APPLIED INFORMATION SECURITY LABS

Second Edition

Solutions

Dr. Randall Boyle

Jeffrey G. Proudfoot

CONTENTS

CHAPTER 1: DOS COMMANDS

1.1 DOS BASICS

1. **Can you use the DIR command to show only executables? How?**

   Answer: You can use **dir /ad** to show only directories. You can use the command **dir *.exe** to see only executables.

2. **What happens if you start typing part of an existing file name and then press the Tab key?**

   Answer: It will complete the rest of the file name.

3. **Can you start programs from the command prompt? How?**

   Answer: Yes, you can start programs from the command prompt by typing in the name of the program. For example, you can type **explorer** to start a new Windows Explorer window.

4. **What happens if you drag-and-drop a file from Windows Explorer onto the DOS window?**

   Answer: It displays the complete path to that file.

1.2 IPCONFIG

1. **What is the practical difference between an IP address and a physical (MAC) address?**

   Answer: IP addresses help route packets as they move between networks. MAC addresses are used to pass packets across a single network. IP addresses on a packet won't change in transit, but a packet can have multiple frames with different MAC addresses. A host's MAC address won't change, but a host can switch IP addresses many times throughout a single day.

2. **What is the Default Gateway?**

   Answer: It's the computer that stands between you and the Internet.

3. **What do DNS servers do?**

   Answer: DNS servers will change domain names like www.Google.com into IP addresses.

4. **What is a subnet mask?**

   Answer: It tells you the size of your network and the number of hosts on your network.

1.3 PING

1. **Can you adjust the number of packets that are sent? How?**

   Answer: Yes, you use the –n option followed by the number of requests you'd like to send.

2. **What did the -t, -n, and –l options do?**

   Answer: The -t option pinged the host until stopped. The -n option set the number of echo requests. The -l option adjusted the buffer size that was sent.

3. **Why would you experience packet loss?**

   Answer: There are many different reasons a packet could get lost: electromagnetic interference, power failure, faulty NICs, incorrectly configured networking equipment, solar flares, etc.

4. **Why would you want to send larger packets?**

   Answer: Sending larger packets would give you an idea of how packet size affects bandwidth, response times, fragmentation, etc.

1.4 TRACERT

1. **Why would you use the -d option?**

   Answer: It would not resolve addresses to host names.

2. **If you had several nodes "time out," how would the -w option help?**

   Answer: The -w option could be used to increase/decrease the time out option. This would tell you if the nodes were just slow or if they had completely failed.

3. **Why would a network administrator only want to see part of the route?**

   Answer: Being able to see specific network segments along an entire path would help a network administrator troubleshoot latency issues by identifying the problem segment along the path.

4. **How would the pathping results change if you didn't use -q 5 in the command?**

   Answer: If you hadn't used the -q 5 option, you would have sent many more queries (around 100).

1.5 NETSTAT

1. **How can netstat help you track the information coming in and out of your computer?**

   Answer: It can tell you which hosts are connected to your machine and which ports they are using.

2. **How can netstat help you diagnose network problems?**

   Answer: It can give you network statistics and the status of each NIC.

3. **How would the routing table (`netstat -r`) be useful?**

Answer: It will tell you how packets are going to be routed depending on the destination IP address. It will also tell you which IP address is assigned to a given NIC.

4. **Why would someone need different statistics for IP, IPv6, ICMP, TCP, UDP, etc.?**

   Answer: Each protocol can be used for a different purpose. A network administrator might want to know what types of traffic are flowing over his/her network. Knowing the types and quantities of each protocol may help solve a variety of network issues, including faulty equipment, rogue machines, unapproved servers, compromised servers, etc.

1.6 NSLOOKUP

1. **Why are there multiple IP addresses associated with a single domain name (e.g., www.CNN.com and www.Google.com)?**

   Answer: This is done as a first step in load balancing requests sent to Google. Further load balancing is done at one of the Google clusters associated with that IP address.

2. **Why did Nslookup query fiber1.utah.edu instead of querying www.CNN.com directly?**

   Answer: Nslookup is designed to query the DNS server listed on the local host, not the remote Web server. It would need to query the DNS server to resolve the domain name (www.CNN.com) before it could even contact the CNN server.

3. **Why does www.Google.com use an alias?**

   Answer: Google may use an alias if they are virtualizing their web servers, or if they want to make it easier to make maintenance changes at a later date.

4. **How do domain names and IP addresses get registered?**

   Answer: ICANN manages the official assignment of domain names to IP addresses. You can get your domain name registered through a variety of companies (like GoDaddy.com) that will handle the registration process for you.

1.7 FTP

1. **What would have happened if you had run the `mget *` command in interactive mode (i.e., without entering "prompt" first)?**

   Answer: It would not have transferred the files.

2. **Is transferring files with FTP faster than using HTTP?**

   Answer: No, with daily usage, you won't notice any practical differences. There might be slight differences for one small file (i.e., FTP being faster) compared to multiple large files (i.e., HTTP being faster).

3. **What effect did the `binary` command have on the file transfer? Was it necessary?**

Answer: The binary mode (or image mode) causes the sender to transfer all of the characters. Some FTP clients use ASCII mode in certain situations and would only transfer printable characters. This could render images, compressed files, and/or applications unreadable. It is recommended that binary mode is used for all transfers.

4. **Why did you use the `lcd` command?**

   Answer: The lcd command sets the local working directory for the FTP client.

1.8 POWERSHELL

1. **Could you use the Invoke-Command to start a process on a remote computer?**

   Answer: Yes, the Invoke-Command can start/stop a process on a remote computer. This is useful for a network administrator who manages a large number of machines.

2. **In what instances would you use the Measure-Object cmdlet?**

   Answer: The Measure-Object cmdlet will give you basic statistics (e.g., count, average, sum, minimum, and maximum) for any object.

3. **Which cmdlet would you use to stop a service?**

   Answer: You would use the Stop-Service cmdlet.

4. **Pwd is an alias for which cmdlet?**

   Answer: Pwd stands for print working directory. It is an alias for Get-Location.

1.9 HASHING

1. **What does the `-v` option do? (Hint: `fciv /?`)**

   Answer: It verifies the hashes.

2. **Can you store the hashes in a database? How?**

   Answer: Yes, hashes can be stored in a database. They can be written directly to a database. Most modern database management systems include hashing functions.

3. **Which is better, MD5 or SHA1? Why?**

   Answer: SHA1 is better because it is longer.

4. **Are longer hashes better? Why?**

   Answer: Yes, because they reduce the chance of a collision.

1.10 SDELETE

1. **Which option would clean the free space?**

   Answer: The -c option would clean the free space.

2. **Which option would zero the free space?**

   Answer: The –z option would zero the free space.

3. **How does secure deletion differ from normal deletion?**

   Answer: Normal, or nominal, deletion leaves a potentially recoverable file on the storage media or hard disk. Secure deletion makes a file unrecoverable.

4. **What is "free space"?**

   Answer: Free space is a section(s) of storage media that is (are) allocated such that files can be written to those areas.

CHAPTER 2: WINDOWS SECURITY

2.1 LOCAL SECURITY POLICY

1. **How might enforcing a password history make you safer?**

   Answer: Enforcing a password history might make you safer because it would keep you from using the same password for a very long time. If one of your passwords were to be stolen, your accounts would only be vulnerable for a limited amount of time.

2. **How might enforcing a minimum password length make you safer?**

   Answer: A minimum password policy might make you safer by preventing you from using short passwords that are easily cracked.

3. **How might enforcing password complexity requirements make you safer?**

   Answer: Password complexity requirements might make you safer because they would force you to create a password that is more difficult to crack.

4. **How might enforcing an account lockout policy make you safer?**

   Answer: Enforcing an account lockout policy might make you safer because it would prevent an attacker from continuously trying to gain access to your account. It would also give you a warning signal that your account may be a target of an attack.

2.2 WINDOWS FIREWALL

1. **Could you still access some websites with your port 80 rule enabled? Why?**

   Answer: Yes, you could access a website if it was running on a port other than 80 (e.g., 8080). You would have to specify the alternate port in order to get to the website, but it is possible.

2. **Why would you want to allow incoming (not outgoing) port 443, but block incoming port 80?**

   Answer: You may want to only allow encrypted connections coming into your network.

3. **How could blocking all ICMP traffic protect you?**

   Answer: It may keep attackers from mapping your internal network.

4. **How could blocking all ICMP traffic hurt you?**

   Answer: Blocking ICMP may prevent certain applications from working correctly. It may make troubleshooting and network administration much more difficult.

2.3 CONFIGURING BACKUP

1. **How much data would you lose if your hard drive failed right now?**

   Answer: This will be different for each person. In general, most student will lose anywhere from a week to all of their data.

2. **How long would it take to restore your data?**

   Answer: This will be different for each person. For most students it will take anywhere from a few hours to a few days.

3. **How long has it been since you have backed up your data?**

   Answer: This will be different for each person. Some students have weekly backups enabled but most do not. Some students back up at the end of each semester.

4. **Would a cloud-based backup solution be wise? Why or why not?**

   Answer: A cloud-backed backup solution might be a good idea because you wouldn't lose any data if there were a local natural disaster or fire. It might also be more convenient than creating backup storage. However, all online backups must be encrypted. Your privacy is not guaranteed when you use online backup.

2.4 WINDOWS UPDATE

1. **How can updates make your computer more secure?**

   Answer: Updates fix vulnerabilities in your software and operating system.

2. **Could updates cause problems? Why?**

Answer: Yes, updates may inadvertently cause existing applications to fail. An update may fix a potential vulnerability and change the way the application or operating system functions. These changes in functionality may cause applications to fail, especially custom applications.

3. **Should all updates be applied? Why or why not?**

   Answer: For most home users, yes. For corporations, no. Corporations must test all updates on replicated testing servers before they are applied to production servers. Applying updates to production servers can cause outages and data loss.

4. **How do large organizations control updates for hundreds, or thousands, of computers?**

   Answer: It is possible to control the roll out of updates to thousands of computers via a domain level updating service. For example, Microsoft uses Windows Server Update Services to control how updates are applied to domain resources.

2.5 USER MANAGEMENT

1. **How could parental controls protect users (children)?**

   Answer: It could keep users (children) from accessing inappropriate content.

2. **How might time controls protect users (children)?**

   Answer: Time controls can protect children by only allowing them access to a computer while a parent is available to monitor their activity.

3. **How might application controls protect users (children)?**

   Answer: Application controls might protect children by preventing them from using an application that might be harmful. For example, a parent may block an online music sharing application. This would prevent a child from illegally downloading pirated music. It would also prevent others from downloading music from the child's computer, which is also illegal.

4. **How might a user circumvent parental controls?**

   Answer: A user could boot the computer from a USB or DVD that contains a live Linux distribution. The local operating system would not even be accessed, yet the user could have full control of the machine.

2.6 MICROSOFT SECURTIY ESSENTIALS

1. **Why is malware produced?**

   Answer: Motivations vary from economic (to get money), social (to gain respect), curiosity (to see if it can be done), etc.

2. **Should you run multiple antivirus scanners? Why or why not?**

Answer: Not really. One good antivirus scanner is sufficient. Multiple antivirus scanners just consume more CPU cycles without offering significant additional coverage.

3. **Can malware scanners misidentify software as harmful? Why or why not?**

   Answer: Yes, malware (or antivirus) scanners can misidentify software as harmful. Several of the pieces of software in this book may show up as harmful in your antivirus scanner. This happens in some, but not all, scanners. Scanners just look for the patterns identified by the antivirus publisher.

4. **How does Microsoft Security Essentials ensure you are protected against the most current threats?**

   Answer: Yes, Microsoft makes additions to their virus signature files of the most current and prevalent malware threats. Updates are automatically sent out.