp
     port 122 unreachable
22:51:06.932451 192.168.100.254.2049 > 192.168.100.100.514: udp 84
22:51:06.933430 192.168.100.254 > 192.168.100.100: icmp: 192.168.100.254 udp
     port 124 unreachable
[...]
```

Findings

List #09-01 shows that the router responded to *most* UDP packets with a ICMP port unreachable packet. This means that most UDP ports were closed in the router, but it also means that some of them were open. At any rate, the recommended setup includes setting up a filter to discard any UDP packets directed to the router, except for the DHCP queries (if the DHCP service is desired), as it is suggested in CK#12 (LAN ingress filtering).

List #09-01 was not empty. Therefore, the result of this check is **FAIL**.

3.3 Active Services

3.3.1 Check #15: SNMP access

Check ID

CK#15

Check Title

SNMP access

Evidence

Output from the command:

```
3Com-DSL>list snmp communities

SNMP COMMUNITIES
Community Name                     IP Address      Access
3Com-DSL>
```

Findings

The list of SNMP community names is empty. Therefore, the result of this check is **PASS**.

3.4 Console Protection

3.4.1 Check #16: Console password enabled

Check ID

CK#16

Check Title

Console password enabled

Evidence

Output on the console when typing "foo" and pressing RETURN on the console of the router:

```
Password: ***

Login incorrect
Password:
```

Findings

The console required a password. Therefore, the result of this check is **PASS**.

3.4.2 Check #17: Timeout for idle sessions

Check ID

CK#17

Check Title

Timeout for idle sessions

Evidence

Output of the command:

```
3Com-DSL>show command settings

COMMAND SETTINGS
History Depth:                            20
```

```
Current Prompt:                          3Com-DSL>
Local Prompt:                            3Com-DSL>
Console Login Required:                  YES
Console Idle Timeout:                    15
Current Idle Timeout:                    15
3Com-DSL>
```

Findings

The value of "Console Idle Timeout" was greater than zero. Therefore, the result of this check is **PASS**.

3.5 Firmware

3.5.1 Check #19: Firmware version

Check ID

CK#19

Check Title

Firmware version

Evidence

Output from the "show system settings" command:

```
3Com-DSL>show system settings

SYSTEM DESCRIPTION
System Descriptor:
        3Com OfficeConnect Remote ADSL 812 V1.1.9, Built on Jun  1 2001
at 14:22:58.
Object ID:                               ( 1.3.6.1.4.1.429.2.13 )
System UpTime:                           0d 06:04:51
System Contact:                          none
System Name:                             none
System Location:                         none
System Services:                         Internet EndToEnd
Applications
System Version:                          V1.1.9
3Com-DSL>
```

MD5 hash of file "mr010000.exe":

```
$ md5sum mr010000.exe
6be97bd45216410b51f2730a4aa384bd  mr010000.exe
$
```

Findings

The value displayed under "System Version:" matched the most current version available of the firmware, in this case, V1.1.9, and the MD5 hash of file "mr010000.exe" matches that of a copy of that file known to belong to the most current version (and sub-version) of the firmware, in this case version 1.1.9.4: 6be97bd45216410b51f2730a4aa384bd.

Therefore, the result of this check is **PASS**.

4 Audit Report

4.1 Executive Summary

This report is the result of a security audit conducted by David Perez, on March 2004, analyzing the border router of Susan Smith's home office network. The system is a “3COM OfficeConnect Remote 812 ADSL Router" [3CO01], with product number "3CP204144" and serial number “HLY21XXXXXXX”.

The objective of the audit was to analyze the security posture of the router with regards to the security of the information assets accessed through it, and identify ways to improve it, if necessary, in a cost effective manner.

A series of checks was performed on the system and the evidence obtained form each check was analyzed to obtain some findings from which to derive a set of recommendations to improve the security of the system. All the relevant information generated with the checks and its analysis is included in this report.

The objective of the audit was successfully achieved.

4.2 Findings

Table 5 summarizes the results (“PASS” or “FAIL”) of each check performed to the system:

Check ID	Description	Result
CK#01	Response to TCP SYN scan from WAN	FAIL
CK#02	Response to UDP scan from WAN	FAIL
CK#04	WAN traffic originated within the router	FAIL
CK#07	CAN-2002-0888	FAIL
CK#08	Response to TCP SYN scan from LAN	FAIL
CK#09	Response to UDP scan from LAN	FAIL
CK#15	SNMP access	PASS
CK#16	Console password enabled	PASS
CK#17	Timeout for idle sessions	PASS
CK#19	Firmware version	PASS

Table 5 Check results

The rest of this section describes the main findings obtained from the results of the checks performed. Further details on how these findings were obtained and evidence backing them up, are given in sections 2 and 3.

4.2.1 Positive findings

- Administrative access to the system is limited to the serial console only (the services TELNET, HTTP and SNMP are disabled.) and access to the console is protected by password and automatic disconnection of idle sessions (timeout). This is very good practice for preventing potential attackers from changing the configuration of the device.

  See checks CK#15, CK#16 and CK#17 for further information.

- The version of the firmware running on the router is the latest supported version available. This is very good practice for avoiding old vulnerabilities from previous versions of the firmware.

  See check CK#19 for further information.

4.2.2 Negative findings

- The router exhibits the vulnerability CAN-2002-0888, allowing an external attacker to send traffic to any TCP or UDP port of any internal system instead of only allowing communication to certain ports on specific internal systems. This represents a very high risk to the internal systems, which could be running vulnerable network services that an external attacker should never be allowed to access.

  See checks CK#01, CK#02, CK#07, CK#08 and CK#09 for further information.

- Traffic addressed to or generated by the router itself is not being filtered for any of its network interfaces (LAN and WAN). This represents a high risk to the router because it gives external and internal attackers free way to connect to any network service running on the router. Some of these services could be vulnerable or become vulnerable in the future and there is no way to tell exactly which services are running on the router.

  See checks CK#01, CK#02, CK#04, CK#08 and CK#09 for further information.

4.3 Recommendations

These are the main recommendations to help improve the security of the router subject of this audit:

- Eliminate the vulnerability CAN-2002-0888 [CVE01] by simply disabling the “intelligent NAT option” (that is achieved with a single command), at no cost at all (5 minutes of manpower). The only thing to bear in mind is that if in the future some internal server needs to receive external traffic on ports not corresponding to any previous outgoing traffic, those ports will have to be mapped by hand in the configuration of the device. This would solve the problem described in the first negative finding.
- Filter out any traffic directly addressed to or generated within the router itself by applying input and output filters like the ones shown on section 2 to both the LAN and the WAN interfaces. The only cost of applying this recommendation would be about two hours of work to create, apply and test the new filters. This, together with the previous recommendation, would solve the problem described in the second (and last) negative finding.
- Keep the current setup of administrative access to the router: console only[4] and protected by password and timeout. There is no extra cost involved in following this recommendation.
- Keep the version of the firmware always up to date, as it currently is. Given that the product has been obsoleted by 3COM it is improbable that new versions are released, but nonetheless, it is important to keep an eye on it just in case 3COM decided to publish any updates. The cost is negligible: check the 3COM web site every so often (e.g. 2 minutes every week) and apply the new version if available (30 minutes).

[4] HTTP and TELNET access were confirmed to be disabled by the replies (RST) obtained on CK#01 and CK#8.

5 References

[3CO01] 3COM Corporation. *Home page of 3COM Corporation*. http://www.3com.com

[3CO02] 3COM Corporation. *OfficeConnect Remote 812 ADSL Router. CLI User's Guide*. http://support.3com.com/infodeli/tools/remote/ocradsl/812_cli.pdf

[3CO03] 3COM Corporation. *How to setup HTTP Filtering to prevent Denial-of-Service Attacks on the OfficeConnect Remote 812 Router.* http://support.3com.com/infodeli/tools/remote/ocradsl/http_filtering.pdf

[3CO04] 3COM Corporation. *Downloads for 3Com OfficeConnect Remote 812 ADSL Router.* http://www.3com.com/products/en_US/result.jsp?selected=all&sort=effdt&order=desc&sku=3CP4144

[CER01] CERT/CC. *Computer Emergency Response Team Coordination Center.* http://www.cert.org

[CER02] CERT/CC. *Home Network Security.* http://www.cert.org/tech_tips/home_networks.html

[CER03] CERT/CC. *Home Computer Security.* http://www.cert.org/homeusers/HomeComputerSecurity/

[CIS01] Center for Internet Security. *Gold Standard Benchmark for Cisco IOS.http://www.cisecurity.org/tools2/cisco/cisco-ios-router-benchmark.pdf*

[CVE01] CAN-2002-0888. *Vulnerability in 3COM OfficeConnect Remote 812 ADSL Router.* http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0888

[DIC01] Lexyco Publishing Group, LLC. *English Dictionary and Thesaurus Search Service.* http://www.dictionary.com

[GIA01] SANS GIAC web site. *GIAC home page*. http://www.giac.org

[GOO01] Google. *Google Internet Search Engine.*http://www.google.com

[GRA01] Graesser, Dana. *Cisco Router Hardening Step-by-Step.* http://www.sans.org/rr/papers/21/794.pdf

[NSA01] National Security Agency. *Router Security Configuration Guide.*

http://www.cisecurity.org/tools2/cisco/rscg.pdf

[PEL01] Peltier, Thomas R. *Information Security Risk Analysis.* CRC Press LLC, 2001

[SAN01] SANS Institute. *Sans Institute web site.* http://www.sans.org

[TCP01] Tcpdump.org. *Tcpdump*. http://www.tcpdump.org