Sipera Systems

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**

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

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

Agenda

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

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

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?

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.**

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.

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

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**

2nd Method: Sniffing with a Hub

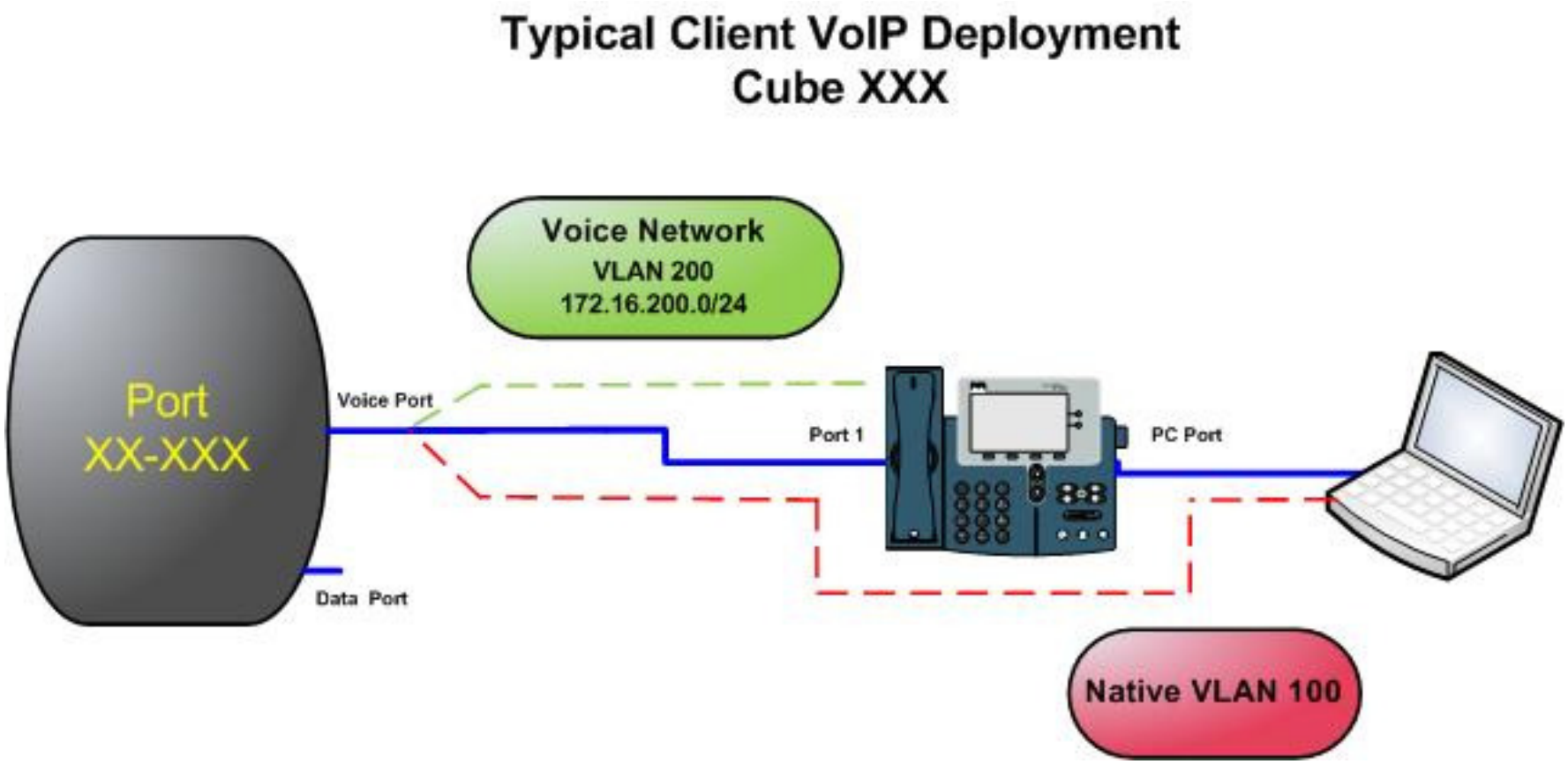
2nd Method: Sniffing with a Hub

- **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

Physical Access to Voice Port

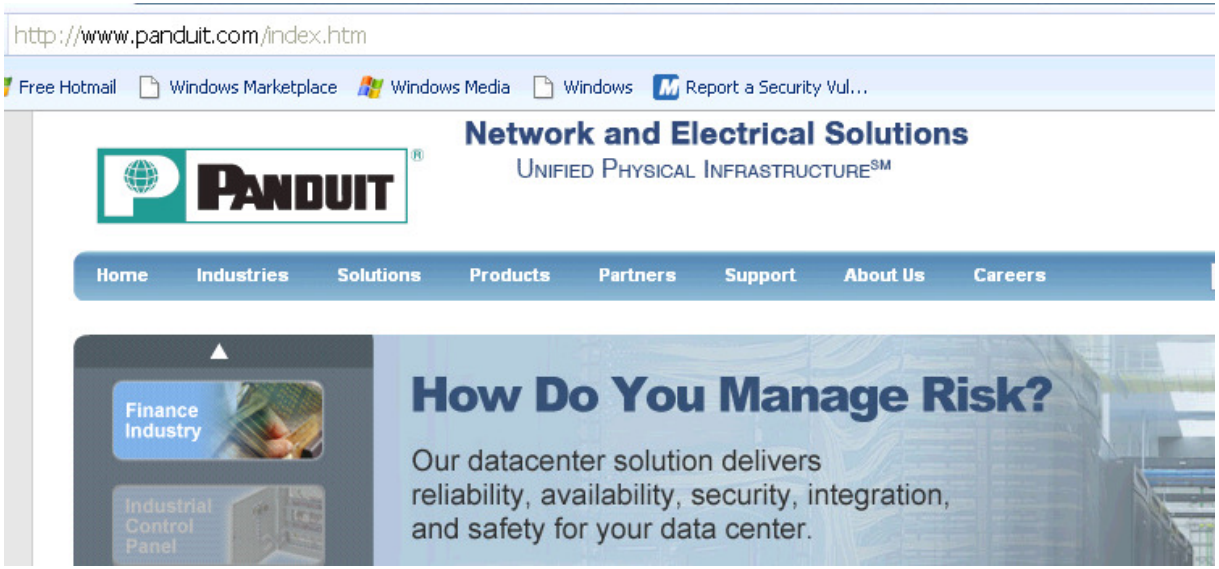
- **Scenario**
  - It's assumed that we are a trusted insider, like any internal VoIP user
  - A typical testing scenario is that the client provides us access to the cube of a regular user, and we can unplug the phone from the wall, plug in our laptop, and run the security testing
- **But do we really 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"**

Typical VoIP Deployment



Physical Access Restricted

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



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**

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

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

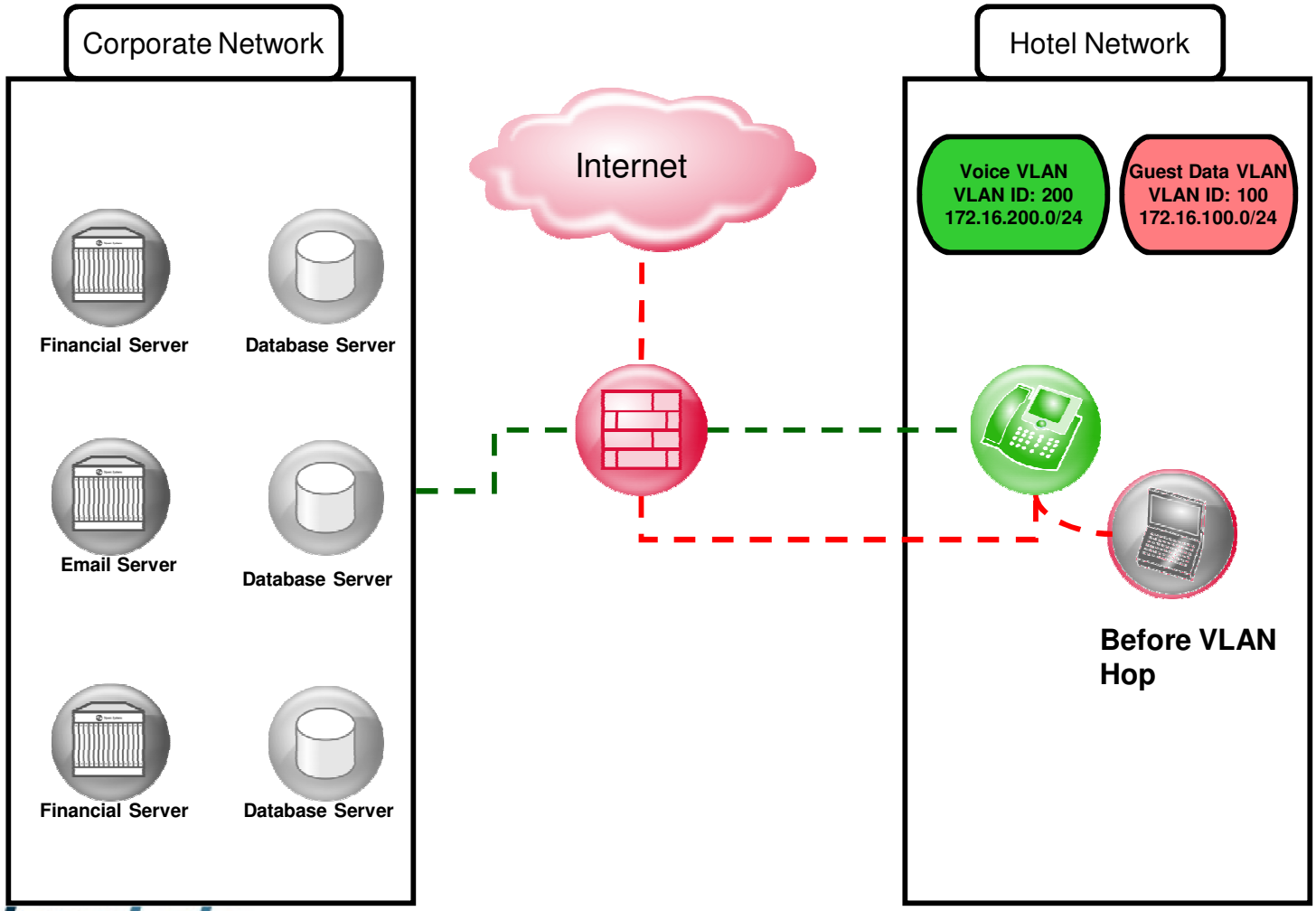
VoIP Penetration Test Results

- 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.

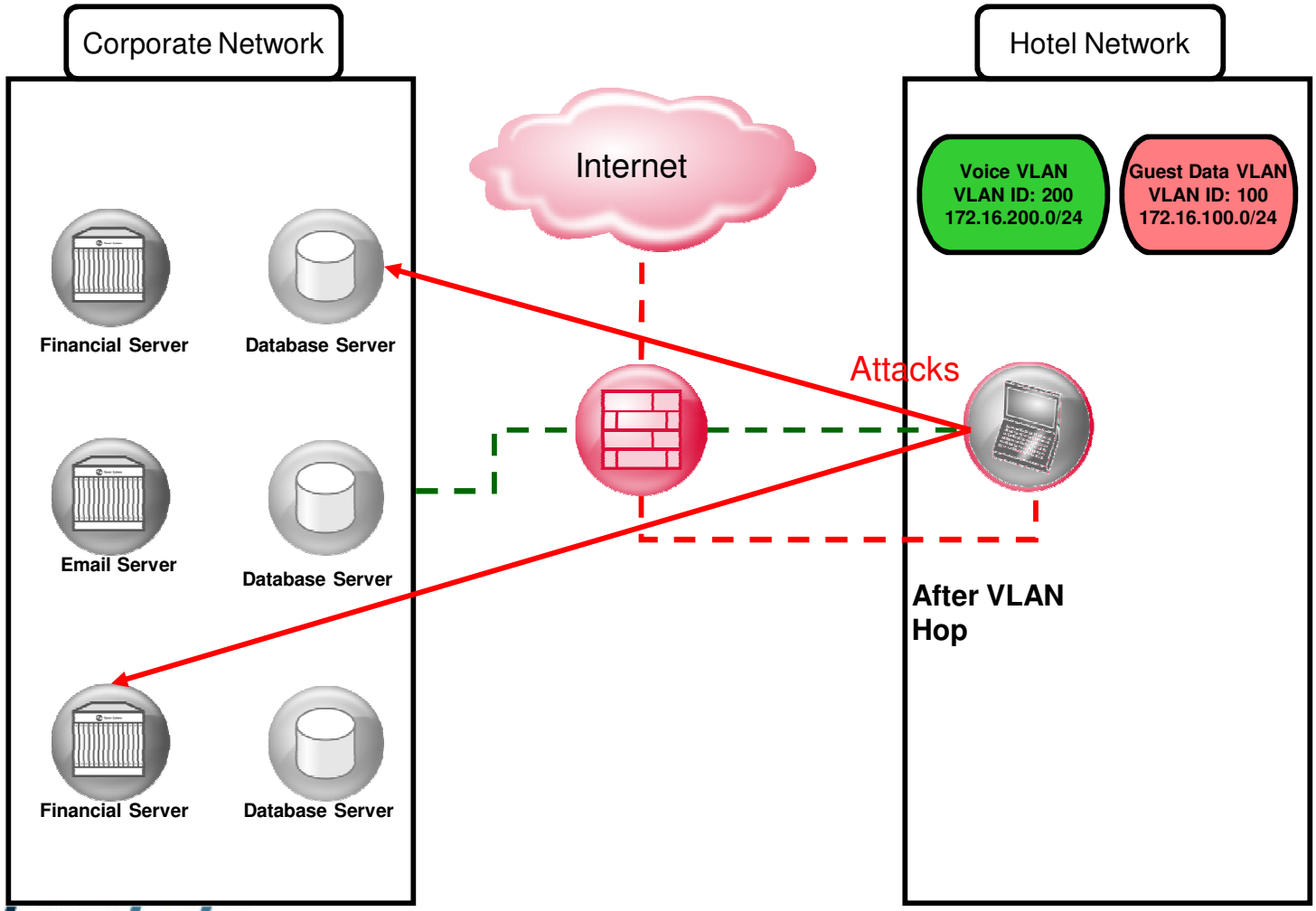
Case Study 1: Hotel Network

- **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

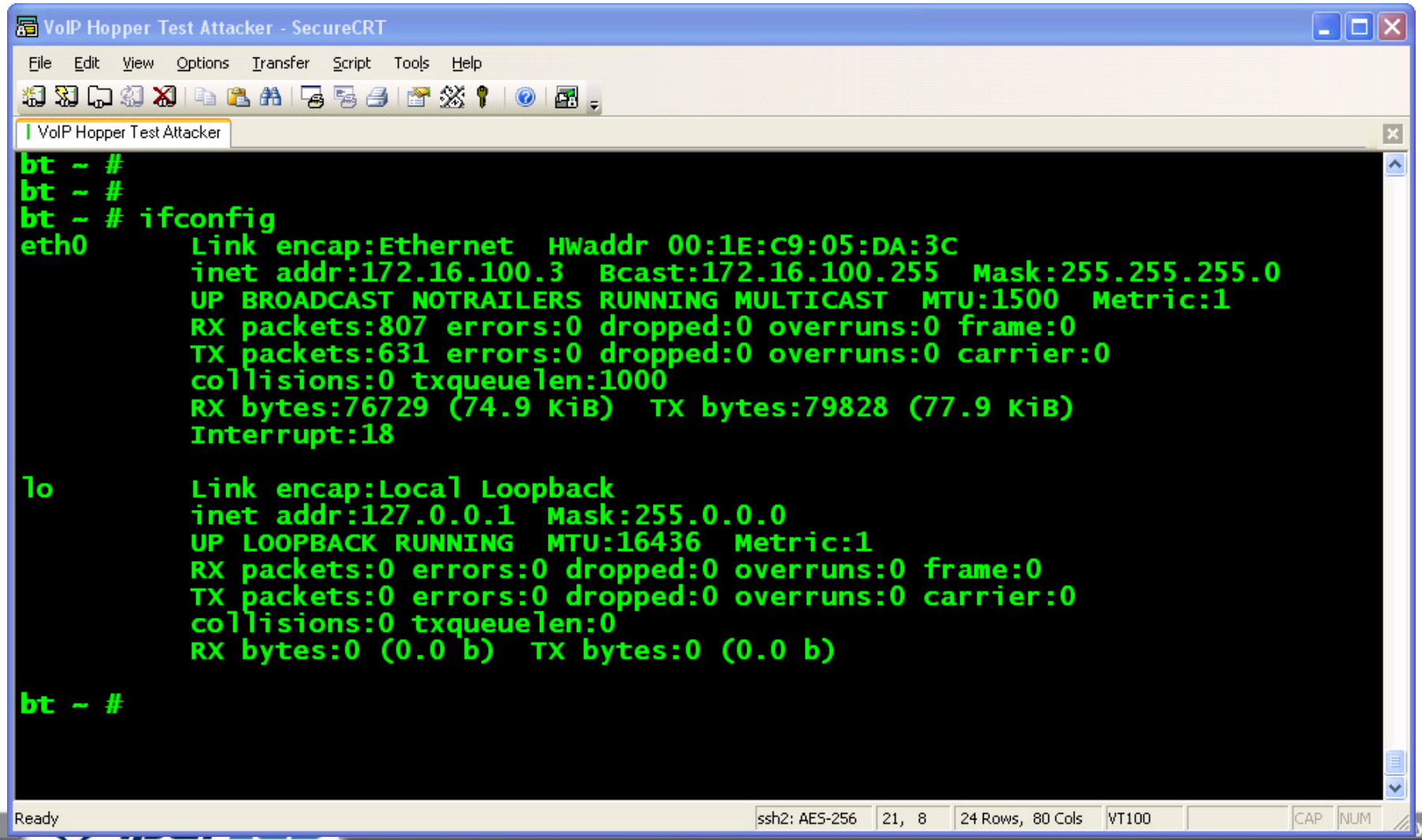
Enterprise VoIP Deployment



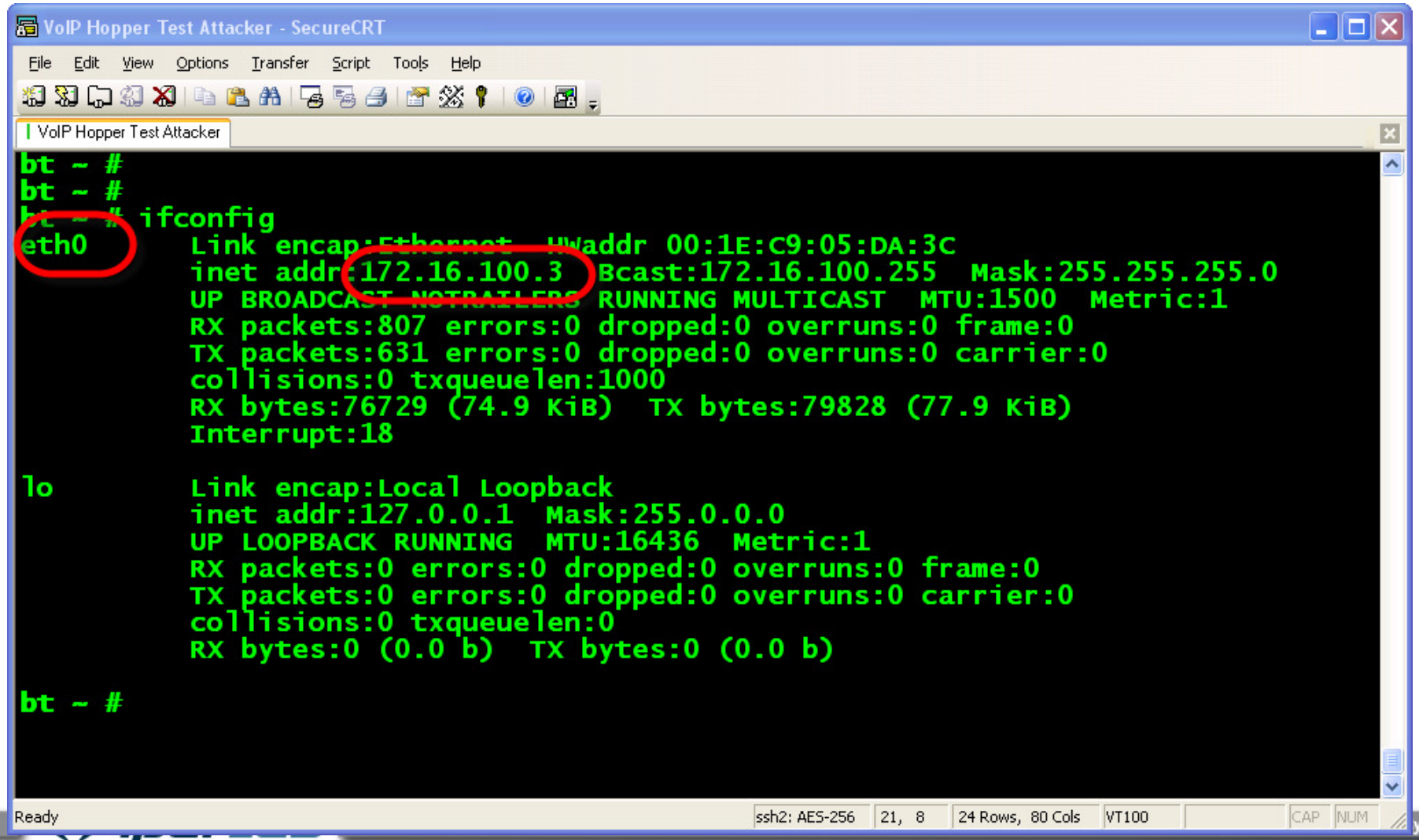
Enterprise VoIP Deployment



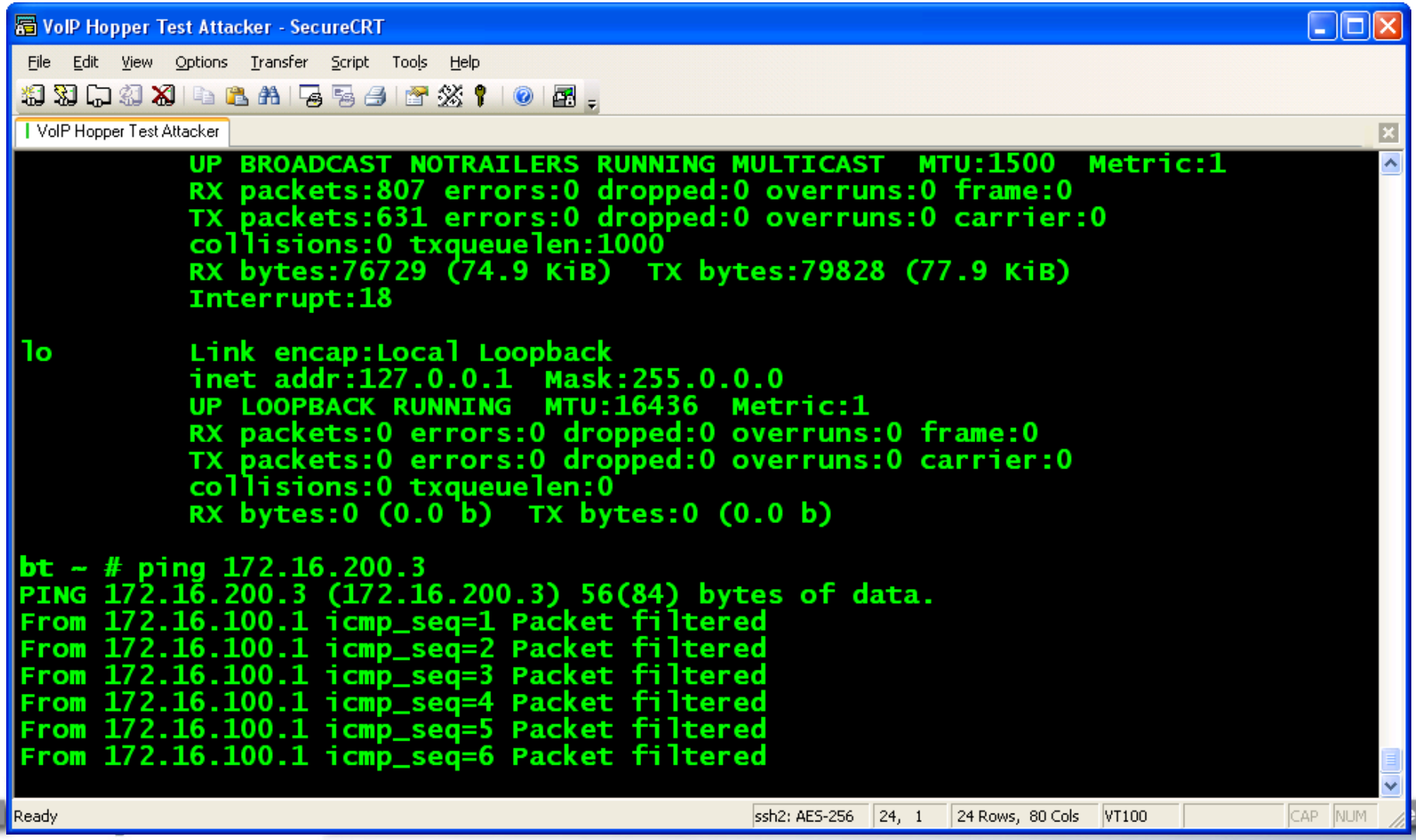
VoIP Hopper Live Demo



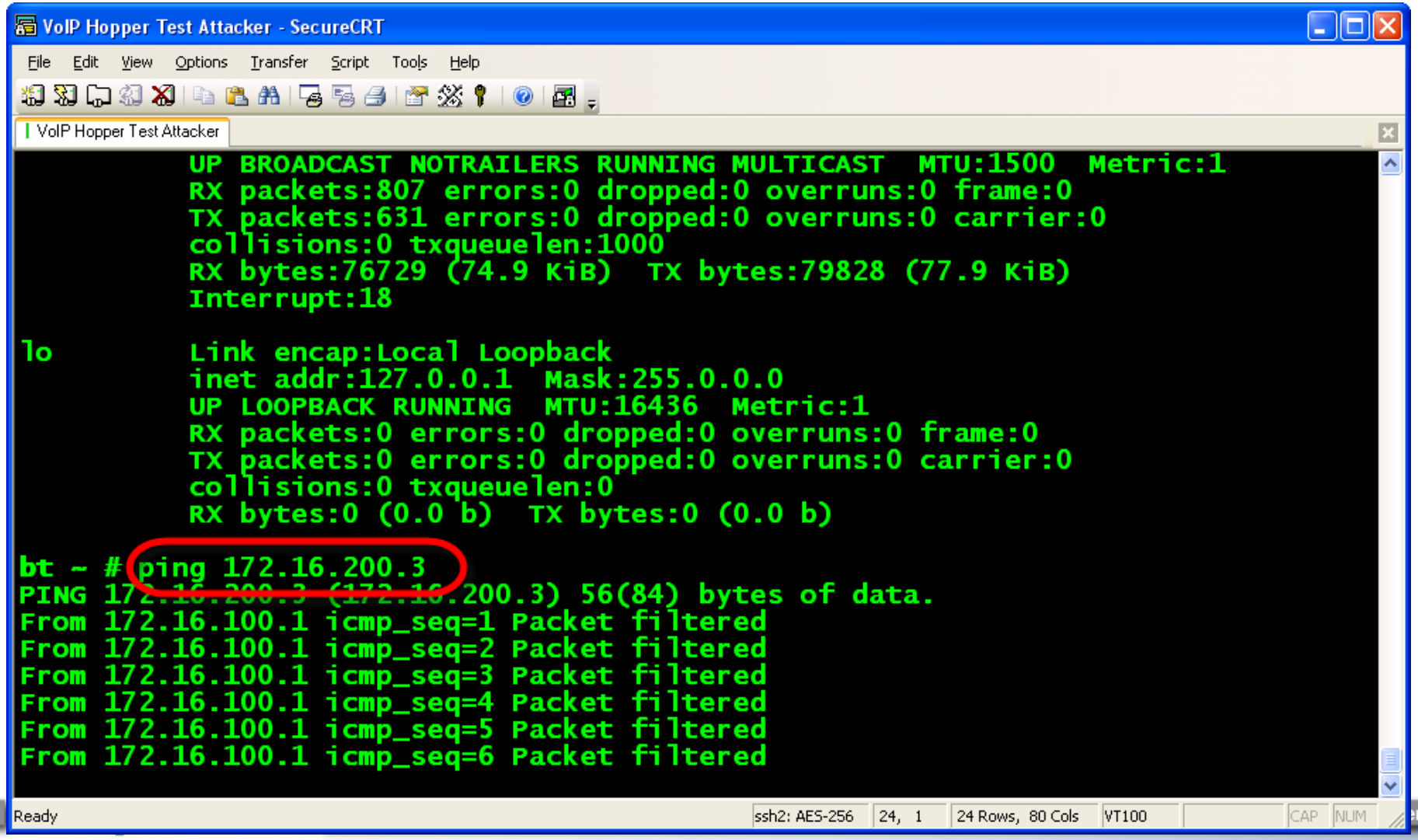
VoIP Hopper: Firewalled Voice Network



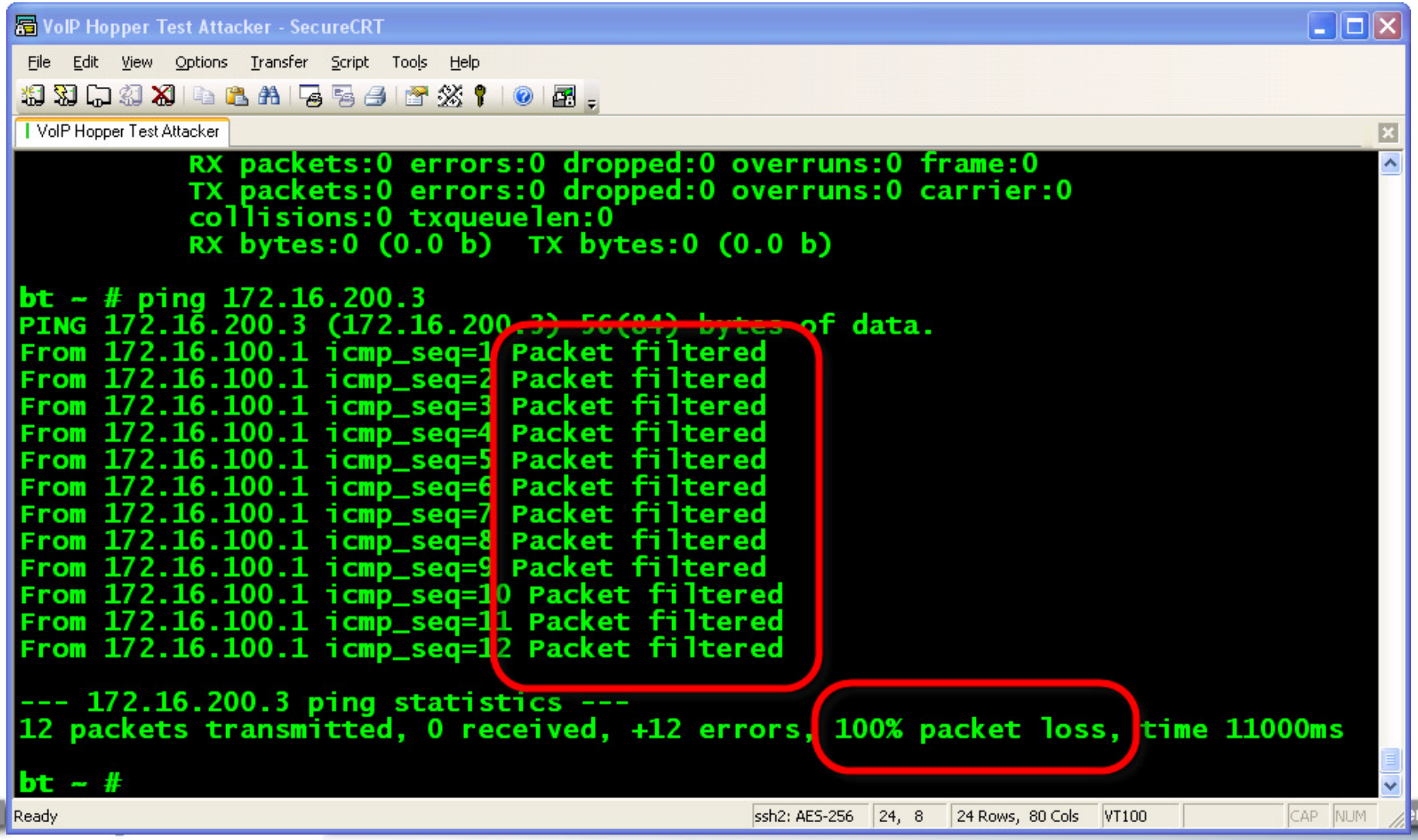
VoIP Hopper: Firewalled Voice Network



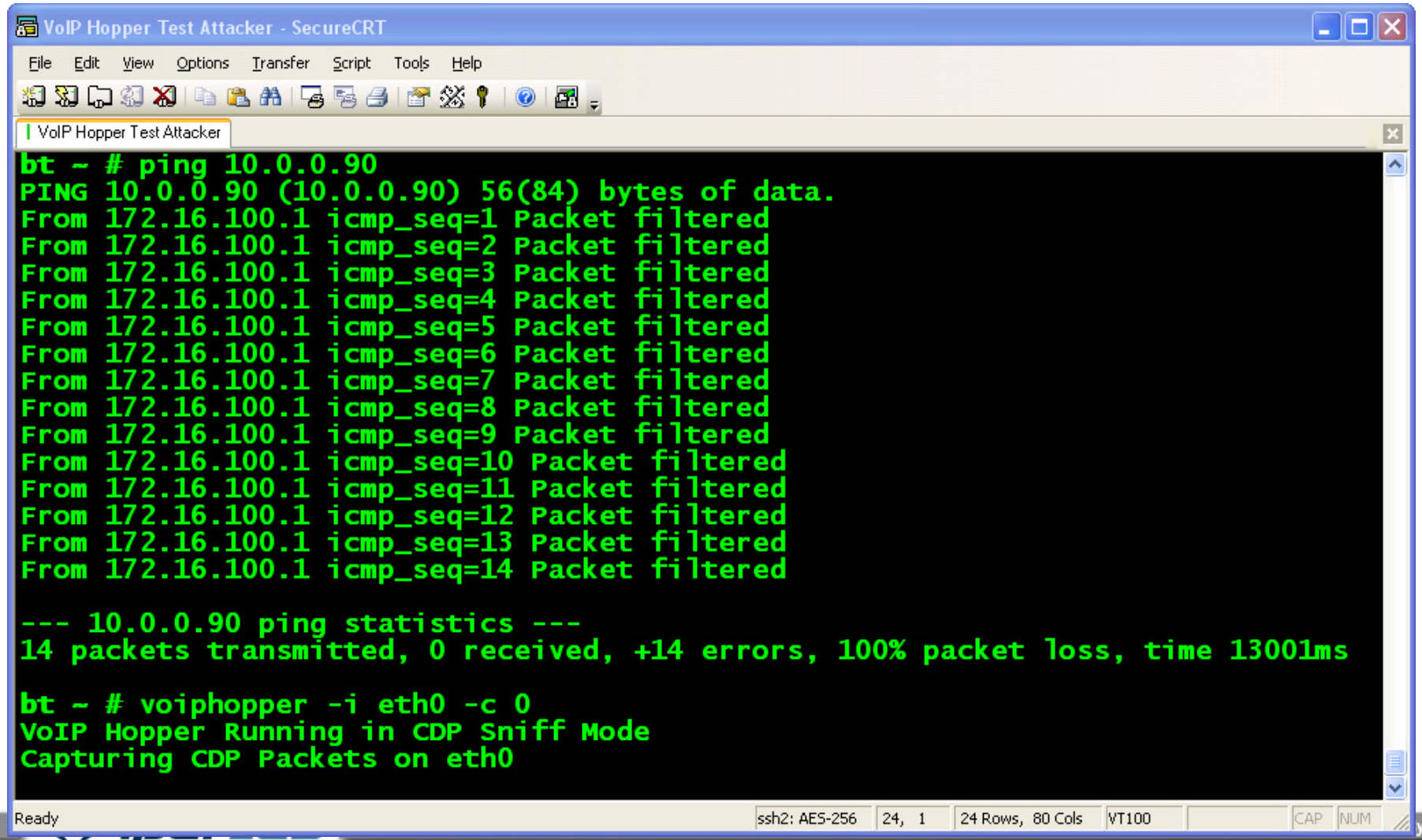
VoIP Hopper: Firewalled Voice Network



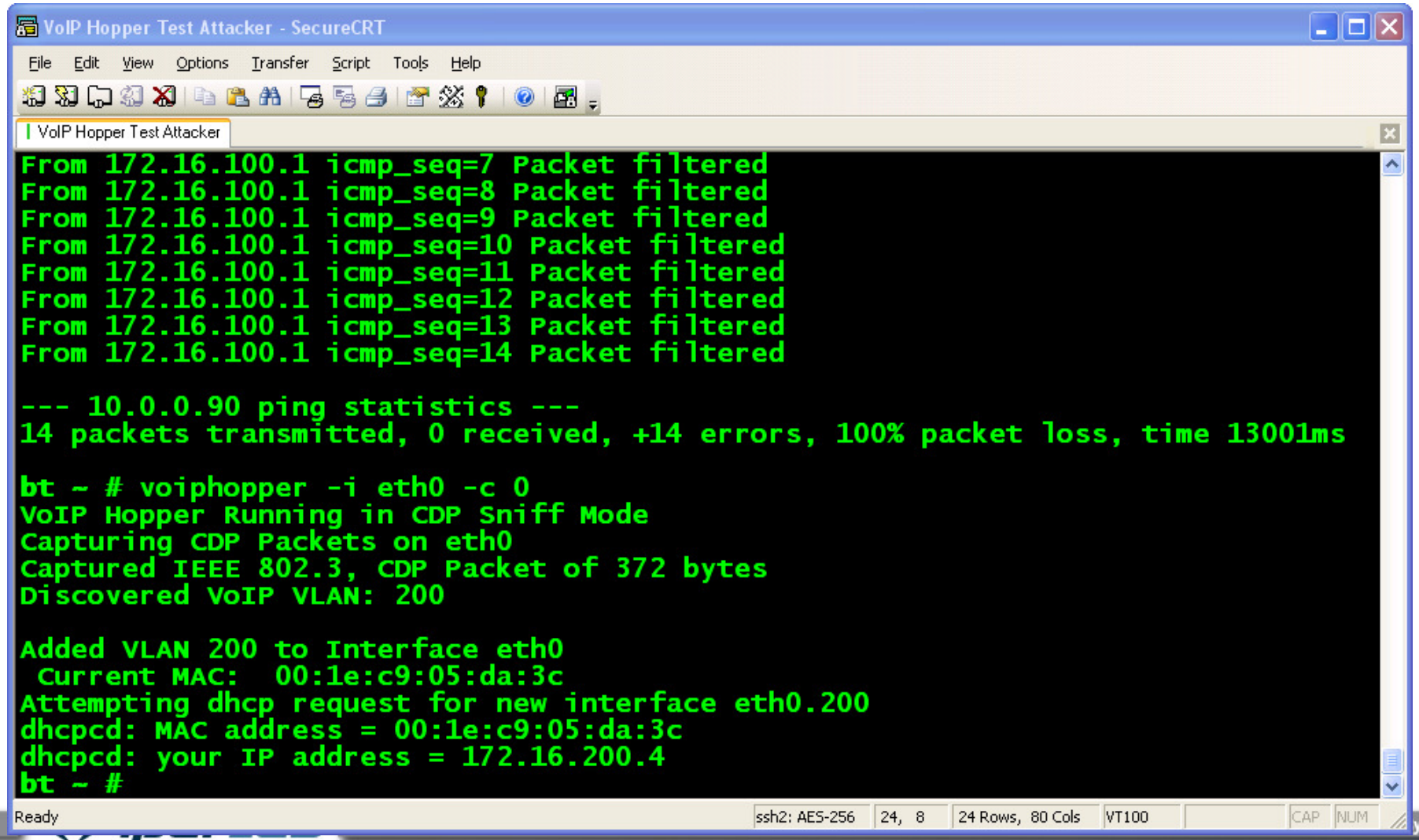
VoIP Hopper: Firewalled Voice Network



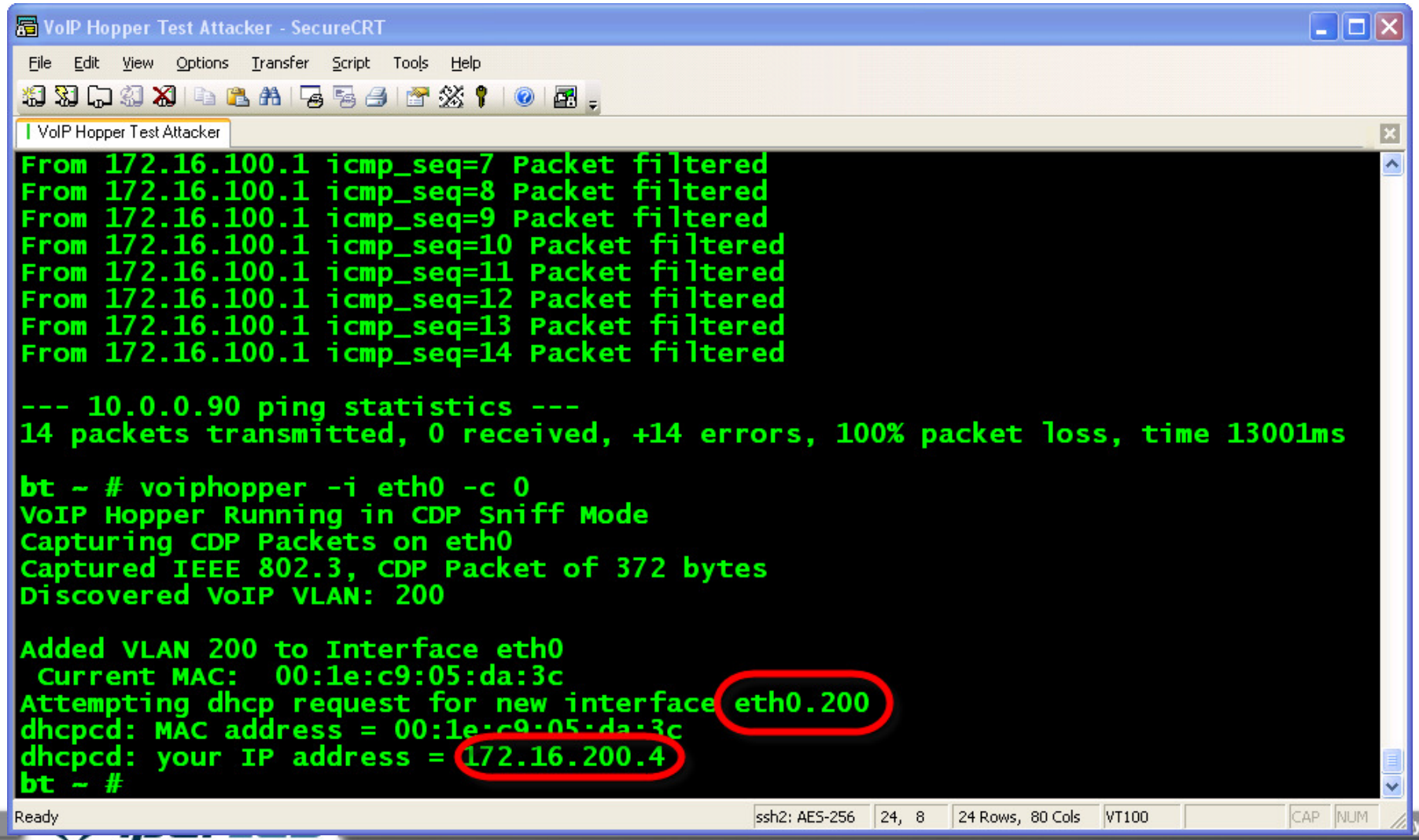
VoIP Hopper: Firewalled Voice Network



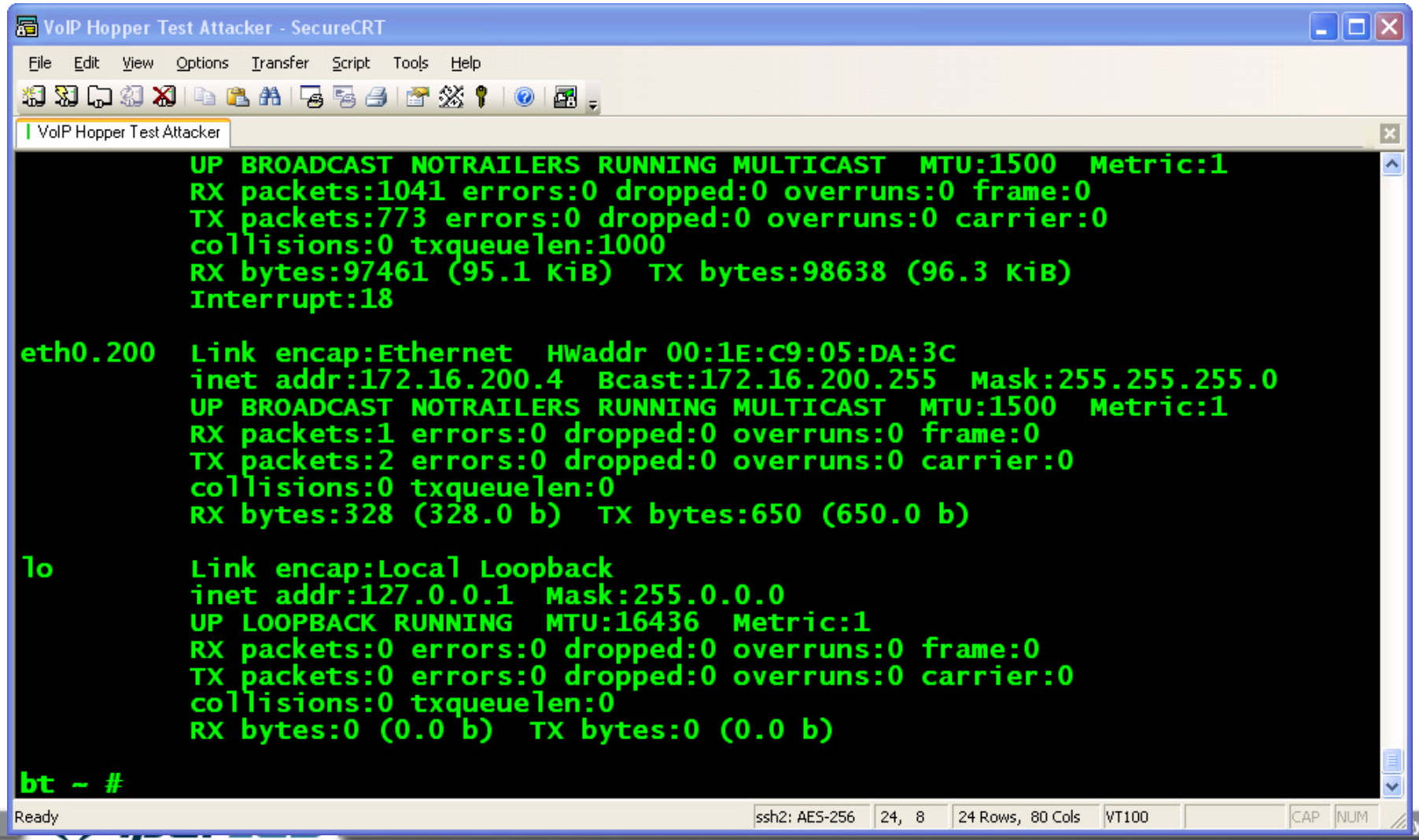
VoIP Hopper: Firewalled Voice Network



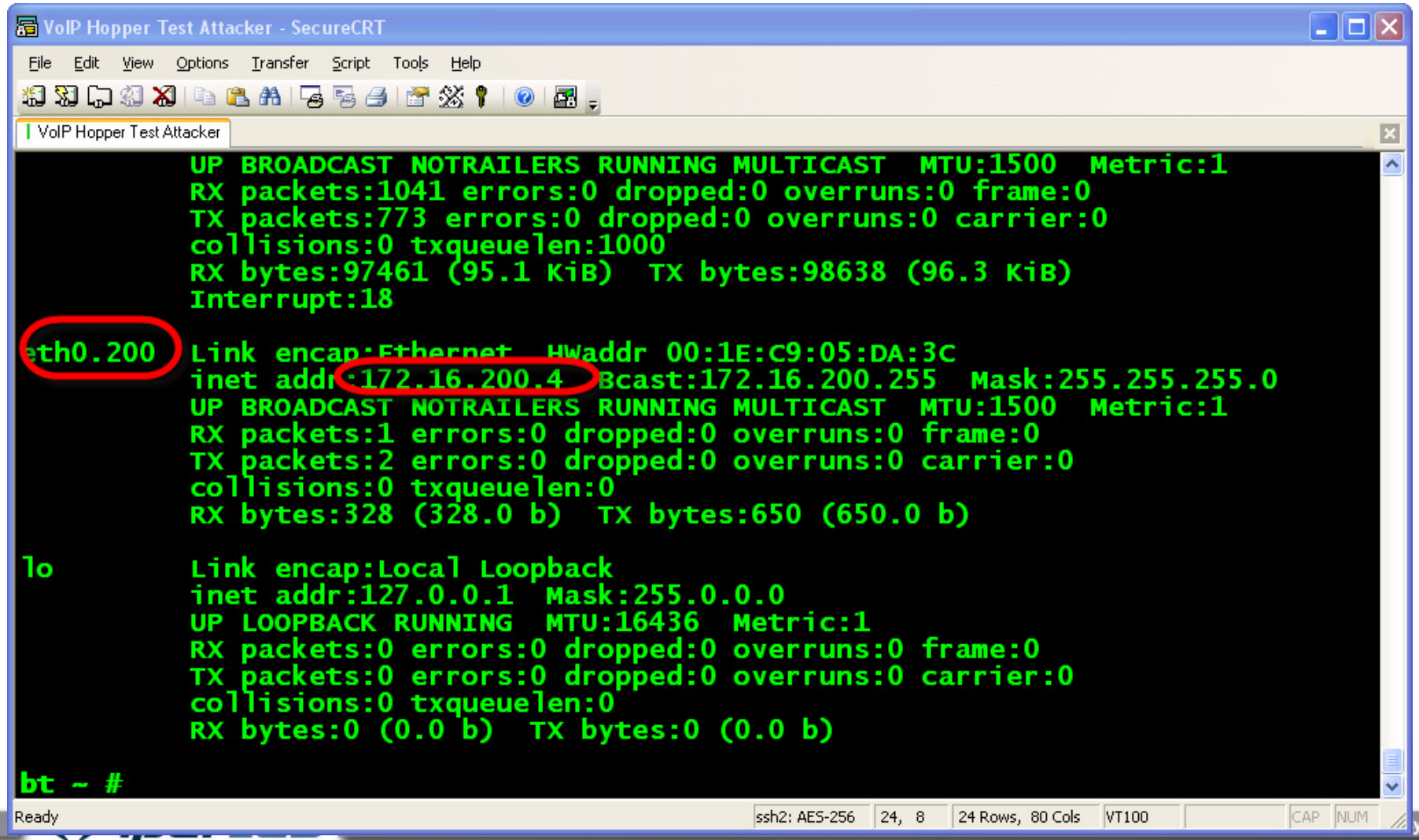
VoIP Hopper: Firewalled Voice Network



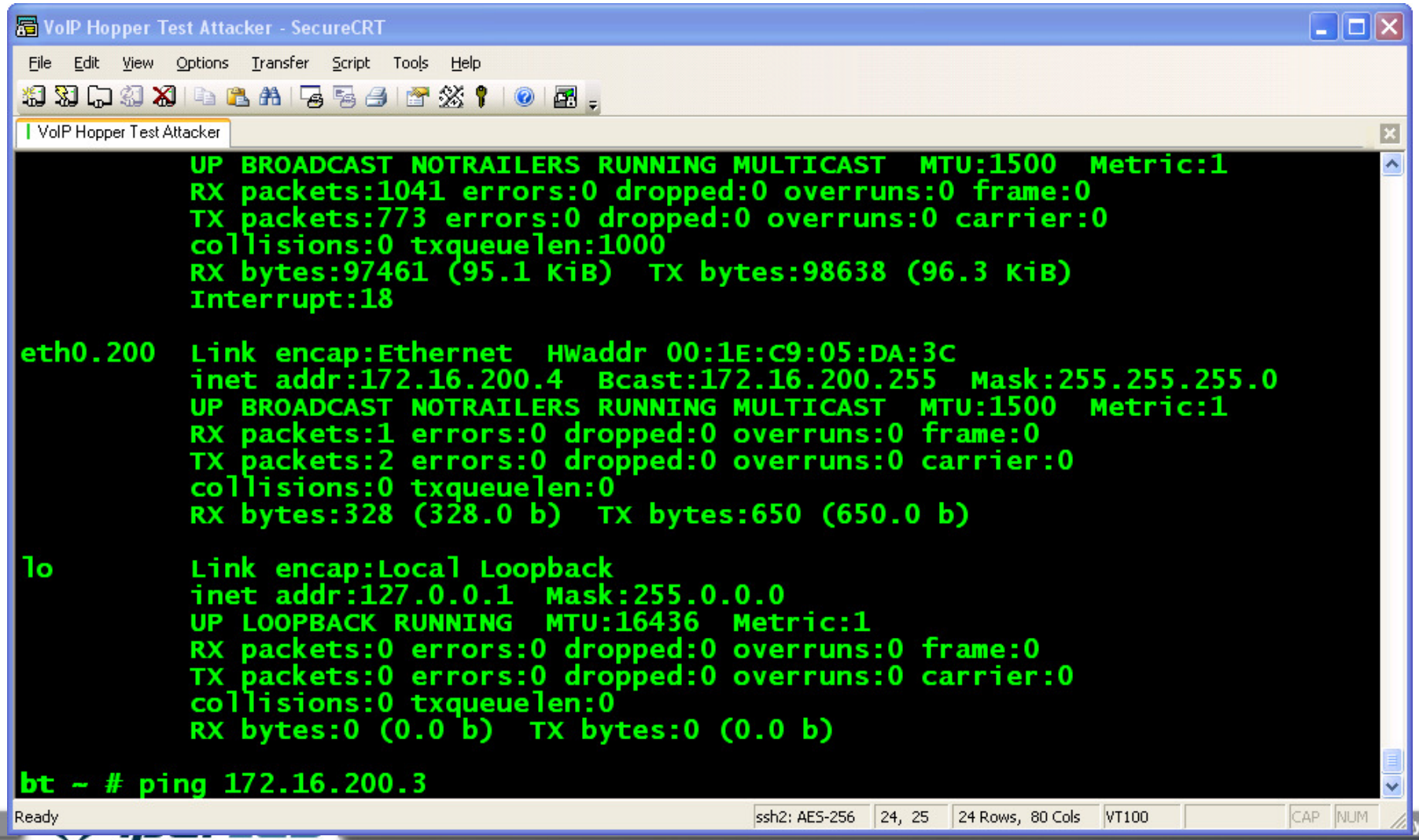
VoIP Hopper: Firewalled Voice Network



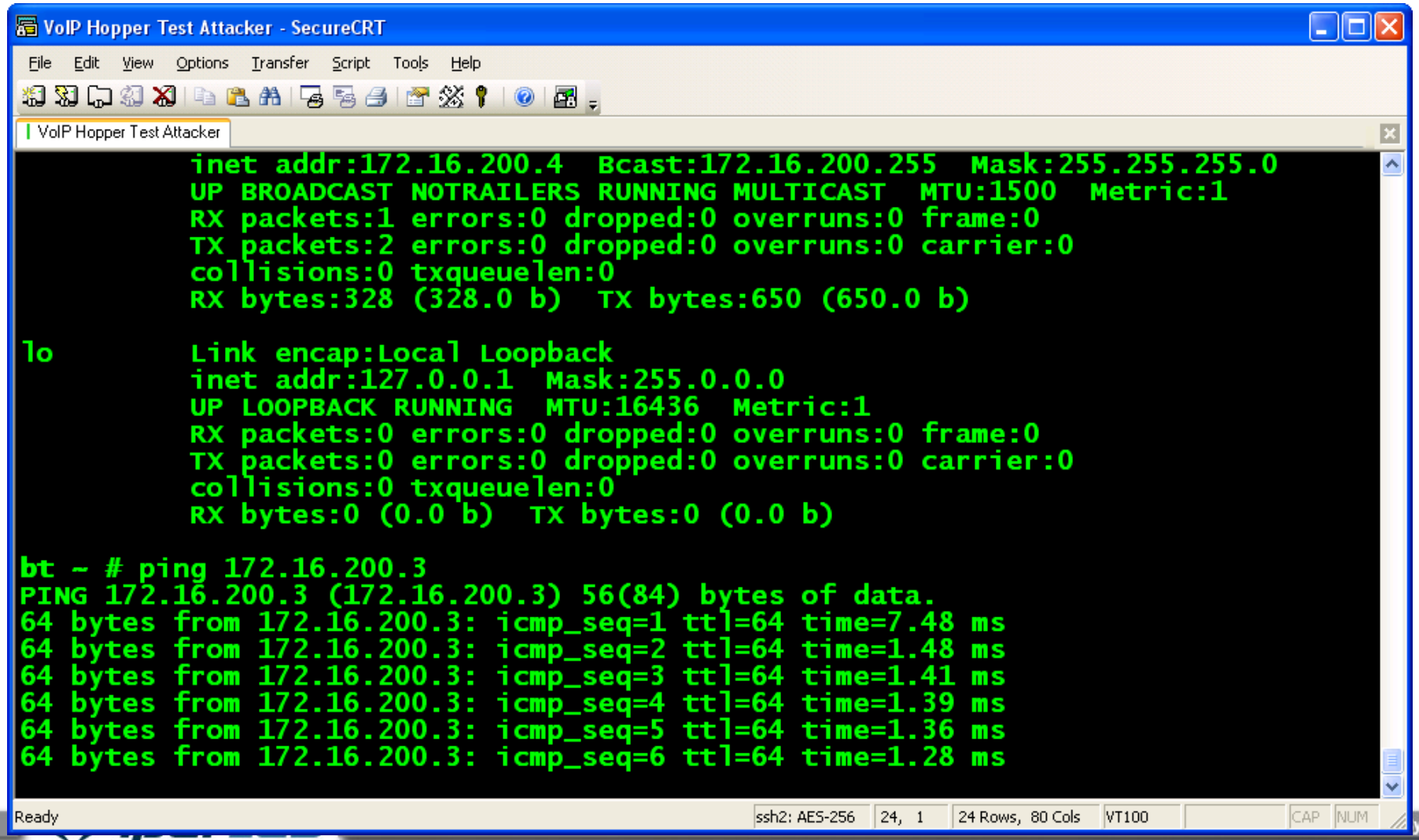
VoIP Hopper: Firewalled Voice Network



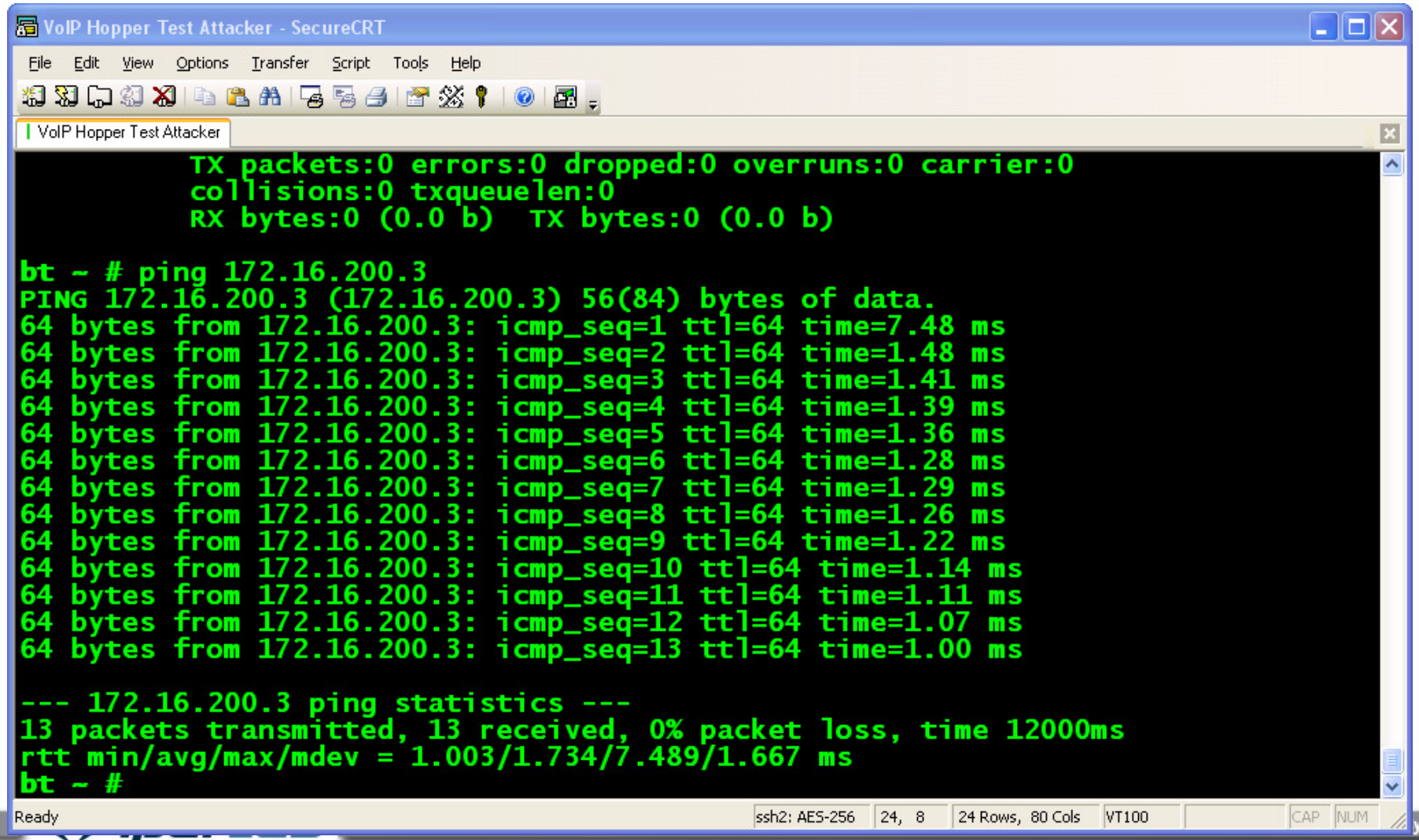
VoIP Hopper: Firewalled Voice Network



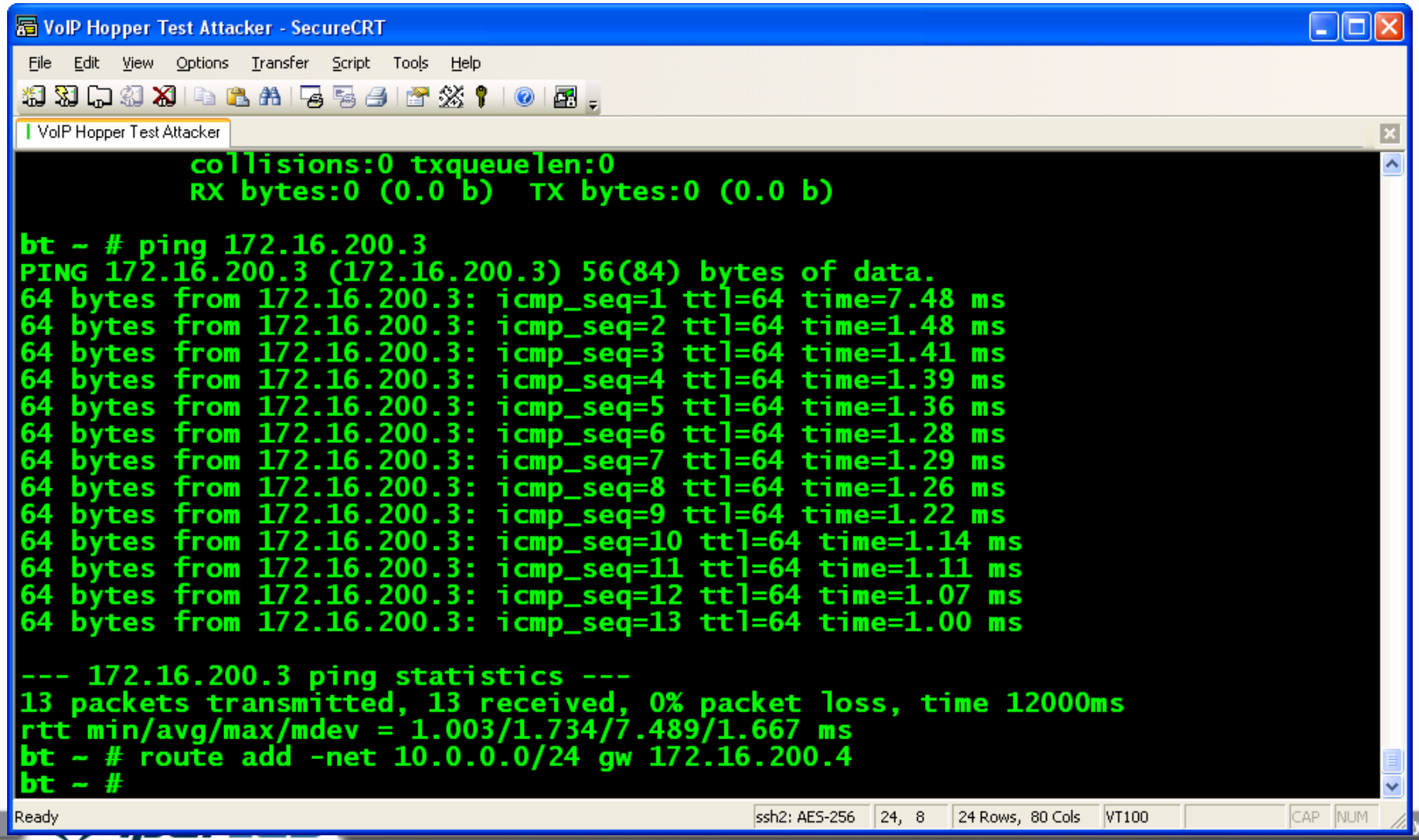
VoIP Hopper: Firewalled Voice Network



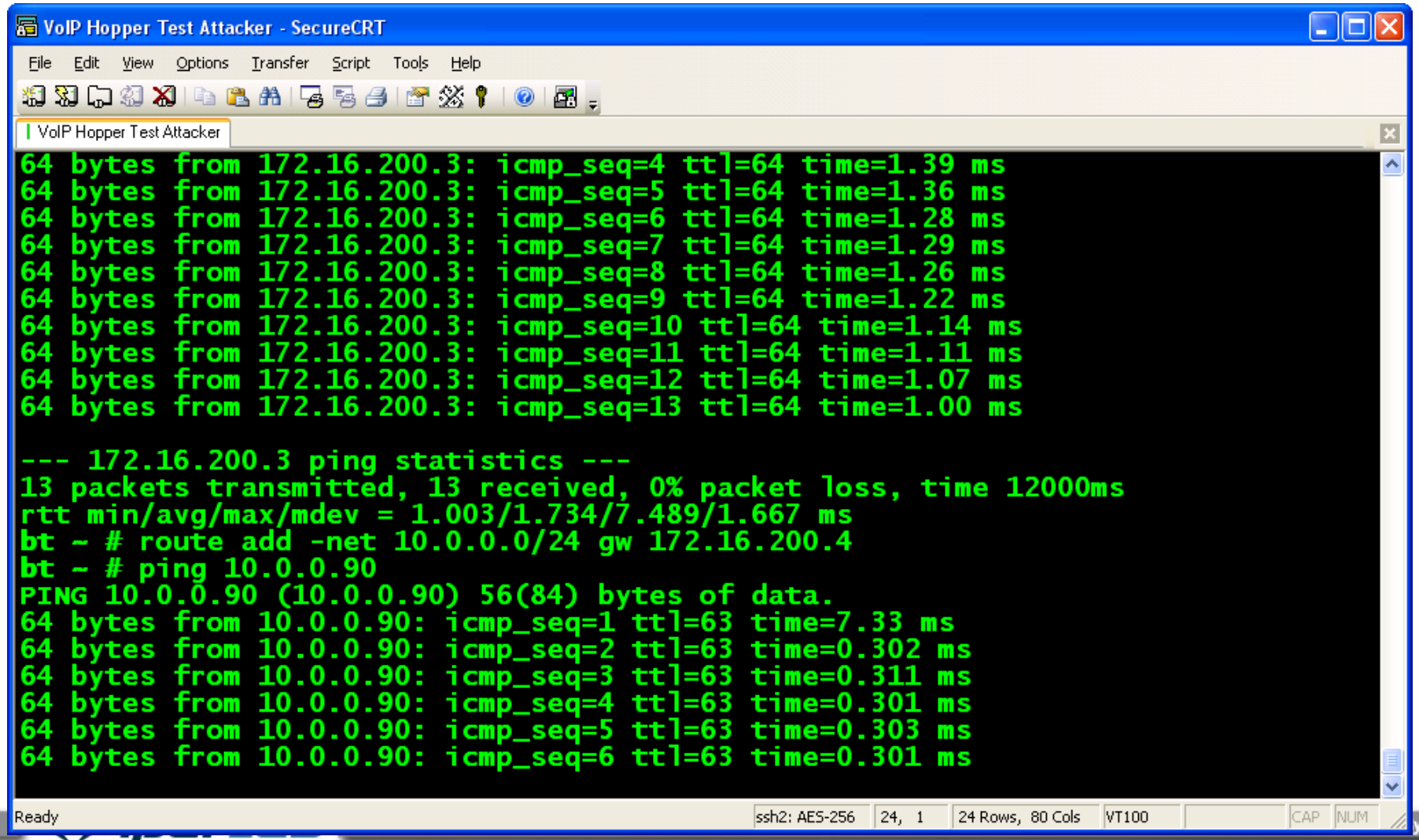
VoIP Hopper: Firewalled Voice Network



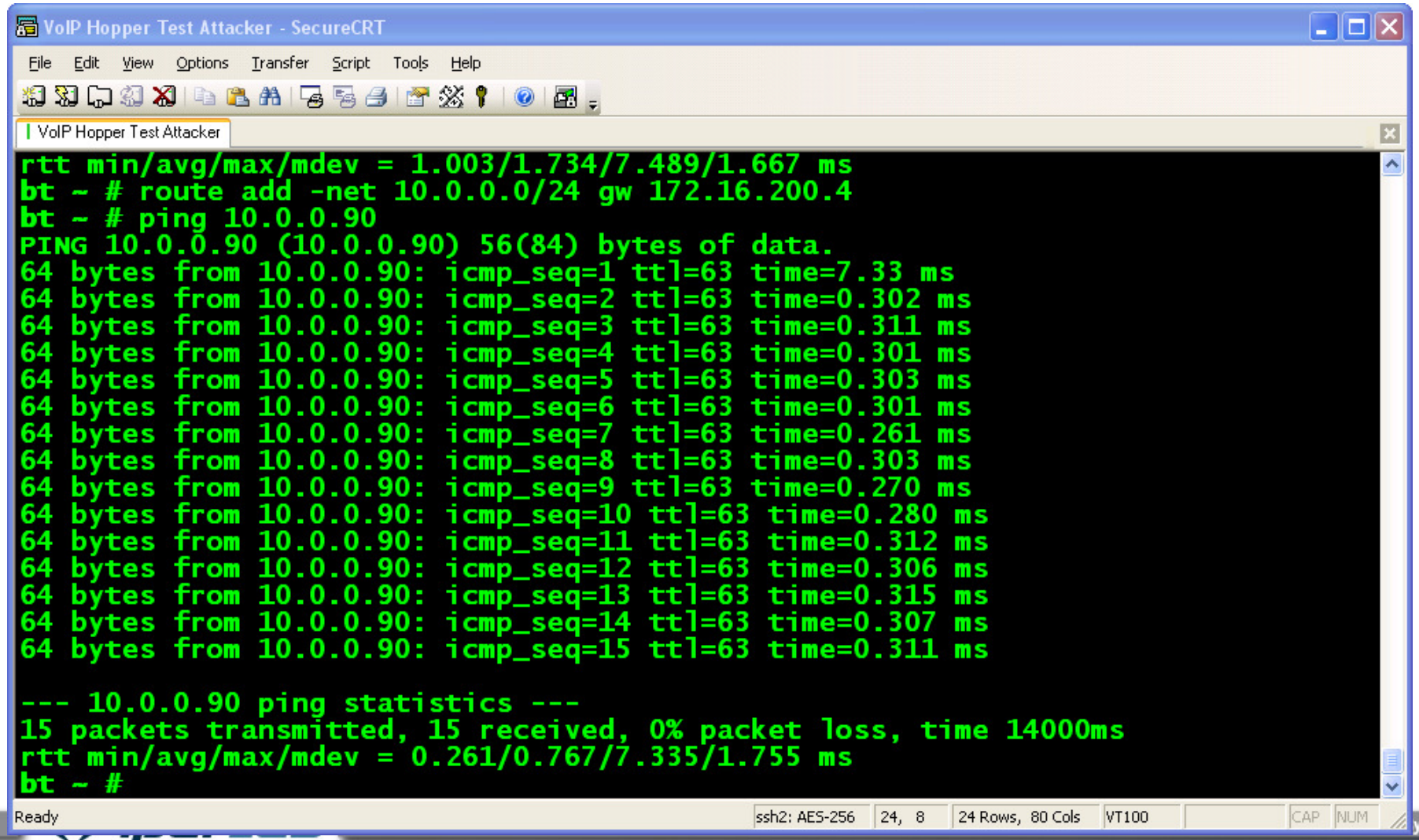
VoIP Hopper: Firewalled Voice Network



VoIP Hopper: Firewalled Voice Network



VoIP Hopper: Firewalled Voice Network



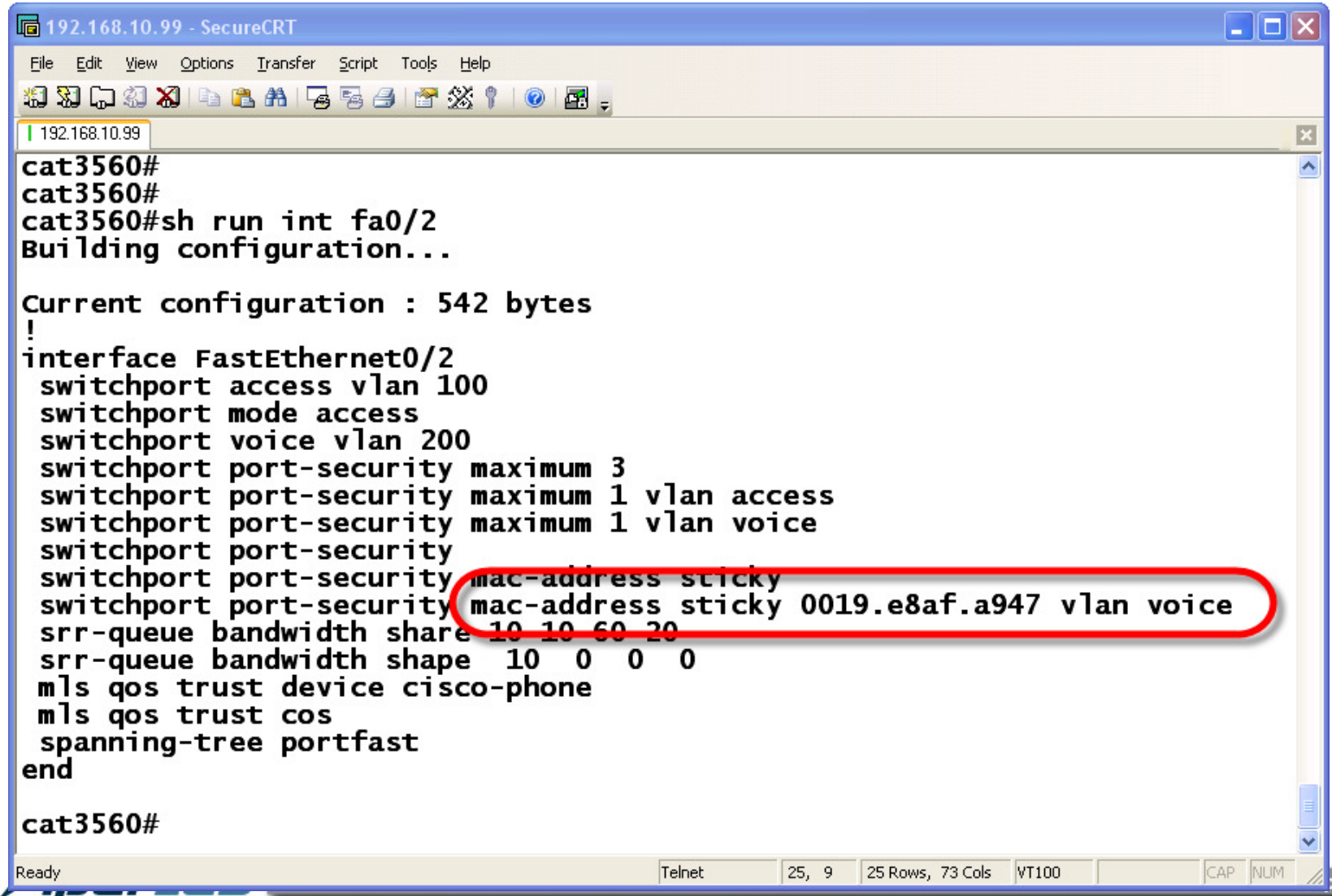
Case Study 1: Lessons learned

- **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

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

MAC Address Filtering



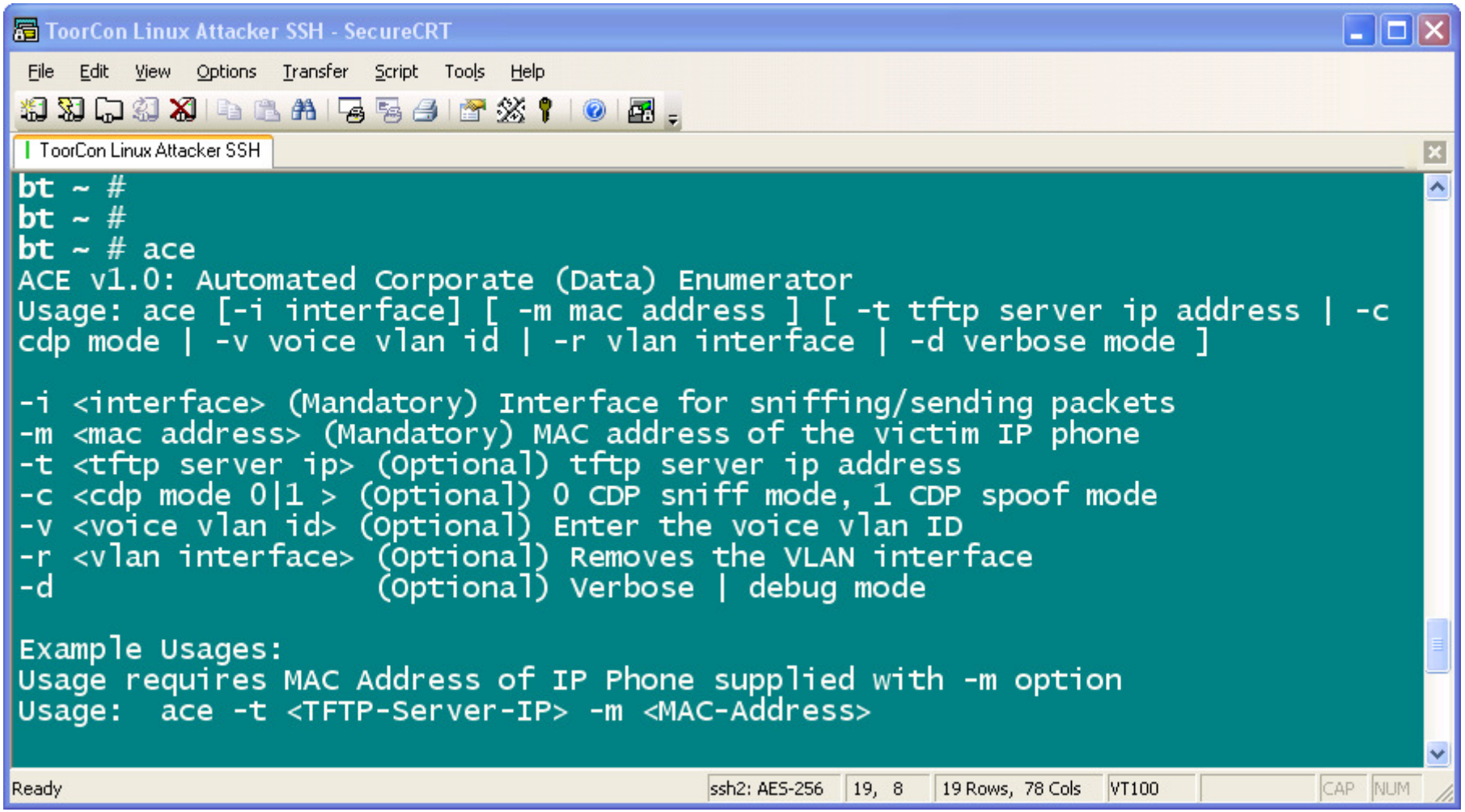
MAC Address Filtering

- **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

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

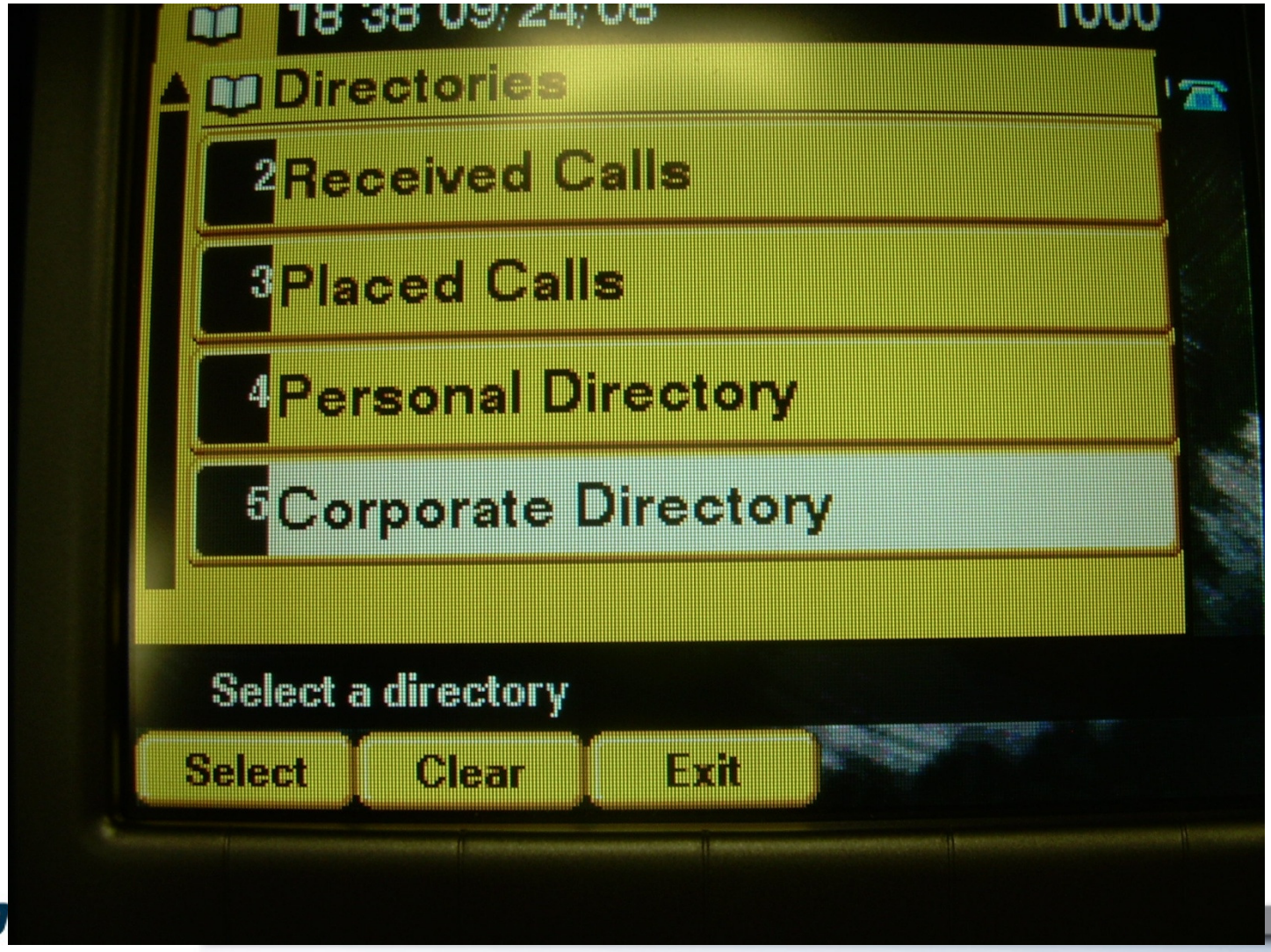
ACE Directory Tool



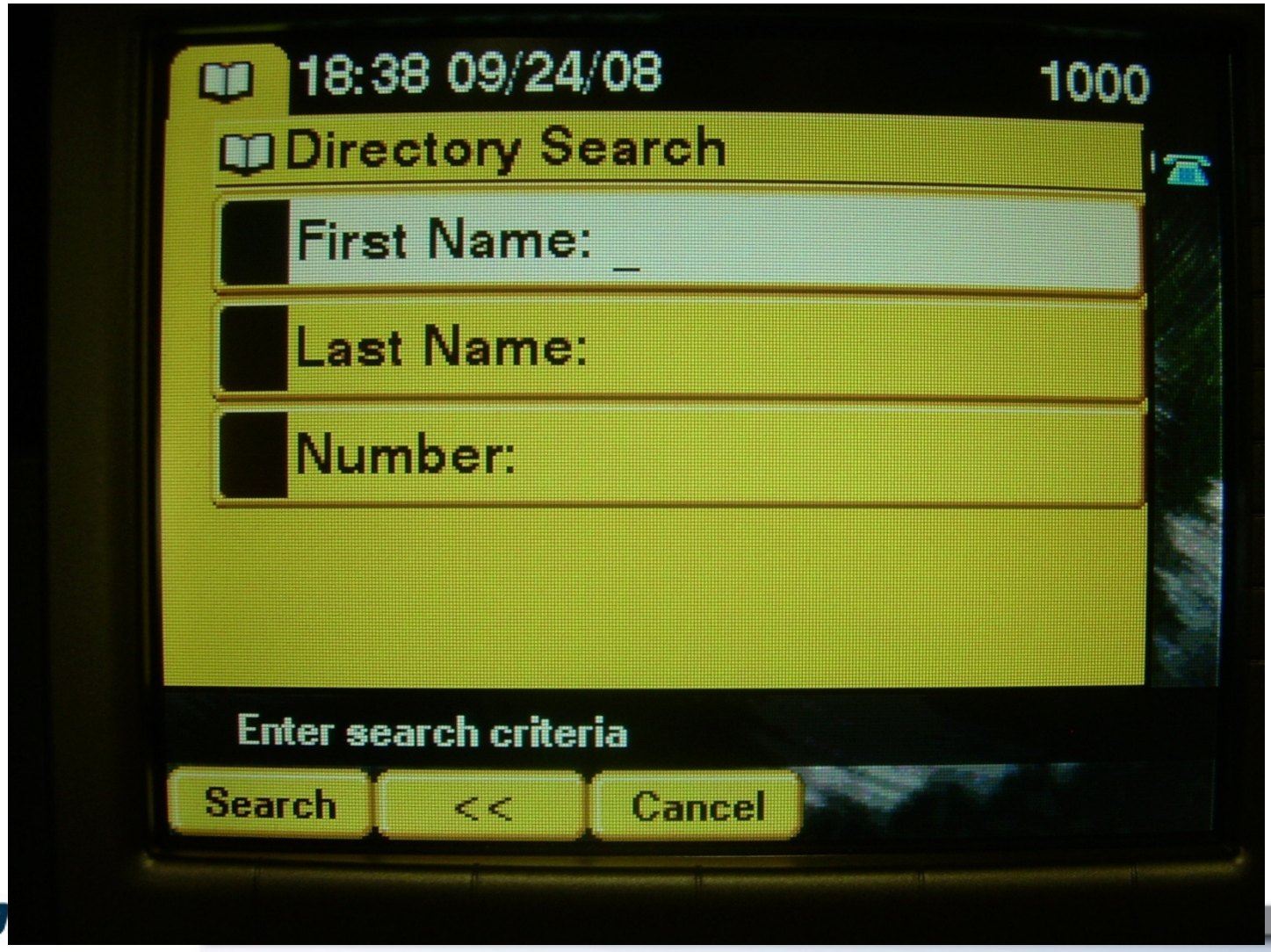
ACE Directory Tool

- **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**

LCD of Cisco IP Phone



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

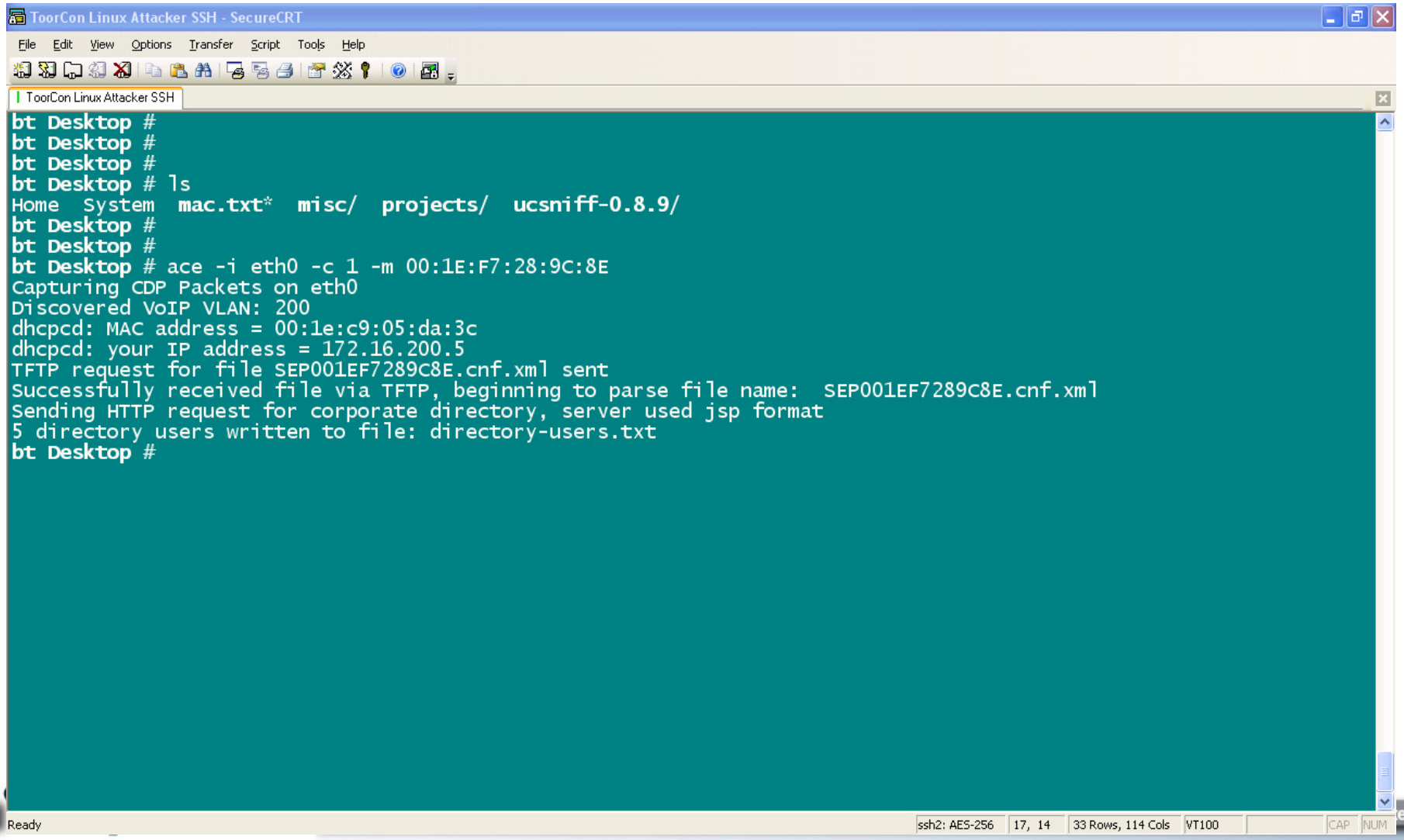


A user can dial by name

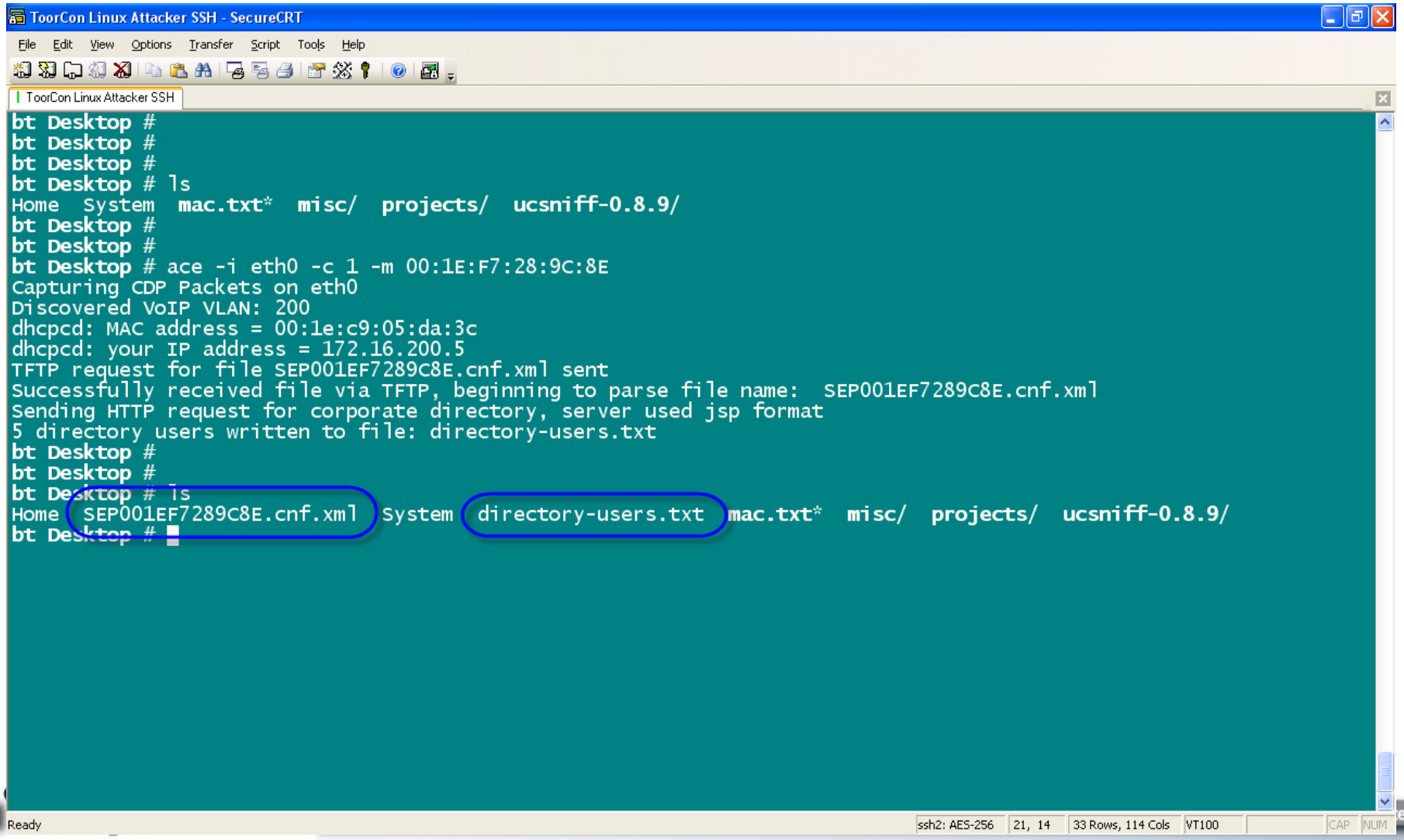
What ACE does

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

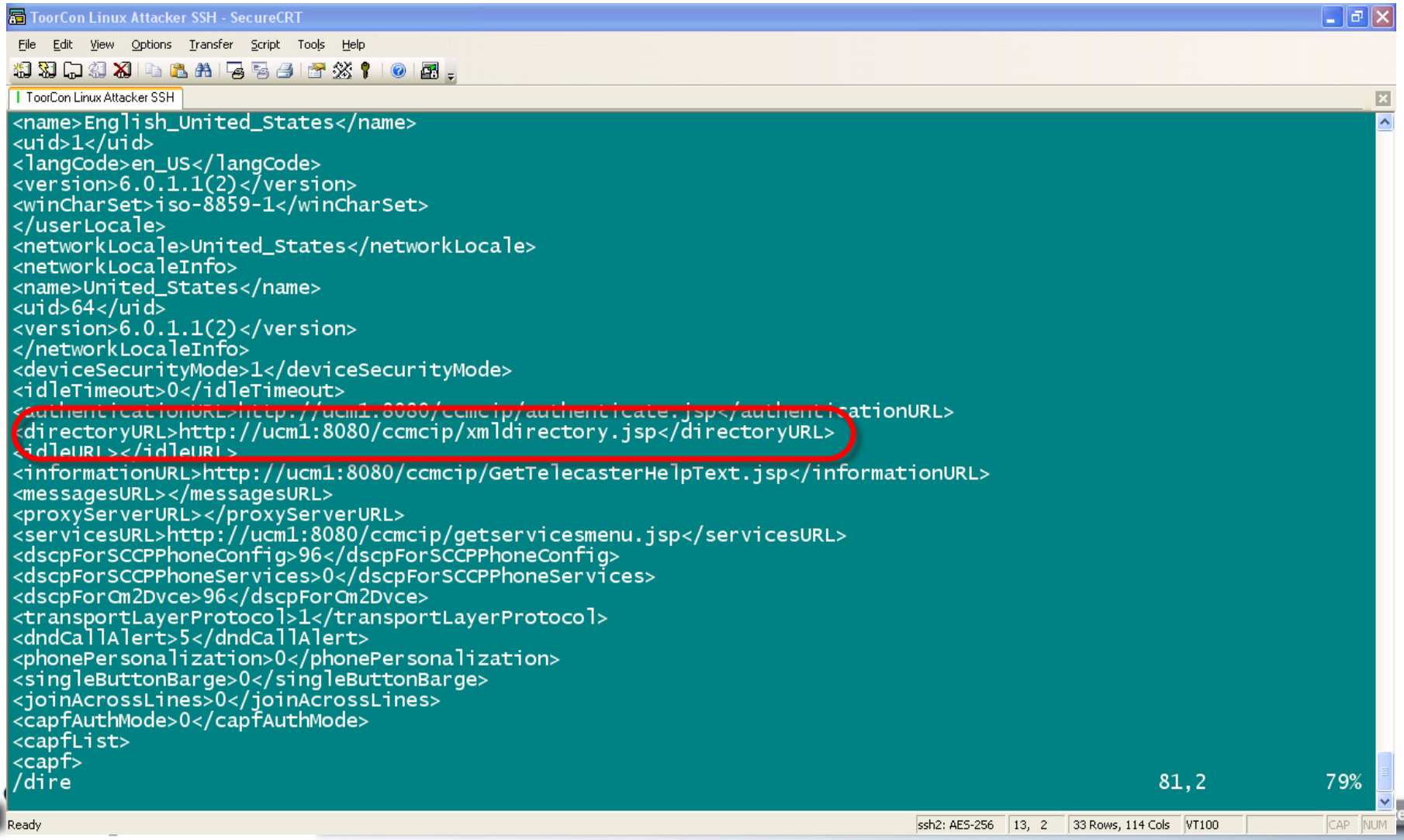
Running ACE



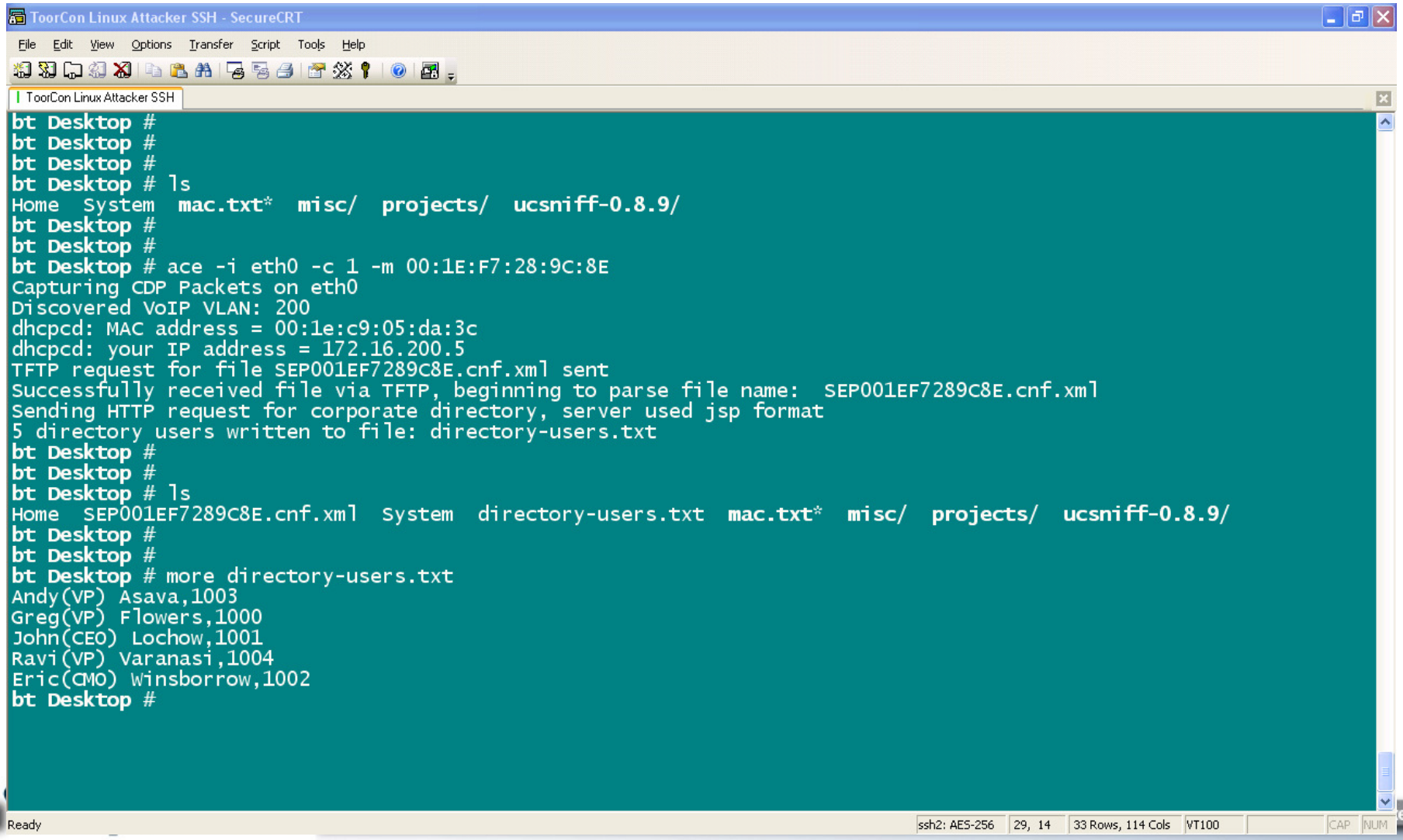
Downloaded Files



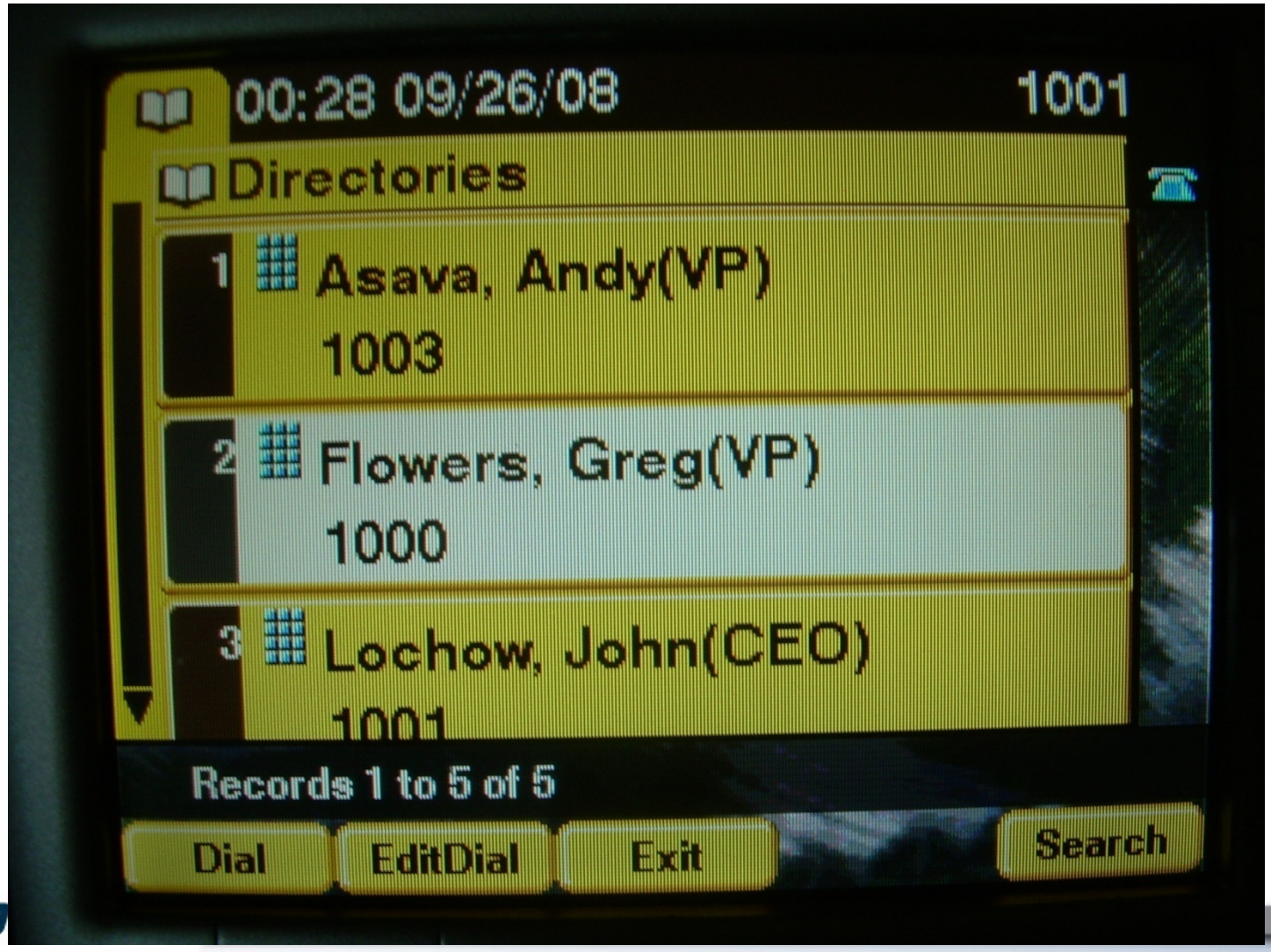
ACE Parsed XML File to get Directory URL



Directory Text File



ACE Output matches Phone Entries



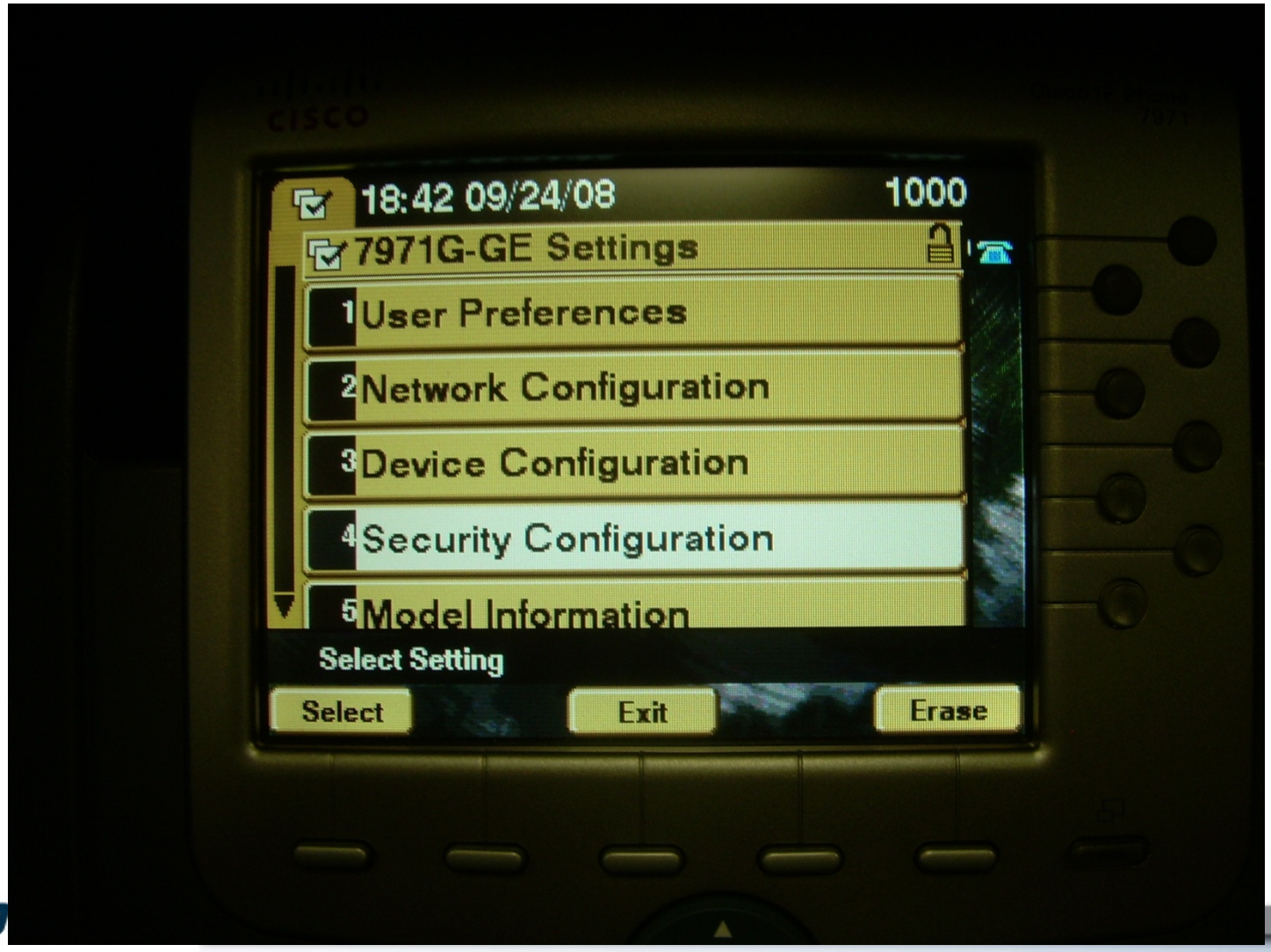
Impact

- 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 it's 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

802.1x and VoIP

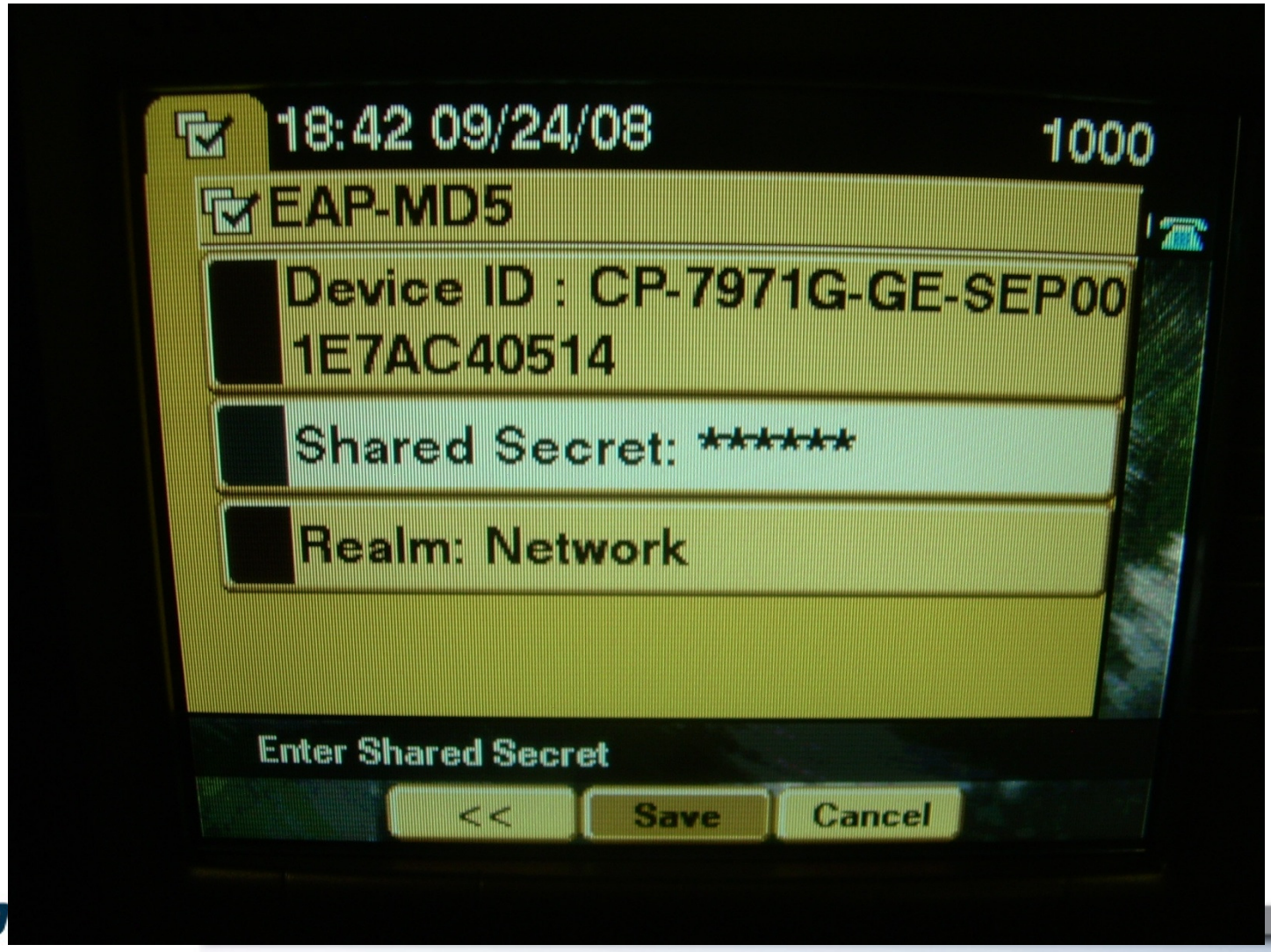
- **Wired 802.1x, to mitigate VLAN Hopping**
- **After an attacker gains access to physical voice port, another layer of security can be added in the form of Wired 802.1x.**
  - Designed to provide strong authentication from 802.1x supplicant in IP Phone sending username and password to Ethernet Switch.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

802.1x Supplicant support in IP Phones



Uses RFC 3847 EAP-MD5

User supplies password to supplicant in IP Phone



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.

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

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

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

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

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**

Technique 2

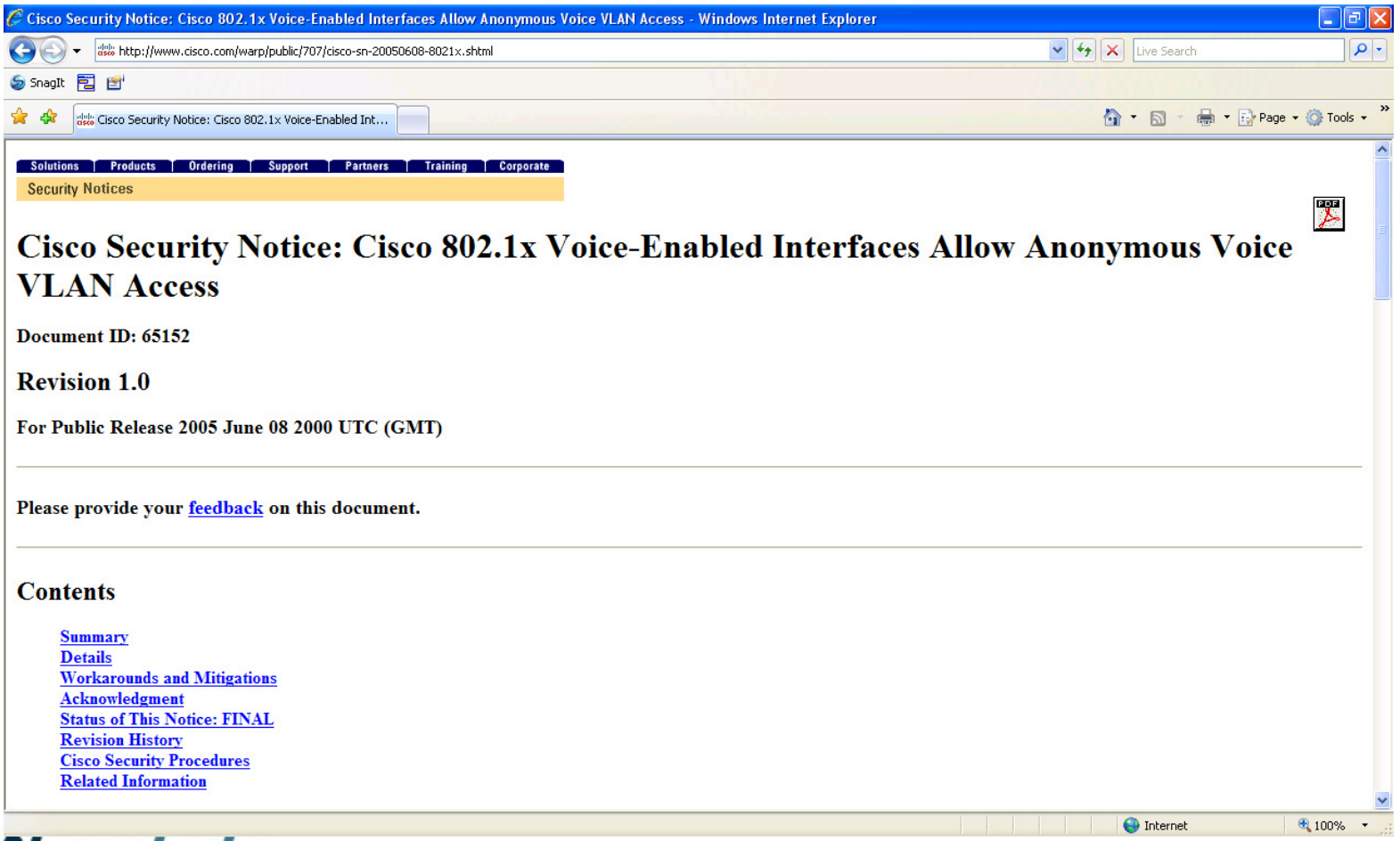
- **Share a hub with laptop and valid IP Phone**
  - Requires power supply for IP Phone, and network hub
- **Wait until the IP Phone boots up**
- **Take note of the IP Phone MAC address**
- **Disconnect the IP Phone**
- **Spoof the MAC Address of the IP Phone**
- **PC issues a DHCP client request**

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.**

Fishnet Security Discovered issue

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



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

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

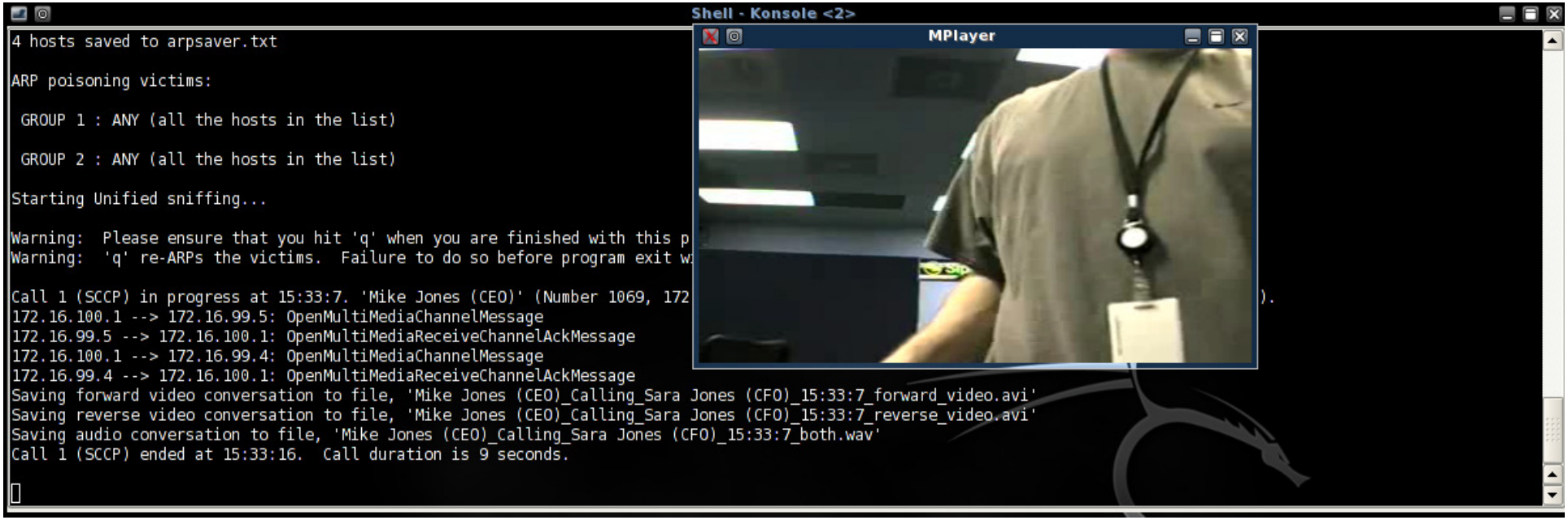
Eavesdropping technique #2

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

Eavesdropping technique #2

UCSniff VoIP Sniffer Live Demo

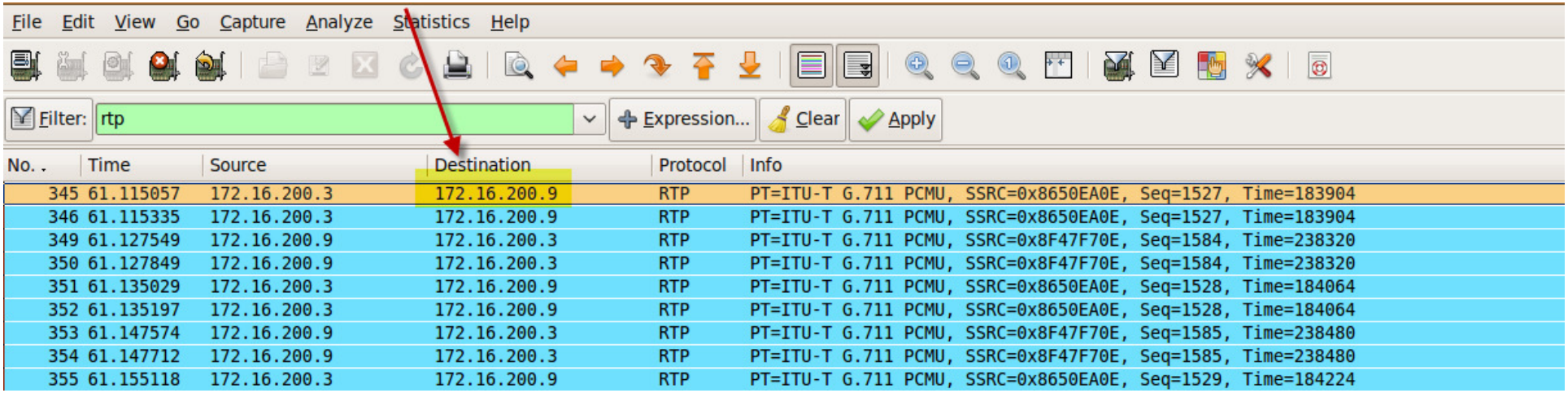


The Ultimate UCSniff Trick

- **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.**

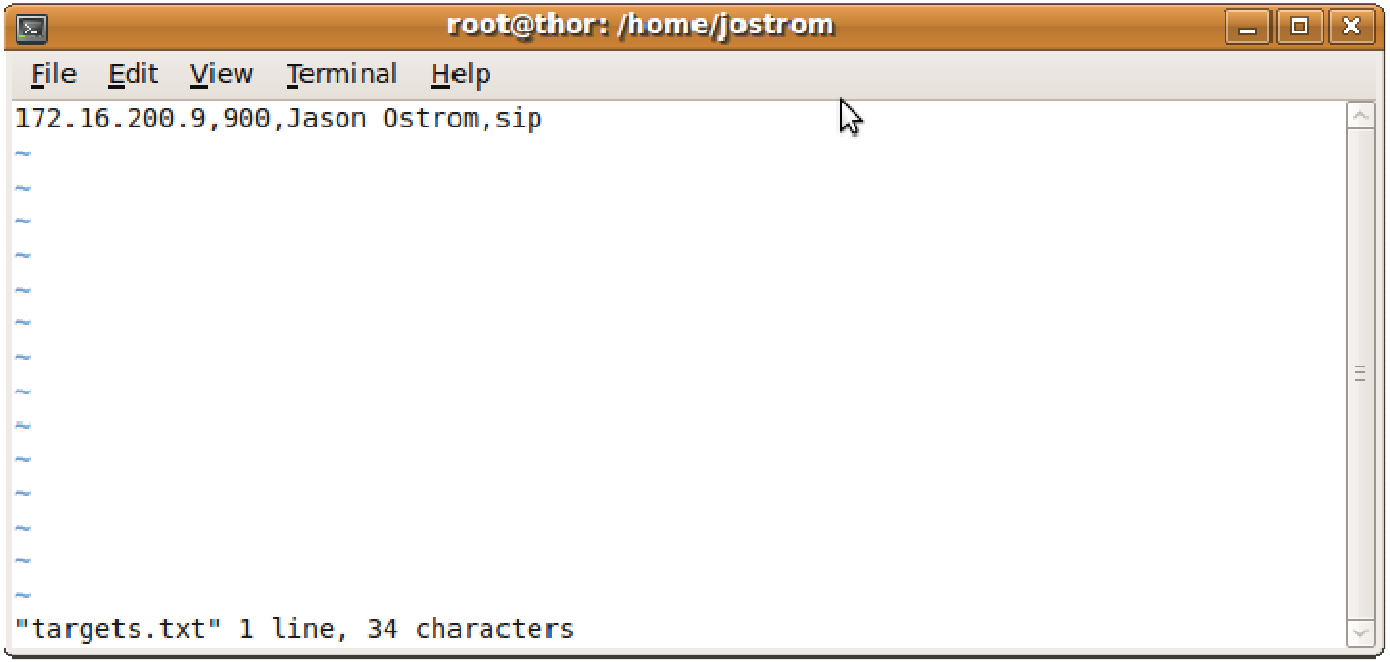
Find IP Address of remote IP Phone

- **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
  - Wirshark RTP filter will find IP address



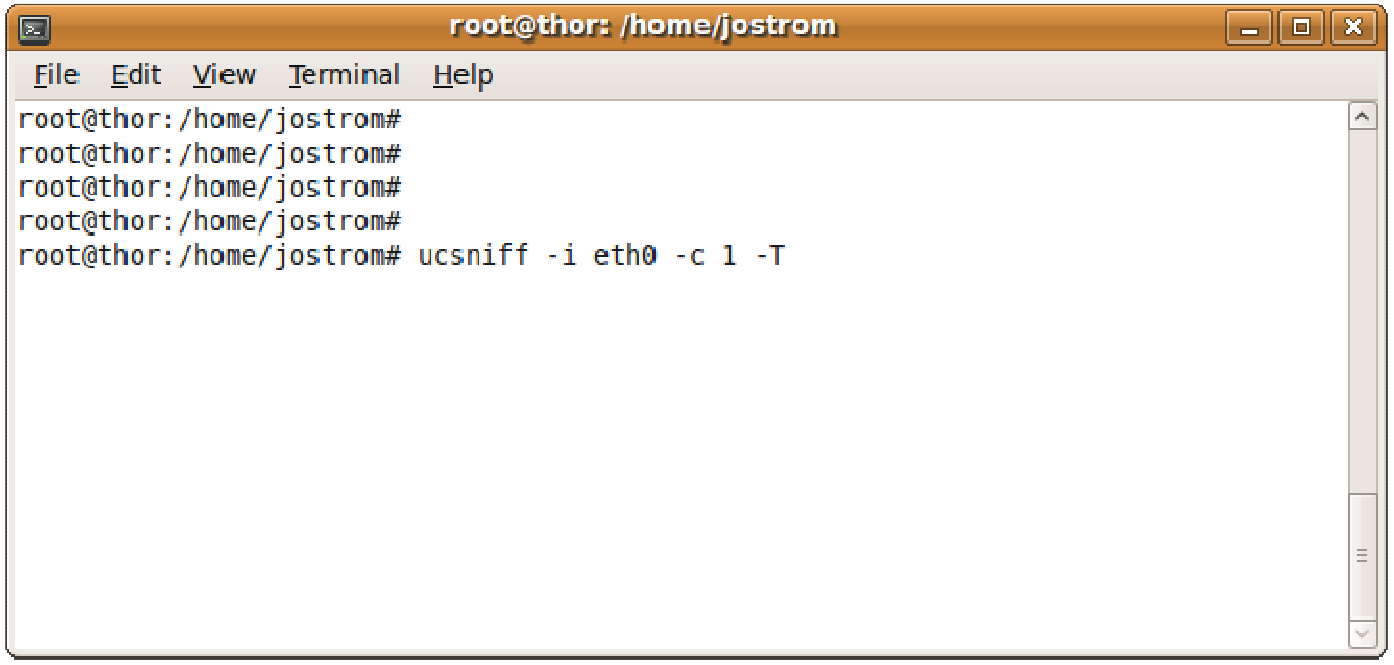
Create Targets Entry

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



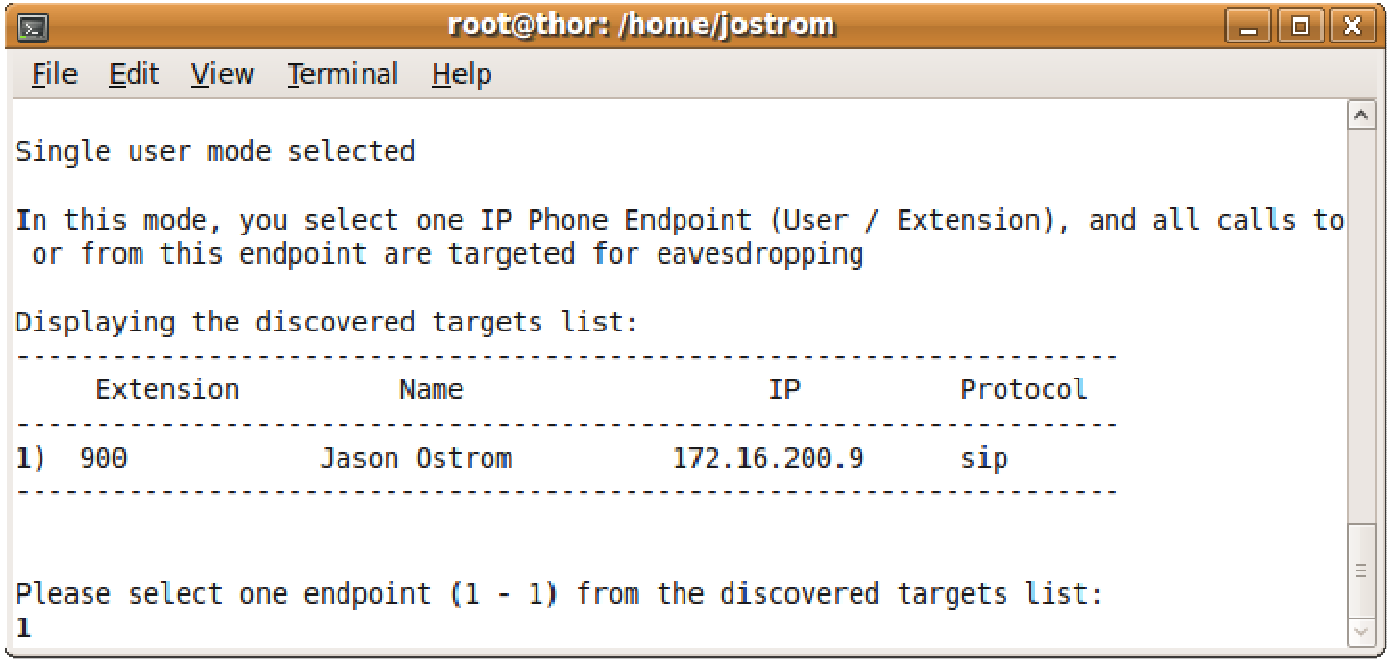
UCSniff Target Mode

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



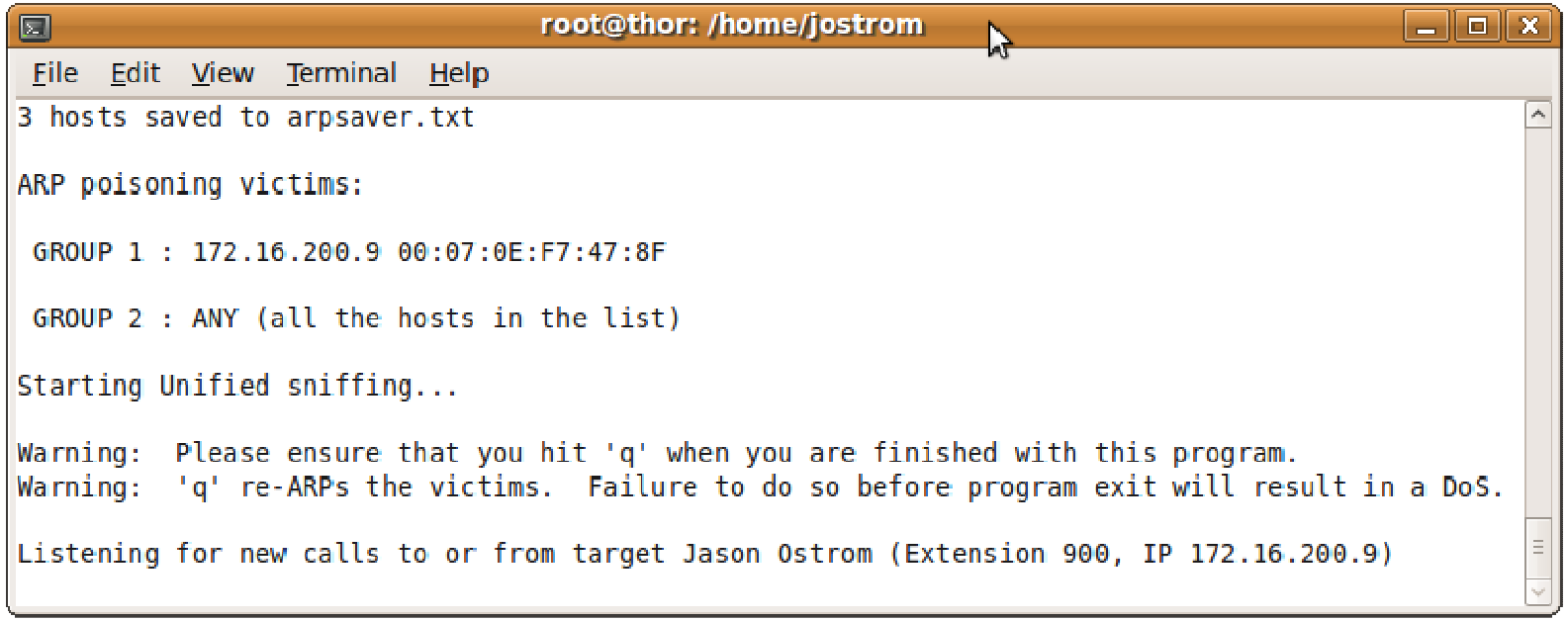
Select Targeted User

- **Select targeted user**



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



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

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

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.**

Agenda

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

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

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

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

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

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)

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

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)

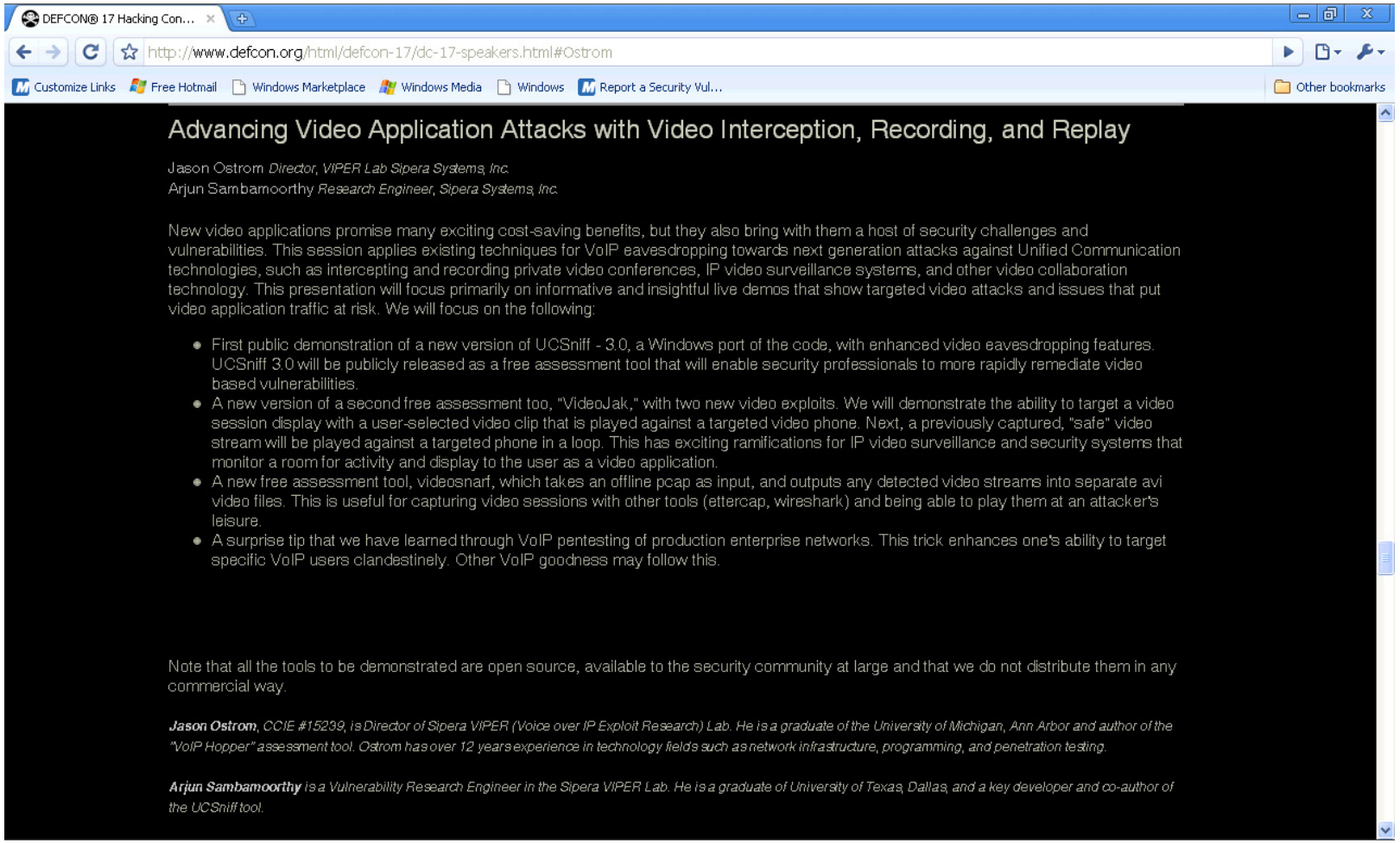
Agenda

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

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

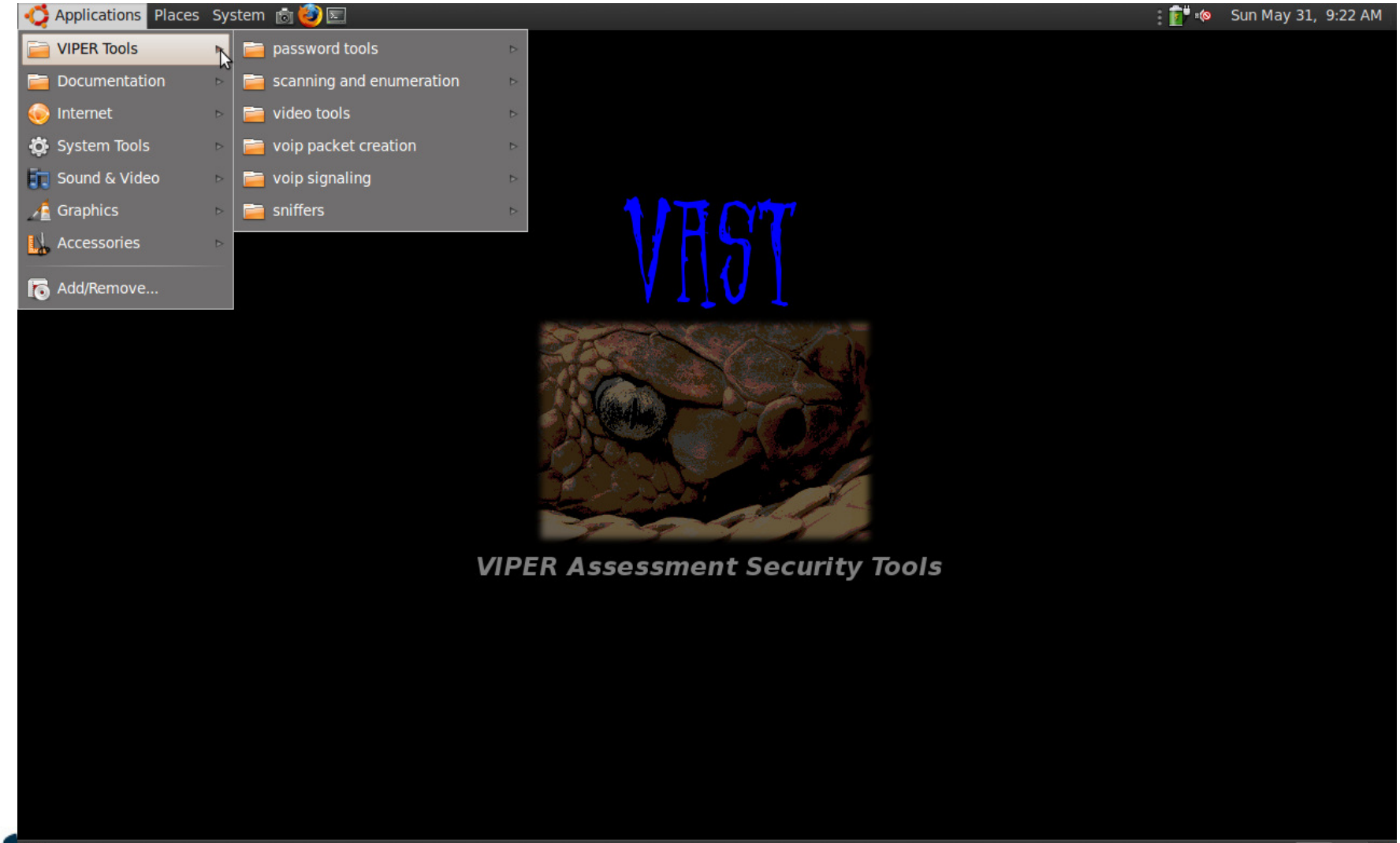
Future Research – DefCON 2009!



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**

VAST



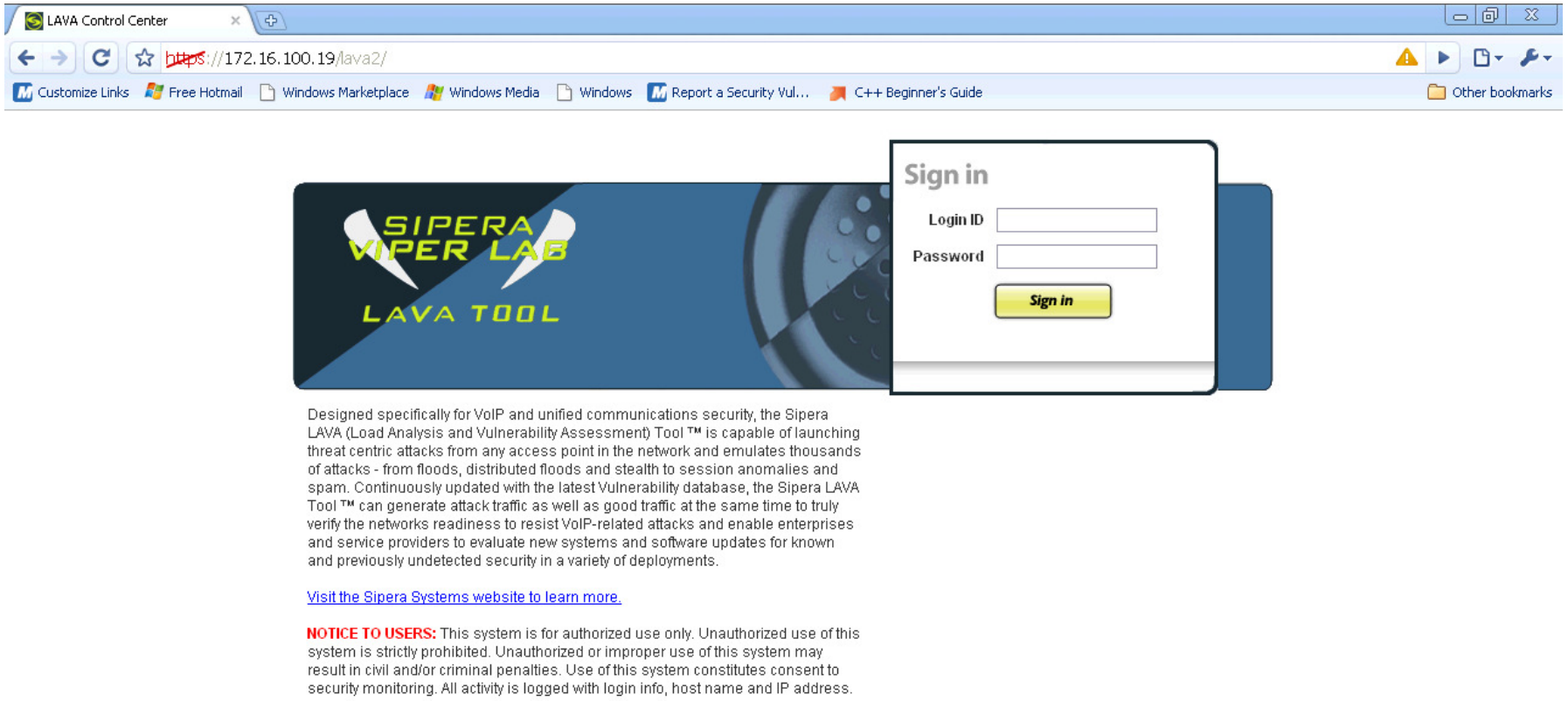
VAST

- 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.

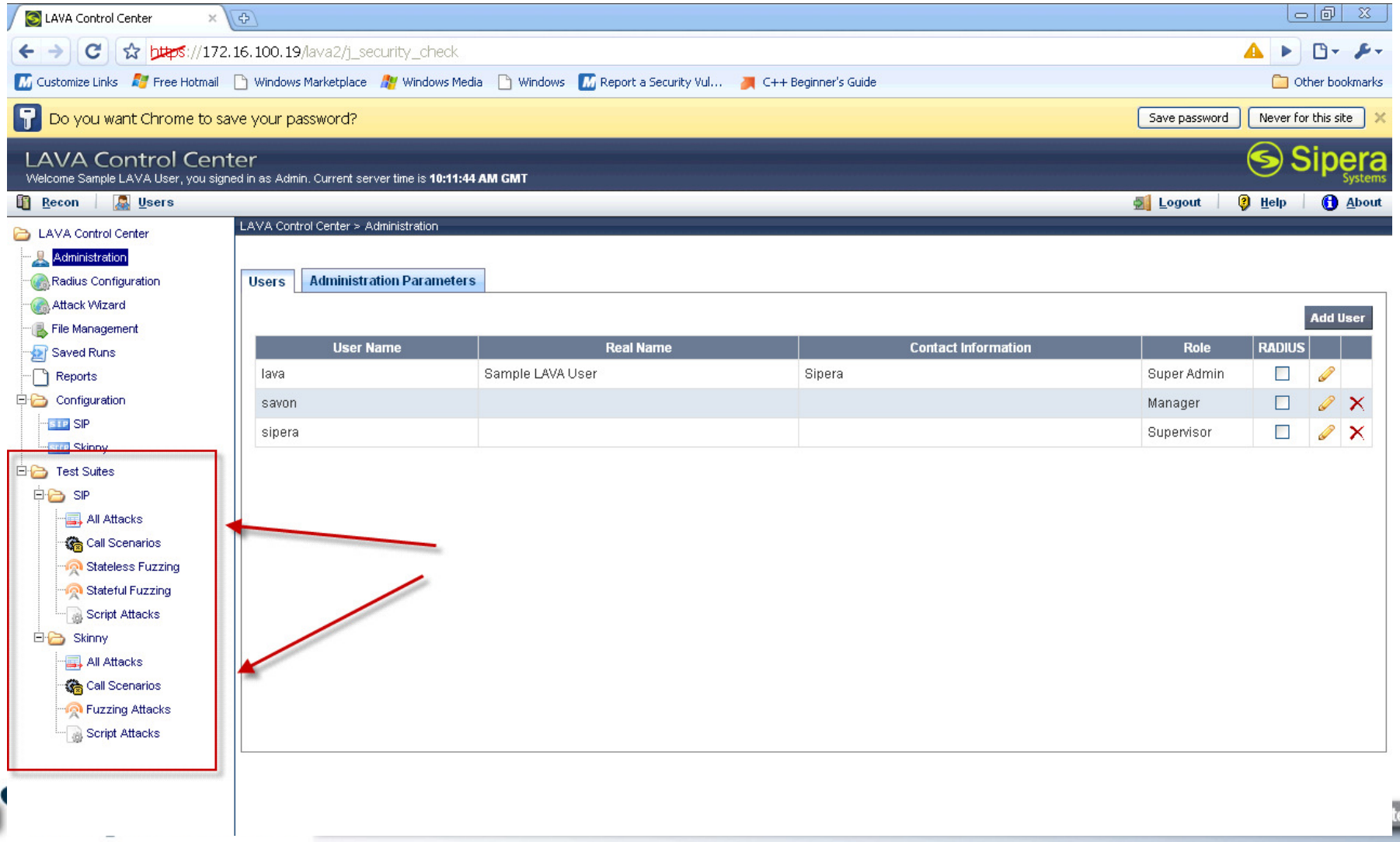
LAVA – What is LAVA?

- 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

LAVA



LAVA



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**