Firewalls and Software Updates

License

This work by Z. Cliffe Schreuders at Leeds Metropolitan University is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.

Contents

General notes about the labs

Often the lab instructions are intentionally open ended, and you will have to figure some things out for yourselves. This module is designed to be challenging, as well as fun!

However, we aim to provide a well planned and fluent experience. If you notice any mistakes in the lab instructions or you feel some important information is missing, please feel free to add a comment to the document by highlighting the text and click the comment icon (▤), and we will try to address any issues. Note that your comments are public.

You should maintain a lab logbook / document, which should include your answers to the questions posed throughout the labs (in this colour).

Preparation

Start by loading the latest version of the LinuxZ template from the IMS system. If you have access to this lab sheet, you can read ahead while you wait for the image to load.

To load the image: press F12 during startup (on the boot screen) to access the IMS system, then login to IMS using your university password. Load the template image: LinuxZ (load the latest version).

Once your LinuxZ image has loaded, log in using the username and password allocated to you by your tutor.

Using the VM download script (as described in the previous lab), download and **start** this VM:

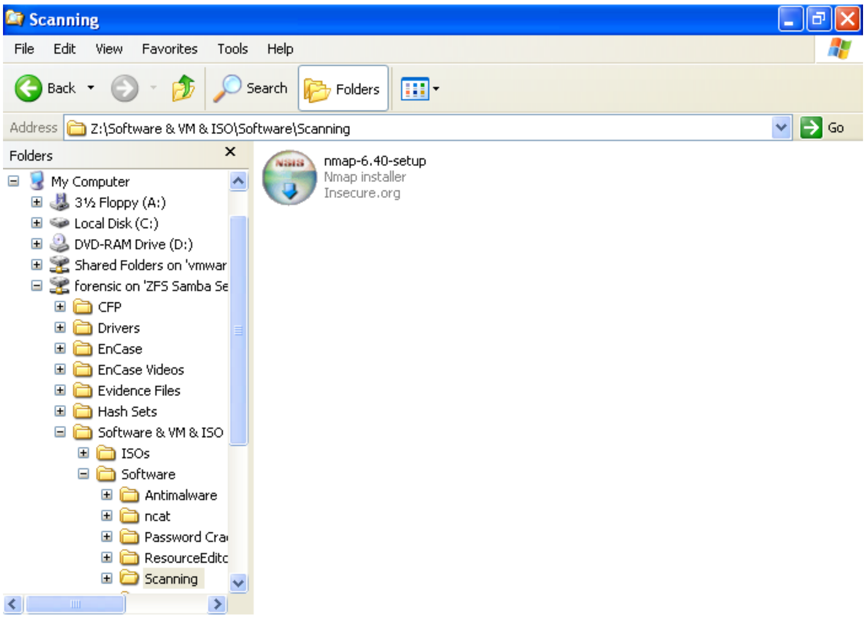
- WinXP Pro - bridged with network share

This lab could be completed on almost any Windows system with Nmap and Ncat installed. Nmap (with Ncat) is available at: http://nmap.org/download.html (you don't need to download the installer from the Internet if you are working in our labs). If you use a different version of Windows the steps will be slightly different, and will need some alteration.

Start by installing Nmap onto the Windows VM.

As illustrated below, the installer can be found on the network drive in "Z:\Software & VM & ISO\Software\Scanning".

Copy the installer to the local disk (for example, My Documents) and then run it.



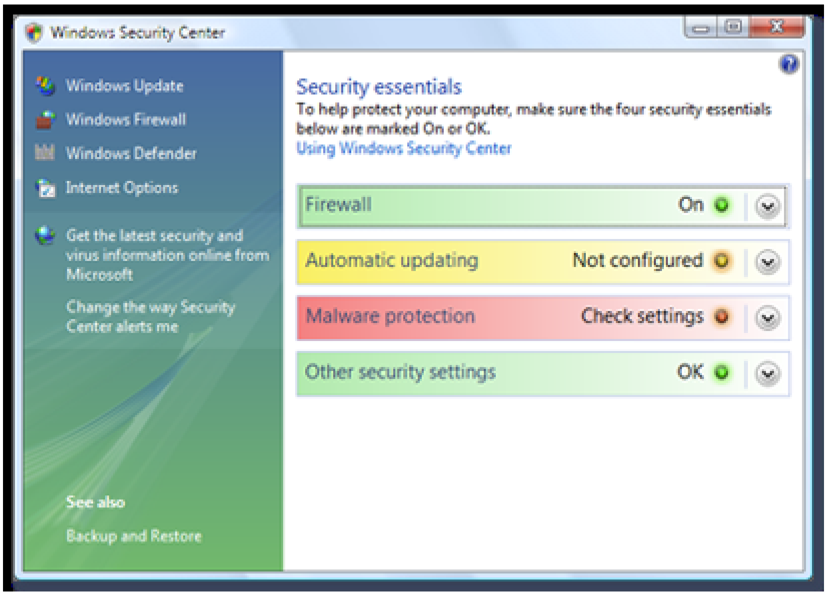
Installing Nmap

Introduction to security mechanisms

These lab exercises cover some fundamental security concepts: firewalls, software updates, and (following on from the the previous lab) malware protections.

Windows XP and Windows Vista have a dialog known as “Windows Security Center”, in Windows 7 and 8 these features are located in the “Action Center”. In either case, this dialog checks the status of security “essentials” on your computer (on newer versions on Windows, the Action Center also monitors other non-security related maintenance events, such as low disk space warnings).

Open Security Center or equivalent (it can be found via the control panel), and have a look at the settings that Microsoft have deemed as *essential* to security. Regardless of the operating system in use (including Apple or Linux-based operating systems), these can be considered desirable security features to have enabled.



Security essentials

To help protect your computer, make sure the four security essentials below are marked On or OK.

Using Windows Security Center

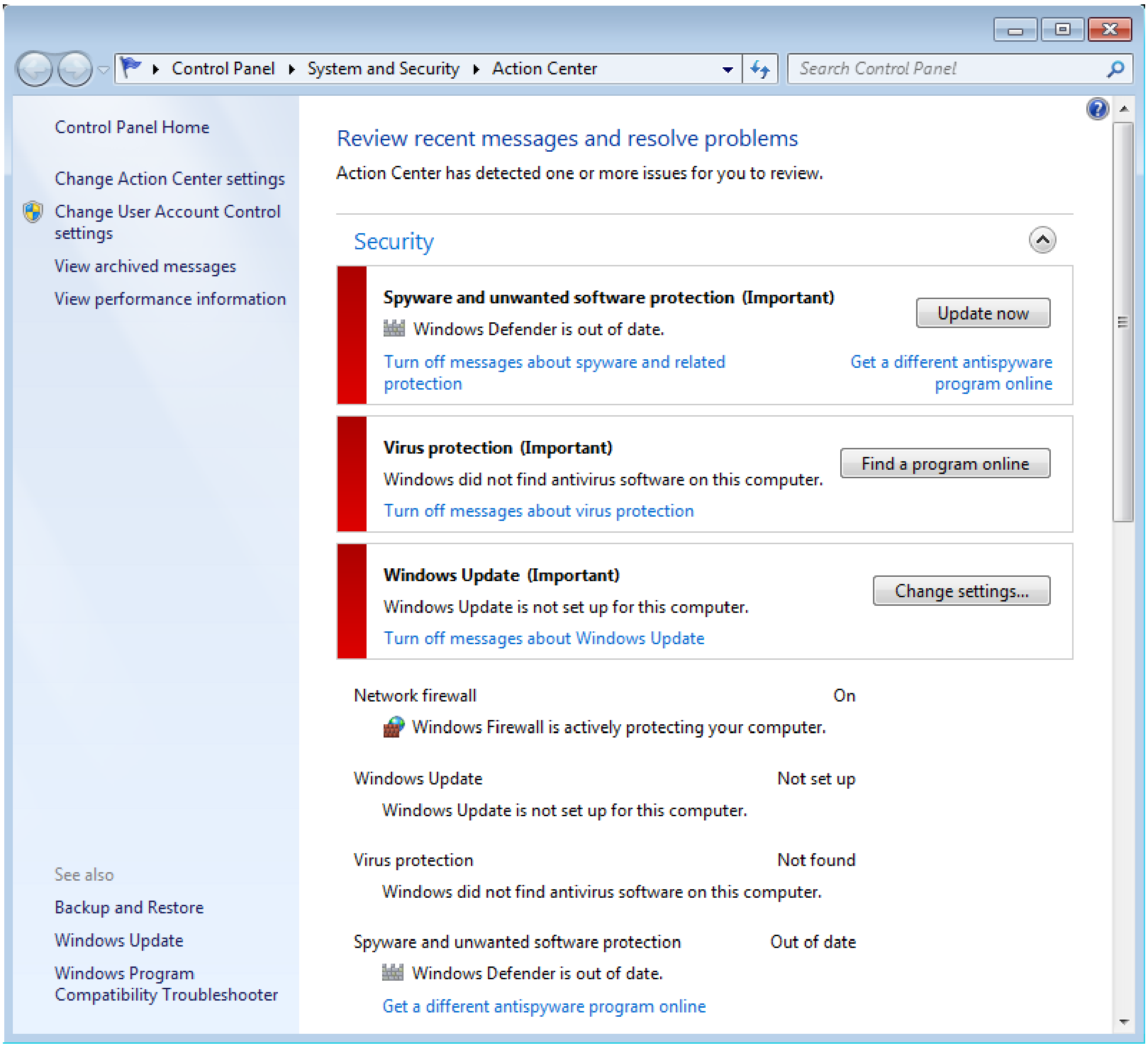
Firewall On

Automatic updating Not configured

Malware protection Check settings

Other security settings OK

Vista Security Center


Control Panel ▸ System and Security ▸ Action Center
Search Control Panel
Control Panel Home
Change Action Center settings
Change User Account Control settings
View archived messages
View performance information
See also
Backup and Restore
Windows Update
Windows Program Compatibility Troubleshooter
Update now
Find a program online
Change settings...

Review recent messages and resolve problems

Action Center has detected one or more issues for you to review.

Security

Spyware and unwanted software protection (Important)
Windows Defender is out of date.
Turn off messages about spyware and related protection
Get a different antispyware program online

Virus protection (Important)
Windows did not find antivirus software on this computer.
Turn off messages about virus protection

Windows Update (Important)
Windows Update is not set up for this computer.
Turn off messages about Windows Update

Network firewall — On
Windows Firewall is actively protecting your computer.

Windows Update — Not set up
Windows Update is not set up for this computer.

Virus protection — Not found
Windows did not find antivirus software on this computer.

Spyware and unwanted software protection — Out of date
Windows Defender is out of date.
Get a different antispyware program online

Windows 7 Action Center

Question: For each of the following “essentials”, are they enabled on your system, and what do they defend against? Hint: search the Web for some information about them. Each are discussed in subsequent sections. Take the time to understand the importance of each.

Firewall:

Automatic Updates:

Malware Protection (antimalware):

Question: Is the computer you are using “secure” as defined by this scheme? If not, what are likely risks?

Question: Regarding software updates, what version of Windows are you using? Is it running the latest service pack (major update)? Hint: My Computer, Help menu, About Windows.

Question: If all of the security settings were flagged as green (ok), would this make your system impervious to attack?

Why not? (Hint: look up the meaning of the term **zero-day**)

Firewall Basics

A host-based software firewall (one running locally on your computer) controls the ways that local programs on a computer can access the network. Rules define what kind of traffic is allowed to come in from the network (for example, from the Internet), and what is allowed out: traffic from your computer to a network.

Most modern network traffic is via the Internet Protocol (IP), using Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) to transfer data between computers. The primary difference between TCP and UDP is that one of the two establishes a connection and performs checks to ensure that traffic reaches its destination, while the other does not.

Question: Fill in the blanks:

___ establishes a connection and performs checks to ensure that traffic reaches its destination, ___ does not.

In either case, IP addresses are used to route traffic to the correct computer, and port numbers are used to determine which program on the computer gets the data.

Firewall rules typically define what traffic is allowed based on factors such as:

- direction of traffic
- who initiated the traffic stream
- the IP address source and destination
- and the port numbers at the source and destination

Firewalls provided by different vendors vary in their complexity and sophistication. The simplest form is known as a “packet filter”, it only looks at individual packets (each chunk of data as it arrives). “Stateful” firewalls also consider previous traffic so that, for example, new connections can be treated differently to traffic that is part of an established connection. “Deep packet inspection” firewalls can also consider the actual content of data streams, and can enforce that specific protocols are only on specific ports, which can prevent some malicious traffic from using otherwise allowed ports.

The aim of these techniques is to only allow legitimate network traffic in order to avoid malicious attempts to misuse the network, such as attempts to gain control of the computer. As such, firewalls can reduce the **attack surface** that is exposed to the wider Internet.

To illustrate the defence provided we turn to Nmap. Nmap is the *de facto* network scanning software, as used by network administrators, security professionals, and attackers. Nmap is free open source software (FOSS), and can conduct a wide range of network diagnostics, and host and service discovery. It can be used to determine what hosts are available on a network, and what services are running (that is, what ports are open and accepting connections).

Before we conduct the scan, lets use Ncat to listen on a port. Ncat is a modern version of Netcat, the “Swiss-army knife for TCP/IP”. Ncat can be used to read from and write the network via TCP or UDP.

Open a command prompt. (On your keyboard, hold the Windows button and press “R”, then type “cmd” and press Enter.) Note: you need to open the command prompt *after* Nmap has been installed.

Run the command:

```
ncat -h
```

The output describes how Ncat can be used, with various command line arguments.

Question: What do each of these arguments do?:

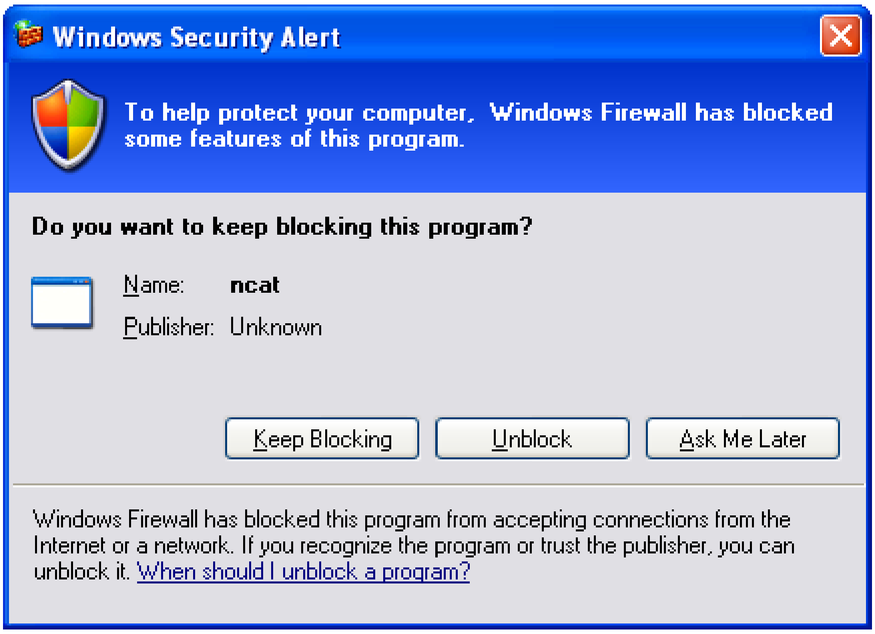
- `-l`
- `-p`
- `-k`

Instruct Ncat to listen on a port and print out any data it receives...

Run the command:

```
ncat -l -k -p 12345
```

Windows may prompt to inform you that the firewall is blocking the port. Click “Ask Me Later” to let it continue to block connections from the network.



Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: ncat

Publisher: Unknown

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Windows XP firewall prompt

Ncat should be waiting for network input. Leave the command prompt open and continue on.

Open another command prompt.

Nmap can be used to list all of the open ports on a system.

Run the command:

```
nmap -sT localhost
```

To save time, you can instruct Nmap to just check a range of ports near the port we are interested in (for example from TCP port 12340 to port 12350).

Run the command:

```
nmap -sT -p12340-12350 localhost
```

Paste the command and results into your log book.

> Hint: to take a screenshot, move the mouse out of the VM, and press the "Print Scrn" key. Click "Take a New Snapshot", and select the area of the screen you want to save. Double click your selected area, and click "Copy". You can now paste your screenshot into your lab book. Alternatively, if your lab book is within the VM (not recommended) rather than in LinuxZ, then you can from the command prompt by right clicking on the text, click Mark, highlight the text, and press enter.

The significance of this listing, is that it describes the ports that you can connect to on your own machine, *from your own computer* (since that is where you are running Nmap from). You should be able to see port 12345 listed as being **open**. It is described as the "**netbus**" port, because that is the program that typically uses that port. However, the program actually listening to the port is the Netcat program, which you started earlier. The firewall allows us to connect to that port, *even though you told Windows Firewall to continue to block the port*.

Now use Nmap to scan a classmate's computer for that port...

> Alternatively, you can scan your Windows VM from another of your own VMs or computers (if available, you could start another machine in the lab), or from the LinuxZ console prompt (as below, but use "nc" rather than "ncat").
>
> You need to know the IP address of the other computer. To find your own IP address use the command "ipconfig", tell someone else your IP address so that they can see which ports they could connect to on your machine.

Run the command:

```
nmap -sT -Pn -p12340-12350 their_IP_address
```

> Note that the -Pn is used to tell Nmap not to wait for a ping response, since the firewall may be blocking ping requests.

Paste the command and results into your log book.

The significance of this listing, is that it describes all the ports that you can connect to on someone else's machine. If the ports are listed as "open", it is possible to connect to these services to either do something legitimate, or perhaps to attempt to attack the machine. A port that is listed as “filtered” is not giving a response, possibly due to a firewall. A port that is listed as “closed” has not been filtered by a firewall, but does not have a program listening to the port.

Ncat can not only listen on a port (as we have done above, which should be still running), but it can also be used to connect to a remote port, and send and receive data. Connect to your classmate’s system (or if you are working alone, connect to your first Windows VM from another system). Run:

```
ncat their_IP_address 12345
```

Question: Can you connect to their system? Were any of the ports listed as open?

Now lets lower defences and see what access the firewall was denying.

Turn off Windows Firewall, on both computers. (Open “Windows Firewall” from within the Control Panel), set firewall to “off” and save your changes by clicking “Ok”.

Run the above command again, and record the results.

This time you should be able to see the port listed as “open”. Meaning you can connect to the port and communicate with the remote system.

Connect to the Ncat running on the remote machine. Run the command:

```
ncat their_IP_address 12345
```

Type some text and watch the output of Netcat on their computer. You should be able to type messages to each other. Send some messages to each other via ncat on port 12345.

Now figure out how to (and do) configure your firewall to allow the Ncat program to access the network even when your firewall is turned on.

> Hint: if you have told the firewall to keep asking, it may prompt each time Netcat is started. If the prompt does not display, you can alternatively configure the firewall via the Windows Firewall configuration program (via control panel).

Turn on the firewall, and ensure your classmate can still connect to Netcat from the other computer.

Test using Ncat to listen on an alternative port (for example, 12346). Does your previous exception allow this?

Question: Why may you wish to restrict an application to only using certain ports?

Edit your firewall rules to allow any programs to accept connections on TCP **port 12345 only** (and remove any exceptions for Ncat).

Confirm that you can still receive connections when Ncat listens on port 12345, but not when it listens on any other ports.

Question: What are the advantages and disadvantages of basing firewall rules on ports rather than programs?

Enable firewall logging for accepted and dropped connections (on WinXP, Windows Firewall, Advanced, Security Logging, Settings).

Make some connections using Nmap, and view the firewall logs.

Question: Why wouldn't you normally want to open TCP port 12345 to all programs? Hint: what is the port typically used for?

Configure the firewall to allow connections on port 80.

Save the below HTML (or an altered version) as `c:\webpage.html`. Hint: you may want to use Notepad.

```
<html>

<head><title>Hello!</title></head>

<body>Hello there!</body>

</html>
```

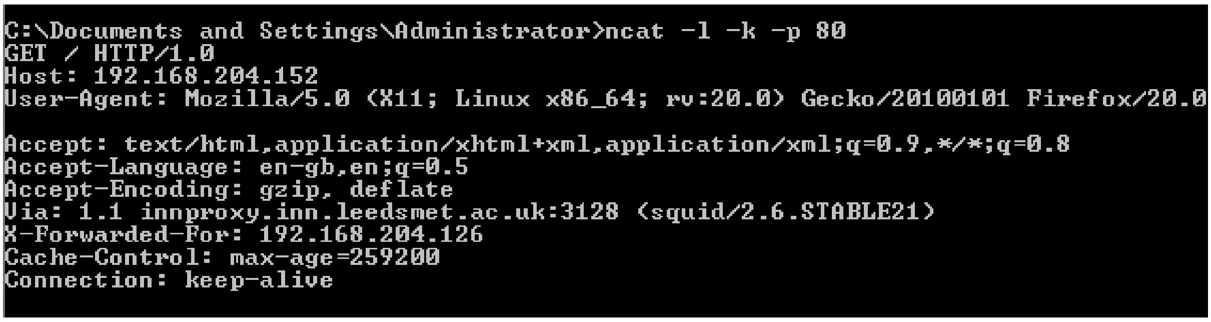
Run the Ncat listener as follows:

```
ncat -l -k -p 80 -c "type c:\webpage.html"
```

From a remote system, open a Web browser (for example Firefox, Chrome, or Internet Explorer), and enter the IP address of your Windows XP VM.

> Tip: if you get an error message from the proxy "The Requested URL could not be retrieved", then you need to configure your Web browser not to use the proxy for local IP addresses. If you are working in the Leeds Met IMS labs, in Firefox, "Edit" (menu), "Preferences" (menu), "Advanced"

(tab), “Network Settings” (Tab), “No Proxy For” (Textbox), and append “**,192.168.0.0/16**”.



```
C:\Documents and Settings\Administrator>ncat -l -k -p 80
GET / HTTP/1.0
Host: 192.168.204.152
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:20.0) Gecko/20100101 Firefox/20.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip, deflate
Via: 1.1 innproxy.inn.leedsmet.ac.uk:3128 (squid/2.6.STABLE21)
X-Forwarded-For: 192.168.204.126
Cache-Control: max-age=259200
Connection: keep-alive
```

Listening on port 80, talking to a Web browser (not displayed when using “-c type ...”)

When the Web browser connects it will send a request for a Web page (as shown above), Ncat will respond with the contents of the text file (the HTML code).

This is essentially how HTTP works, a Web server listens on port 80, Web browsers connect and request Web resources, then the Web server sends out HTML code representing a Web site (although this usually also includes headers in the response).

Modify the above command, to tell Ncat to only accept connections from one specific IP address (hint “*--allow IP*”). Test your command.

Modify your firewall rules to achieve the same effect. Test your new rules.

Question: If you were managing a corporate network, why wouldn’t you want PCs on the network from listening to connections on port 80?

Allowing any local program to communicate with the network has some security risk.

For example, using Ncat it is possible to spawn a command shell and feed this through to any connections.

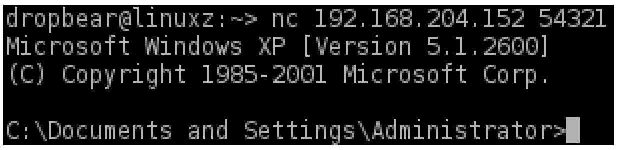
Run:

```
ncat -l -k -p 54321 -e cmd
```

Connect from a remote system to this port:

```
ncat your_IP_address 54321
```

You will be prompted with a command line access to the system!



```
dropbear@linuxz:~> nc 192.168.204.152 54321
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>
```

Try running:

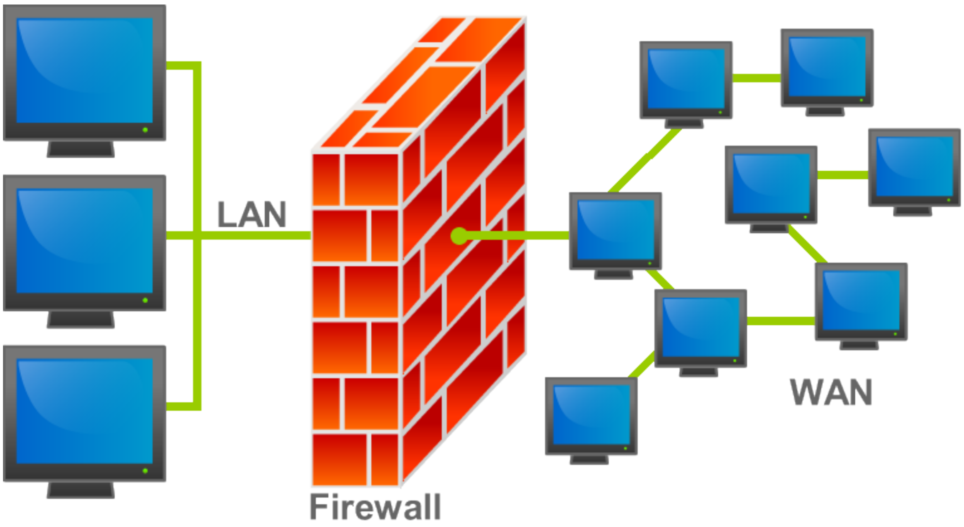
```
dir
```

Attempt to use your command line access to list the remote system's files in their "C:\" directory.

Ncat with "-e" or "-c" could be deployed by an attacker as a backdoor into a system! After the program has been started on the victim's system, anyone that can connect to the program can then issue commands to the system and do whatever they like to the system. Note this is related to the concept of malware: software (such as Ncat) may be acting maliciously, and if we have trusted it with access to files and the network there is the risk that the software will misbehave.

Even if you do deny an application to listen to ports and accept connections, the application can typically connect out to another system, which would circumvent firewall rules that focus on incoming connections.

Windows XP has a simple firewall, that is not very feature rich, but as illustrated it does provide some level of protection. Newer versions of Windows, and other operating systems such as Linux, have more robust firewalls. As illustrated in the figure below, in addition to host-based software firewalls, firewalls are also placed between networks to control network traffic that is allowed to specific hosts or networks.



Firewall in a network (image: GNU Free Documentation License, http://commons.wikimedia.org/wiki/File:Firewall.png)

Question: Which of the following does the Windows Firewall do to protect users?

- Block malware from reaching your computer? (If yes, to what degree?)
- Detect malware on your computer?
- Block spam/phishing emails?
- Stop you from making bad decisions which allow dangerous network traffic?
- Block all outgoing connections unless otherwise configured by the user?
- Block all incoming connections unless otherwise configured by the user?
- Block certain programs or ports from accepting incoming connections from the network?

Keeping Software Up-to-date

A **software vulnerability** is a weakness in the security of a program, often due to a design decision mistake, or an implementation mistake. Even if the authors of software are trying to do the right thing, it is easy for a small mistake to result in attackers being able to take control of the software. Therefore, as a result of some coding mistakes, attackers often are able to assume the identity of vulnerable software running on someone else's computer. An **exploit** is an action (or piece of software that takes an action) that takes advantage of a vulnerability.

The importance of keeping software up-to-date is perhaps best illustrated by exploring the rate that security bugs are discovered in software.

Goto http://www.securityfocus.com/bid and select vendor:Microsoft, title:Windows XP

Question: How many security vulnerabilities in Windows XP have been discovered recently?

Question: Look at a few of them in more detail. Has there been an update issued to fix those problems?

Question: Do you think your VM is up-to-date enough to be protected from these security flaws?

The **window of vulnerability** is the time between when the vulnerability exists in software until an end user's computer is protected.

Question: If you always apply software updates as soon as they are available, will you always be protected from attacks?

Why not?

Antimalware

If you have not already do so when completing the previous lab, install a free antivirus product, such as Microsoft Security Essentials, Comodo Antivirus, or AVG Free.

Comodo Antivirus is available on the network drive, in:

“Z:\Software & VM & ISO\Software\Antimalware\”

Try running the NetBus server from the network share (as described in the previous lab sheet). The malware protection software should detect and remove the Trojan horse.

Conclusion

You are now familiar with essential security mechanisms available for PCs: firewalls (to restrict unnecessary network traffic), software updates (to patch potentially vulnerable software), and antimalware (to protect against common viruses, worms, and Trojan horses). This foundational knowledge will help you to understand how to maintain the basic security for a computer. However, it should be noted that a skilled attacker can often circumvent these controls by out-thinking the people that configure them and those that provide updates to these mechanisms. For example, by finding a new way (AKA, a **zero-day**) to attack a system.