

The Guide to Monitoring and Controlling a Network
Daniel Owens
Security Analyst with DanielSecurities

At A Glance

AT A GLANCE	II
CONTENTS	III
NETWORKING AND THE INTERNET	V
<i>Hubs/Repeaters</i>	v
<i>Switches/Bridges</i>	v
<i>Routers</i>	v
SECURITY	VI
<i>What Is It?</i>	vi
<i>Becoming More Secure</i>	vi
THE GREAT HAT CONCEPT	VI
MONITORING A NETWORK	2
SOME LEGITIMATE PURPOSES:	2
UNSECURED NETWORKS:	2
<i>Procedures:</i>	2
<i>Hubbed/Switched Networks:</i>	4
Limitations:	4
<i>Routed Networks Without Taking Over the Router:</i>	4
Limitations:	4
Overcoming the Limitations:	4
SECURED NETWORKS:	5
<i>Procedures:</i>	5
Limitations:	6
TAKING OVER A SYSTEM OR NETWORK	6
SOME LEGITIMATE PURPOSES:	6
TECHNIQUES:	7
<i>ARP Cache Poisoning:</i>	7
Procedures:	7
Limitations:	9
<i>Routing Information Protocol (RIP) Spoofing:</i>	9
<i>DHCP/DNS Spoofing:</i>	9
<i>Exploiting Vulnerabilities:</i>	10
<i>Denial of Service (DoS):</i>	10
<i>Password Cracking:</i>	12
<i>Bypassing Passwords:</i>	13
BIBLIOGRAPHY	15
APPENDIX A: LINKS TO SOFTWARE USED	16
APPENDIX B: GLOSSARY OF TERMS AND ACRONYMS	17
LIST OF FIGURES	19
INDEX	20
FURTHER READING	21

Contents

AT A GLANCE	II
CONTENTS	III
NETWORKING AND THE INTERNET	v
<i>Hubs/Repeaters</i>	v
<i>Switches/Bridges</i>	v
<i>Routers</i>	v
SECURITY	VI
<i>What Is It?</i>	vi
<i>Becoming More Secure</i>	vi
THE GREAT HAT CONCEPT	VI
MONITORING A NETWORK	2
SOME LEGITIMATE PURPOSES:	2
UNSECURED NETWORKS:	2
<i>Procedures:</i>	2
<i>Hubbed/Switched Networks:</i>	4
Limitations:	4
<i>Routed Networks Without Taking Over the Router:</i>	4
Limitations:	4
Overcoming the Limitations:	4
SECURED NETWORKS:	5
<i>Procedures:</i>	5
Limitations:	6
TAKING OVER A SYSTEM OR NETWORK	6
SOME LEGITIMATE PURPOSES:	6
TECHNIQUES:	7
<i>ARP Cache Poisoning:</i>	7
Procedures:	7
Limitations:	9
<i>Routing Information Protocol (RIP) Spoofing:</i>	9
<i>DHCP/DNS Spoofing:</i>	9
<i>Exploiting Vulnerabilities:</i>	10
<i>Denial of Service (DoS):</i>	10
Big Pipe-Little Pipe Denial of Service:	11
Distributed Denial of Service (DDoS):	11
Ping of Death and SYN Floods:	11
<i>Password Cracking:</i>	12
Against a Web Interface:	12
Against an LM and NTLM Network:	12
Procedures:	12
Against a Windows Account:	13
<i>Bypassing Passwords:</i>	13
Windows 9x:	13
*NIX:	13
UNIX, Linux, and Mac OS X:	14
BIBLIOGRAPHY	15
APPENDIX A: LINKS TO SOFTWARE USED	16
APPENDIX B: GLOSSARY OF TERMS AND ACRONYMS	17
LIST OF FIGURES	19
INDEX	20

FURTHER READING.....21

Introduction

Networking and the Internet

Hubs/Repeaters

Hubs and repeaters are networking devices that operate on the OSI Level 1, which is the lowest level in the OSI model (Network cards also operate at this level) (*OSI Reference Model* pp 425-432). These devices are unintelligent and merely serve to retransmit traffic indiscriminately to any attached device or to amplify the traffic's signal and clarity. There is no security built into such devices and they are not efficient if there is a significant amount of traffic or attached devices thanks to their nature. The easiest way to know if the device in question is a hub/repeater is to see if all traffic sent or received by a single device attached to the networking device is sent to and received by all other devices attached to the networking device. In addition, if the networking device has a light that is marked "Collision", or anything to that effect, it is a Level 1 device. Monitoring traffic on such devices is trivial as all systems receive all of the traffic; moreover, there is no way or point to take over a hubbed network given that traffic seen by all systems, so if you are attached to such a device, you need not read beyond the "Monitoring a Network" chapter.

Switches/Bridges

Switched and bridges are networking devices that operate on the OSI Level 2, which is the second level in the OSI model (*OSI Reference Model* pp 425-432). These devices may or may not be very intelligent and often have some security, but not much. Instead of broadcasting traffic to all ports on the network, it selects the port that has the system to which the traffic is addressed and shows only that system the traffic. Switches and bridges are easily monitored using ARP cache poisoning; a technique described in the chapter called "Taking Over a System or Network". The products that you are able to purchase at a place such as Best Buy are more than likely either a hub or switch, even if they claim to be routers. The easiest way to know is to attempt to use ARP cache poisoning to take over the network; if you can do this, you are most likely on a switch or a bridge.

Routers

Routers are networking devices that operate on the OSI Level 3, which is the highest level in the OSI model at which networking devices operate (*OSI Reference Model* pp 425-432). These devices are intelligent and often tremendous control and security to the owner. They are very expensive, fast, and can handle inter-network traffic, unlike the devices at Level 1 and Level 2. Routers will likely require spoofing of a routing protocol such as RIP, which is described in the chapter called "Taking Over a System or Network". As a warning, routers can handle vast amounts of traffic, more than any of the networks that attach into them. Monitoring all of the traffic that the router sees can overload the monitoring system.

Security

What Is It?

Security is something that is always reached for, but can never be attained. Networks and systems will always have one weak point and it is merely a matter of time, energy, and patience as to whether or not a system will be breached. The most that can be attained is increasing the time and energy required to compromise a system or network, however, it is important that anyone on a network attempt to do this; most “hackers” are children and teenagers who know little or nothing and merely used something that they read off the internet or an application that they found. If you harden your system, most “hackers” will not be able to break into it as they will not have the skill level, knowledge, or abilities required. Perhaps by reading this manual, you will better understand the dynamics involved in monitoring and taking over a system. Hopefully, you will be able to understand that the internet is insecure, be able to make certain that people are not looking at inappropriate material on the internet, and be able to better control your home or business network from the inside.

Becoming More Secure

Knowledge about the internet and networks is the key to increasing security. By reading this guide, you will be able to monitor your network, look at what others on your network are doing (or not doing), and see malicious or suspicious traffic. If everyone in the world were to harden their systems, the internet would be a far friendlier place with fewer thefts of both information and identities. Locked-down systems would prevent children from become prey for a sexual predator, parents and spouses could monitor of porn, and worms would be ineffective. It is our duty as internet users to try to make the internet a safer, happier place. Are you doing your part?

The Great Hat Concept

There exist three types of people, as far as security is concerned: those who are malicious, those who are neither malicious nor good, and those who are good. Often times those in Systems’ Security refer to each group as the color of a hat: black hats are malicious, grey or red hats are neither malicious nor good, and white hats are good. This concept may seem familiar to anyone who has read fictional works with wizards given that the concept is barrowed from such works. This manual is intended for white and red hats only, as it purposely avoids giving information that could be used to damage a network or steal information from other networks. The techniques described herein are not stealthy and this was done on purpose, as it is assumed that the reader owns the network to be monitored or taken over so stealth is not required. If the reader intends or wishes to read a black hat oriented manual, this is not the manual desired.

Monitoring a Network

Some Legitimate Purposes:

System Administrators and Network Administrators who are ensuring that the network is working efficiently, flawlessly, and that the network is not under any sort of attack by someone malicious or a worm most often monitor networks. Networks that are monitored in such a manner are legal only because of company policy and a piece of paper that employees sign. It is important to note that if the policy is not explained to the employees or the employees do not sign an agreement to be monitored, the company cannot legally monitor the employees and the internet usage by the employees.

More general reasons for monitoring a network in a legal and legitimate way is to monitor your personal network or to have a firewall, Intrusion Detection System (IDS), or Network Intrusion Detection System (NIDS) monitor the network.



WARNING: It is illegal to take over a network or system that you do not own without the owner's permission!

Unsecured Networks:

Procedures:

Uses—Ethereal

1. Open Ethereal
2. You will likely want to set your default preferences, if not skip to step 3
 - a. Click “Edit” from the menu
 - b. Click on “Preferences”, which is at the bottom of “Edit”
 - c. Click on “Capture” and set the default networking interface to be the interface through which you are connected to the network that you wish to monitor
 - d. Make certain that “Capture

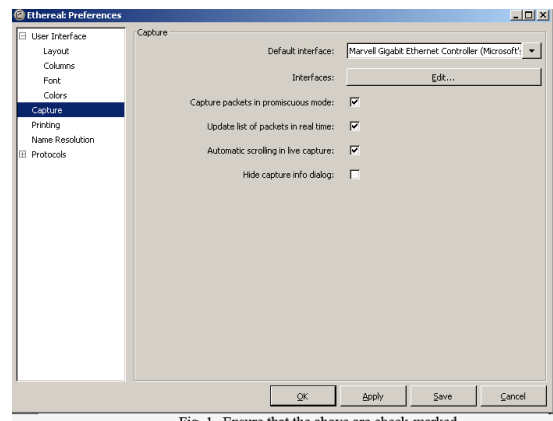


Fig. 1--Ensure that the above are check-marked

Figure 1--Ensure that the above are check-marked

packets in promiscuous mode”, “Update list of packets in real time”, and “Automatic scrolling in live capture” are checked (Fig. 1)

- e. Click the “Save” button
 - f. Click the “Apply” button
 - g. Click the “OK” button
3. To begin capturing, click “Capture” from the menu and select “Options”
 4. If you wish to apply a Capture Filter, to enable you to capture only specific packets, follow the example below, otherwise continue to step 5

- a. Click the “Capture Filter” button
- b. Select “HTTP TCP port (80)”; this filter shows only traffic using TCP port 80, which is the usual port for websites (Fig. 2)
- c. Click the “OK” button
- d. Now Ethereal will only capture traffic that uses TCP port 80, which is beneficial if that is the only traffic that you want to see anyway as you will save space by not capturing other traffic

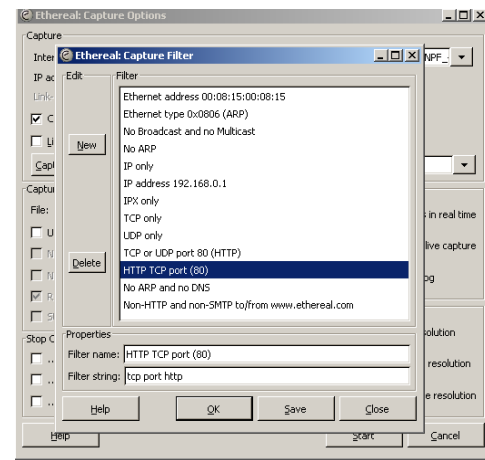


Fig. 2--Select HTTP TCP port (80)

Figure 2--Select HTTP TCP port (80)

5. If you want to have Ethereal automatically stop capturing packets, you can set conditions by using the appropriate “Stop Capture after” options
6. To begin capturing packets, press the “Start” button
7. As Ethereal captures packets, some brief information is displayed on the main interface. This information allows you to get an idea of what the packet contains by telling you the protocol used and the general contents of the packet
8. Ethereal will let you see the information contained in the packet if you select the packet and look at the raw information displayed near the bottom of the program, or if you double click on the packet
9. More often than not, the information displayed must be looked at over the span of multiple packets to make sense. To do this, we add a Filter to Ethereal (you can do this after the capture session is over, before you start capturing, or while you are

capturing). The easiest way to add a filter is to right click on a packet and select “Follow TCP Stream”, so that we see no other packets than the ones that we are interested in viewing

10. To take off a Filter, merely hit the “Clear” button next to the Filter and then click “Apply”

Hubbed/Switched Networks:

Limitations:

On a hubbed or switched network, there is no limit to the amount of information or what information can be gathered using the method described above. Anything that traverses these sorts of networks can be seen by any system on the network with relative ease. This is important because it means that such networks can be silently monitored (it is hard to detect monitoring on these networks).

Routed Networks Without Taking Over the Router:

Limitations:

When monitoring traffic on a network that has a router using the method described above, you will find that the only traffic visible to you, if you are on the inside of the router, is the traffic on your subdomain. If you are on Port X of the router, you cannot see the traffic of Port Y, only the traffic that is also on Port X. This is because you are not technically a part of Port Y’s network, unlike when you are on a hubbed or switched network. The only traffic that is visible to you, without taking over the router, is the traffic of your network, subdomain, and port.

Overcoming the Limitations:

There are a couple of different ways to overcome the limitations posed by being on a routed network, but they all lead back to having to takeover the router or moving to the outside of the router. By moving to the outside of the router to capture traffic, however, you will miss inter-network traffic and only get traffic destined for the outside or coming from the outside into the inside. In other words, you move to the outer

parameter, you can only see traffic destined for or coming from the outer parameter and you miss anything that stays in the inner parameter. This is obviously not what you want unless you merely want to see outer parameter traffic, so in most cases the best choice is to take control of the router using ARP cache poisoning or similar techniques described in the chapter titled “Taking Over a System or Network”.

Secured Networks:

Procedures:

Uses—Cain & Abel

1. Open Cain & Abel
2. Click “Configure” in the menu
3. Ensure that the proper network is selected (normally the IP address will be something to the effect of 192.168.0.x or 192.168.1.x, where x is any number from 1 to 254) (Fig. 3)
4. Click the “OK” button
5. Press the Start/Stop Sniffer button (Fig. 4)
6. Cain & Abel will monitor the network and attempt to capture passwords and secured communications of different types, including any password sent via HTTP (a web browser). To view these passwords, click on the “Sniffer” tab and then on the “Passwords” tab
7. If there is any password that needs to be decrypted, merely right-click on the entry in the “Passwords” tab and Select “Send to Cracker”

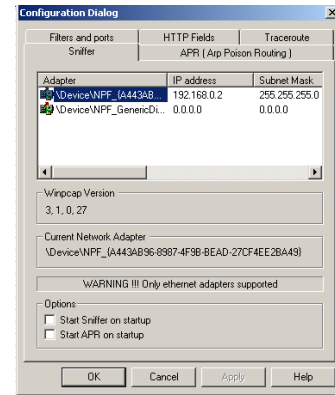


Fig. 3--Select the Adapter with an IP address

Figure 3--Select the proper adapter

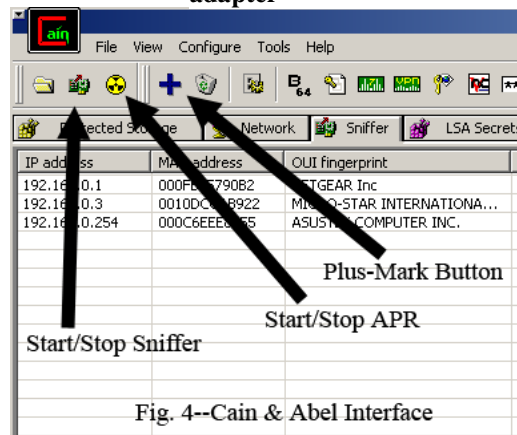


Fig. 4--Cain & Abel Interface

Figure 4--Toolbar Layout

8. Now click on the “Cracker” tab and right-click on the entry that has migrated to the Cracker section of the application and choose either “Brute-Force Attack” or “Dictionary Attack”, selecting the appropriate settings

Limitations:

Cain & Abel is very good at intercepting and decoding/decrypting passwords, FTP sessions, and other such communications, but it does not show you the traffic involved. The plus side to this is that you do not have to filter through the results, but it also means that if someone is viewing pornography and does not log onto the website, you would not know. To overcome this, you can use both Cain & Abel and Ethereal at the same time, which is something that will be advised later in order to take care of some other issues, such as taking over a router, and still being able to monitor all communications.

Taking Over a System or Network

Some Legitimate Purposes:

Networks with routers are essentially taken over by a Network or Systems Administrator all of the time. This is done by using the router to monitor the traffic and send reports, but this process can be complex and does not always work as intended. More often than not, in addition to having the router monitor the traffic, the Administrator will also have some sort of firewall and IDS monitor traffic. Using costly routers, such as CISCO routers, the Administrator can route traffic through the firewall and IDS, control the flow of traffic, gather statistics, or gather suspicious packets for review.

Now that we have seen how to monitor traffic, and we have seen that the technique above cannot gather all traffic on a routed network, we should be better able to understand why someone might want or need to take over the network. If you take over the network, you can see all of the traffic across the network using the monitoring techniques described above.



WARNING: It is illegal to take over a network or system that you do not own without the owner's permission!

Techniques:

ARP Cache Poisoning:

Procedures:

Uses—Cain & Abel

1. Open Cain & Abel
2. Click “Configure” from the menu and make certain that the proper network is selected
3. Click on the “APR (Arp Poison Routing)” tab if you wish to hide your identity, otherwise continue to step 4
 - a. Under “Spoofing Options” click on the radial button “Use Spoofed IP and MAC address”
 - b. Enter a free IP address for your network; if you already know what address is free, skip to step 3. b.
 - i. Click the “Cancel” button
 - ii. Click the “Sniffer” tab
 - iii. Activate the Sniffer by clicking on the “Activate/Deactivate Sniffer” button (second from the left in the taskbar), if it is not already active (Fig. 4)
 - iv. Press the button that looks like a plus-sign (fourth from the left in the taskbar) (Fig. 4)
 - v. Check the option under “Promiscuous-Mode Scanner” that says “All Tests”
 - vi. Press the “OK” button
 - vii. Once Cain & Abel finishes the scan, click “Configure” again
 - viii. Proceed back to the “APR (Arp Poison Routing)” tab
 - ix. Enter in an IP address that is in your subnet (between any number that showed up in your scan from 1 to 254) that did not appear in your scan
4. Click the “OK” button

5. Click the “APR” tab at the bottom of the window
6. Click on the “APR” icon in the left menu, if it is not already selected

7. Click on the top window in the center frame (see Fig. 5)

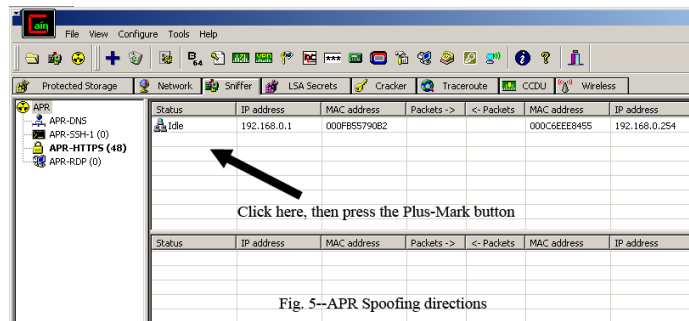


Figure 5--APR Screen Layout

8. Press the button that looks like a plus-sign (fourth from the left in the taskbar) (Fig. 4)
9. Select the gateway from the left pane. If you know which system is the gateway, continue to step 10.
 - a. Open the Start Menu
 - b. Click the “Run...” button
 - c. Type command and press the “Enter” or “Return” key
 - d. Type ipconfig and press the “Enter” or “Return” key
 - e. Use the “Default Gateway” as the gateway for step 9.



WARNING: If the gateway receives more traffic than your system can handle, packets will be dropped and the network may become slow and unstable!

10. Select the system that you wish to target from the right pane (you can select multiple systems, or all of the systems, depending on how many you wish to monitor) (Fig. 6)

11. Press the “OK” button

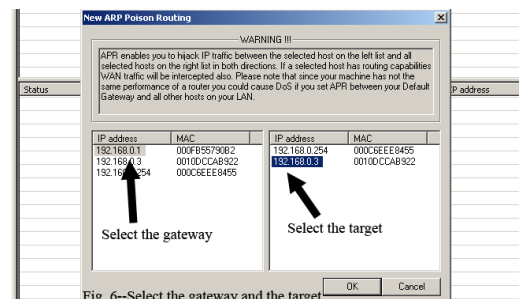


Figure 6--Select the gateway and the target

12. To activate ARP cache poisoning, the “Start/Stop APR” button must be depressed (the third button from the left in the taskbar) (Fig. 4)
13. You have now high-jacked the network and can use one of the above monitoring techniques to monitor traffic

NOTE: In performing the ARP Cache poisoning, you have already started the Monitoring a Network: Secured Network technique; all that is left is to run Ethereal if you wish to view all packets.

Limitations:

This technique works on Layer 2 systems (i.e. switches and bridges) and will work on routers, but with less success. If you are trying to work with a router, DHCP/DNS spoofing or Routing Information Protocol spoofing will be more fruitful and easier as you only poison the router, instead of having to poison multiple systems on your network.

Routing Information Protocol (RIP) Spoofing:

There are currently two versions of RIP: RIP v1 and RIP v2. RIP v1 has no authentication, thereby allowing anyone to send packets to the RIP router. RIP v2 has authentication, but it is cleartext, so if you use Cain & Abel and sniff traffic as described in the chapter “Monitoring a Network” you will be able to see the password. Most routers use RIP so that Administrators do not have to input routes for traffic to take manually in environments where there are multiple routers.

Using Cain & Abel you can easily monitor the RIP tables. Spoofing RIP is as simple as using Packet Excalibur to make a RIP packet where you set your IP as being the gateway (similar to ARP cache poisoning). Unlike ARP cache poisoning, however, there is currently no software that will perform all of the steps necessary to allow the traffic to come to your system and then be forwarded to the final destination. This manual does not intend to go into such depth, however *Hacking Exposed: Network Security Secrets & Solutions* has detailed instructions as to how to perform the steps required to not only spoof a RIP packet (use Packet Excalibur instead of srip), but also to forward the traffic to its final destination (pp 394-396).



WARNING: If the gateway receives more traffic than your system can handle, packets will be dropped and the network may become slow and unstable!

DHCP/DNS Spoofing:

Dynamic Host Configuration Protocol (DHCP) is used to give systems on a network an IP address that is not currently in use. To spoof DHCP, you merely have to install and configure a DHCP server where you route all traffic through the server, calling it a gateway. The server then may examine the traffic, if you wish, and then send the

information to the real gateway. This attack is very simple to perform, with the most difficult part being setting up a DHCP server (Windows 2003 makes this a very simple process, however). Once the rogue server is on the network, DoS any other DHCP servers present, to prevent them from communicating with clients, thereby forcing clients to go to the rogue server to get IP addressing information. Given this manual is not intended to explain how to setup a DHCP server since there are many different ones, see Further Reading for a list of places to procure both a DHCP server and directions on configuration.

Exploiting Vulnerabilities:

A widely used technique for entering and controlling a system or network is by exploiting vulnerability in the software that controls the system or network. Most often, vulnerabilities in software other than the Operating System itself are exploited, largely because Operating Systems are difficult to attack given the amount of code evolved. Finding vulnerability in an Operating System as large as Linux or Windows is a massive undertaking since the code for each is well into the millions of lines.

Software vulnerabilities could be as simple as a way to get around having to use a password to view sensitive information. Given the large amount of software on most machines, finding software that can be exploited on a machine is trivial. A very helpful resource containing vulnerabilities is SecuriTeam and can be found on the internet at <http://www.securiteam.com>. Merely search for vulnerability in select software, find a good vulnerability that allows you the power and control that you need, and then exploit that vulnerability.

Denial of Service (DoS):

If traffic is monitored that is damaging to the network in some fashion, serious action can be taken, such as shutting down the offender with a Denial of Service if physical access is not available or timely. It is also good to examine what a DoS looks like by monitoring the traffic while attempting a DoS. While the concept over a Denial of Service remains the same, the methods of triggering one are constantly changing. Many DoS attacks exist, but it is important to note that as these attacks age, they are often rendered obsolete by patches and fixes.



WARNING: Denial of Service attacks can do serious damage to the system being attacked, including loss of information and harming the whole network!

Big Pipe-Little Pipe Denial of Service:

This attack is where the attacker simply has more network speed and resources available than the victim does. The attacker overwhelms the network of the victim with traffic (it can be either valid or invalid traffic), leaving the victim's network unable to communicate with the outside world or, in the worst case, being able to communicate even internally. These sorts of DoS attacks were highly popular when cable internet began to make its debut because phone modems were far less capable. The Distributed Denial of Service attack is merely a variant of this technique, using multiple systems to simulate a bigger "pipe" than the victim does.

Distributed Denial of Service (DDoS):

Distributed Denial of Service attacks are arguably the most destructive of the DoS attacks available. Many times "zombies" are linked together and programmed to launch a DoS at or near the same time on a single system or network. There is, however, a far more destructive and insidious form of DDoS that has scared both Administrators and the "black hat" communities alike: the use of high capacity, powerful routers and servers to amplify attacks. This method is highly dangerous as the systems amplifying the attacks are at speeds above T3, which is the speed that corporate and government networks operate at near the Point of Contact (where networks are brought together to connect to the internet). This form of DDoS is thought to have moved from the theoretical realm to the physical realm in 2000 when major websites around the world were attacked (*Hacking Exposed* p 494).

Ping of Death and SYN Floods:

The "Ping of Death" is an attack whereby you can merely ping the victim until it crashes or becomes unresponsive. This attack has largely been patched against by Operating Systems but is the parent of SYN floods and similar attacks. SYN floods involve spoofing the sending address to a non-existent IP address. When the victim receives the spoofed packet, it attempts to reply by sending an ACK

(Acknowledgement) to the IP address that allegedly sent the packet. The victim will wait a period of time (ranging from 75 seconds to 23 minutes based on the Operating System) for a response, holding resources for in case there is a response. The attacker continues to send the spoofed packets and drains the victim's resources to the point that the victim locks up or shuts down completely.

Password Cracking:

Against a Web Interface:

Web interfaces are normally trivial to break into because usually the password is not encrypted. If you use the monitoring techniques for secured communications presented in "Monitoring a Network", you will find that you can easily see passwords and usernames for most websites. Some sites, however, encrypt the passwords using a variety of techniques, or perhaps you wish to break into your router and do not know the password. If the password is encrypted, tools such as AccessDiver try to figure out a password; however, they can be very slow and are easily detected. The best way to find a password in such a case is to direct traffic to a system under your control and then to use Cain & Abel to grab the SSL certificates. You then "remake" the website in question, but do not encrypt the password. When a victim logs into your fake site, you will have the password and username and can easily peek into the account in question.

Against an LM and NTLM Network:

Procedures:

1. Open Cain & Abel
2. Sniff the network using the "Monitoring a Network" chapter's "Secured Networks" subchapter
3. Click on the "Cracker" tab
4. Click on "LM & NTLM Hashes" in the tree to the left

Uses—Cain & Abel

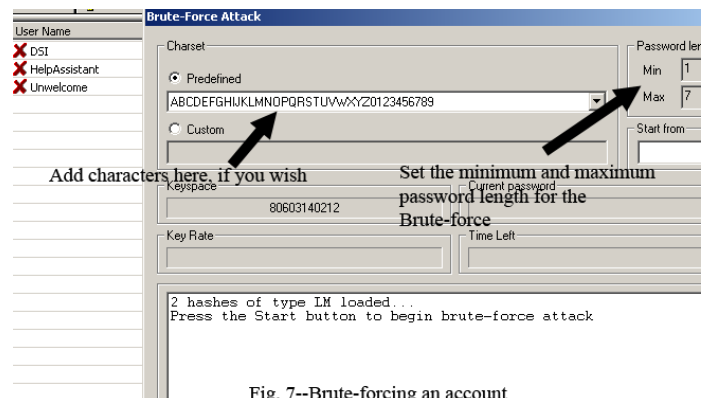


Fig. 7--Brute-forcing an account

Figure 7--Brute-Force Layout

5. To import local accounts, or accounts from a .pwd or .sam file click on the plus-sign in the toolbar and follow the appropriate steps
6. Right click on an account and select either Brute-Force Attack or Dictionary Attack
7. If Brute-forcing, give the characters that you wish to use in the brute-force and the length (Fig. 7)
8. If using a dictionary attack, give the .txt file that contains words that you wish to check
9. Press the “Start” button
10. When the attack is finished, press the “Exit” button and examine any passwords that have been revealed

Against a Windows Account:

Follow the above directions for cracking against an LM and NTLM network, making certain to follow step 5. The easiest way to crack a password is on the system that contains the password or else you have to manage to get the .sam file, if it is a Windows NT, 2000, 2003, XP, or Vista system. If it is a Windows 9x machine, you have to get the .pwl file. The password file on a Windows NT based system is protected and you have to be skilled to get a hold of the file, if you do not have physical access to the system that holds the file.

Bypassing Passwords:

Windows 9x:

Keeping in mind that Windows 9x (that is to say, Windows 95, 98, and Millennium Edition) were never built or marketed for security, bypassing passwords on it is trivial. When a Windows 9x machine asks for a password or for you to log into the system, merely hit the “Cancel” button and you will log into the system anyway.

****NIX:***

*NIX is any Operating System based off the UNIX concept, including UNIX itself. Most *NIX Operating Systems are Open Source and free, so they have gained

acceptance into some circles. Open Source software is software that is available to the public for examination, modification, and recreation. While the concept of UNIX is that the community owns the software and enhances it, this has not shown to offer much in the way of perfecting the security of the Operating System. Furthermore, many formerly free Operating Systems that fall under the *NIX category are requiring payment to “license” the software. This movement is largely because the cost to build and maintain the code, as well as to own servers to store and distribute the code, is astronomical and in many cases donations could not cover the expenses.

UNIX, Linux, and Mac OS X:

Root passwords on these systems are the Holy Grail. *NIX systems contain a flaw such that you can boot into repair mode and set the root password. The worst part is that it does not take a password to do this, merely insert a *NIX installation CD, reboot from the CD, and boot into the repair installation mode. Not only do you bypass the password requirements, but also you can now change the root password for the system and then reboot with complete control of the Operating System.

Bibliography

FX, et al. Stealing the Network: How to Own a Continent. Boston: Syngress, 2004.

Harris, Shon, et al. Gray Hat Hacking: The Ethical Hacker's Handbook. New York: McGraw-Hill, 2005.

Klevinsky, T. J., Scott Laliberte, and Ajay Gupta. Hack I.T.—Security Through Penetration Testing. Boston: Addison-Wesley, 2002.

McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed: Network Security Secrets & Solutions. 5th ed. New York: McGraw-Hill, 2005.

Mitnick, Kevin D., and William L. Simon. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers. New York: John Wiley & Sons, 2005.

Mullen, Timothy, et al. Stealing the Network: How to Own an Identity. Boston: Syngress, 2005.

Zimmermann, Hurbert. "OSI Reference Model—The OSI Model of Architecture for Open Systems Interconnection". *IEEE Transactions on Communications* 28 (Apr. 1980): 425-432.

Appendix A: Links to Software Used

AccessDiver: <http://www.accessdiver.com/>

Cain & Abel: <http://www.oxid.it/cain.html>

Ethereal: <http://ethereal.com/download.html>

Packet Excalibur: <http://www.securitybugware.org/excalibur/>

WinPCap: <http://www.winpcap.org/install/default.htm>

Appendix B: Glossary of Terms and Acronyms

ARP—Address Protocol Resolution. Used by networks to direct traffic to the appropriate gateway

Brute-Force—Brute-forcing is an attempt to discover a password by checking combinations of characters of certain lengths. This method can be very slow

Dictionary Attack—Dictionary attacks are where you take a file that contains words to be checked. Often times you will configure the attack to add certain characters before and after a word in the dictionary, so that you can discover weak passwords such as ‘hi123’ or ‘password6’

DHCP—Dynamic Host Configuration Protocol. The protocol used for giving IP addresses to systems and lookup those IP addresses that have already been given

DNS—Domain Name Server/Service/System. This is used to translate a name, such as <http://www.microsoft.com> into an IP address so that the computer is actually able to contact the system in question

HTTP—Hypertext Transfer Protocol. The protocol used for sending the information required to view a webpage

IP address—Internet Protocol address. This address must be unique on a given network and serves as an identifier for those attempting to communicate with the system holding the IP address. If two systems hold the same IP address on the same network, the network will not know which system to send information to and which system sent the information

LAN—Local Area Network. An intranet; a system of computers grouped together using a networking device

LM—LAN Manager. The method used by Windows 9x and NT to communicate file and printer sharing information on a LAN

NTLM—NT LAN Manager. This is the NT version of LM and offers far more security. There are two versions of NTLM, with NTLM v1 being decent security (although it can be cracked) and NTLM v2, which is used by Windows XP, 2003, and Vista, being generally considered highly secure

OS—Operating System. This is software that includes a kernel. Operating Systems are generally intended to provide an easier means for programmers to program by giving libraries and pathways for programmers to use

OSI Model—Open Systems Interconnection Reference Model. This model divides the functions of a protocol into seven distinct layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

RIP—Routing Information Protocol. This protocol runs on UDP, instead of TCP, and is used by routers to share routing tables and routing information

TCP—Transmission Control Protocol. This is the predominately-used protocol for internet communications, including HTTP communications

UDP—User Datagram Protocol. This protocol does not require connections to be initiated, unlike TCP and is used for streaming information. UDP should be avoided as much as possible

WAN—Wide Area Network. This is normally used to mean the internet, but it includes any network not inside of the LAN

List of Figures

Figure 1--Ensure that the above are check-marked	2
Figure 2--Select HTTP TCP port (80)	3
Figure 3--Select the proper adapter	5
Figure 4--Toolbar Layout	5
Figure 5--APR Screen Layout	8
Figure 6--APR Poisoning Layout	8
Figure 7--Brute-Force Layout	12

*NIX, iii, 13, 14
ARP, ii, iii, v, 5, 7, 8, 9, 17
Brute-Force, 6, 13, 17, 19
Cain & Abel, 5, 6, 7, 9, 12, 16
DDoS, iii, 11
Denial of Service, 10
DHCP, ii, iii, 9, 17, 21
Dictionary Attack, 6, 13, 17
Distributed Denial of Service, iii, 11
DNS, ii, iii, 9, 17, 21

Index

DoS, ii, iii, 10, 11
Ethereal, 2, 3, 6, 8, 16
HTTP, 3, 5, 17, 18, 19
Linux, iii, 10, 14
Mac OS X, iii, 14
RIP, ii, iii, v, 9, 18, *See* Routing
Information Protocol
Routing Information Protocol, 9
UNIX, iii, 13, 14
Windows 9x, iii, 13, 17

Further Reading

The best resources are those listed in the Bibliography, however, there are many more available.

Default Router Password List

<http://www.phenoelit.de/dpl/dpl.html>

DNS/DHCP Spoofing

Farrow, Rick. *Network Defense*. <http://www.spirit.com/Network/net0202.html>

Green, Ian. *DNS Spoofing by The Man In The Middle*. SANS, 2005.

Vulnerabilities

SecuriTeam: <http://www.securiteam.com>