



# Ethical Hacking and Countermeasures

Version 6

## Module XXXVIII

### VoIP Hacking



[Home](#) [Subscriptions](#) [Blogs](#) [White Papers](#) [Tools & Training](#)

JUMP TO PRIORITY:

Choose your priority 

## :: Network Sentry ::

Securing your data and network, inside and outside the perimeter

### VoIP Security Still Falling Short

Posted by Carl Weinschenk on January 18, 2008 at 6:18 pm

It may be a bit late in the month to still be posting “year ahead”-type stories, but the content of this [Help Net Security piece](#) on the security threats facing VoIP makes it worthwhile. The bottom line of this commentary is that VoIP security is not yet where it should be.

The piece, which is based on findings from Siper’s VIPER group, says that the deployment of unified communications (UC) and Session Initiation Protocol (SIP) trunking will accelerate the number of denial-of-service and distributed denial-of-service (DoS and DDoS) attacks during the coming year. (The Korea Information Security Agency [predicts a proliferation of DDoS attacks](#), according to the [Korea IT Daily](#).)

The second category of attacks to watch is eavesdropping. Thirdly — and this seems like a particularly grievous threat — Microsoft Office Communications Server (OCS) 2007 will be the unwitting staging ground for the creation and launch of botnets.

The story adds that hackers will set up their own IP PBXes for VoIP phishing (vishing) and related attacks. Finally, access through Subscriber Identity Modules (SIMs) will facilitate attacks on service providers.

Source: <http://www.itbusinessedge.com/>

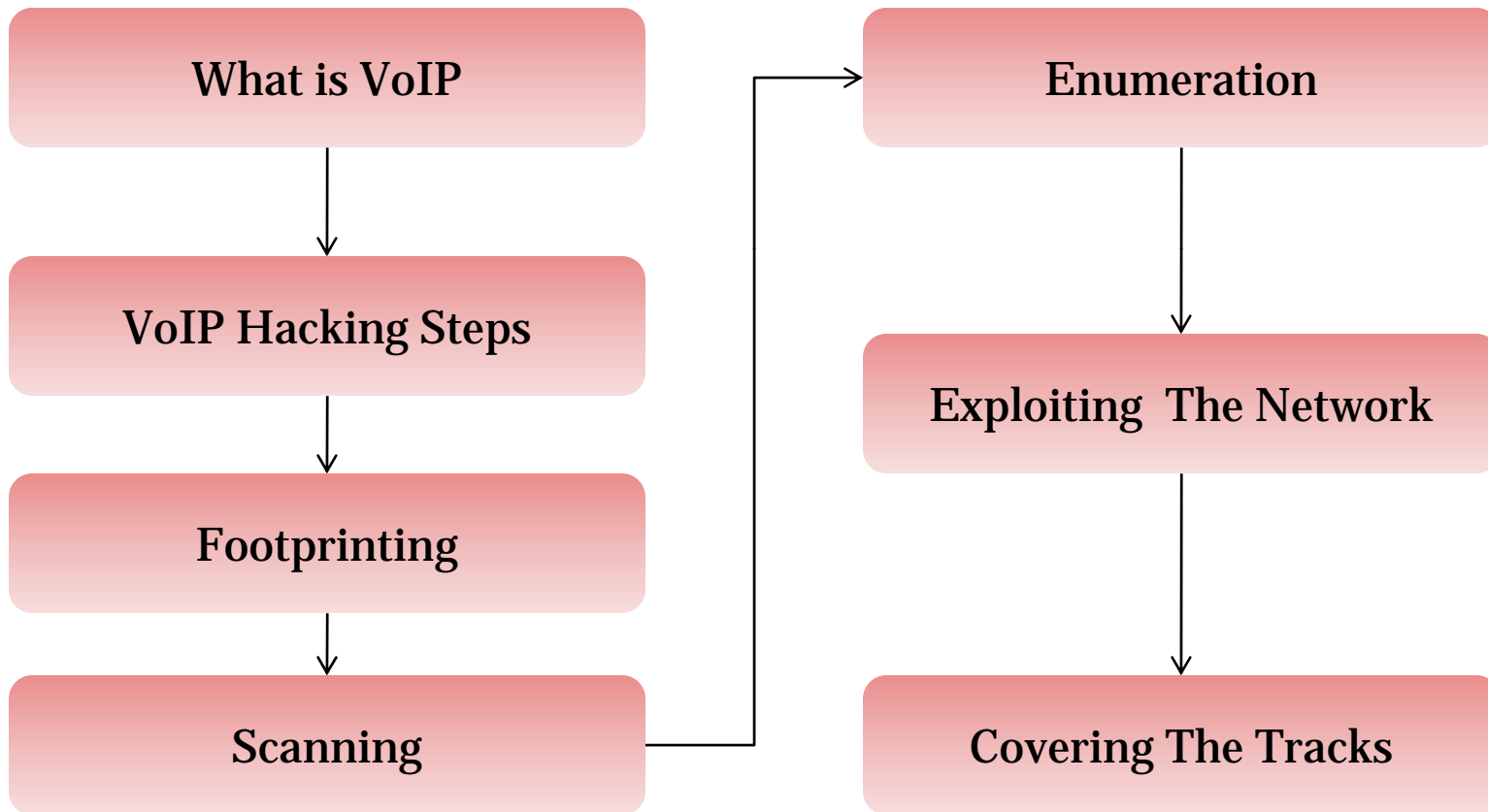
# Module Objective

This module will familiarize you with:

- VoIP
- VoIP Hacking Steps
- Footprinting
- Scanning
- Enumeration
- Exploiting The Network
- Covering The Tracks



# Module Flow



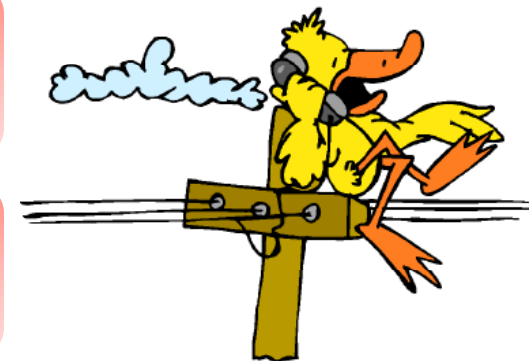
Voice Over Internet Protocol (VoIP) refers to transmission of voice over IP based networks

Also known as “packet telephony”

Uses IP protocol to route voice traffic

Voice is compressed using CODECS-hence bandwidth is utilized efficiently

Renowned for its low cost and advantageous to customers in case of long distance calls





# VoIP Hacking Steps

# VoIP Hacking Steps

Footprinting



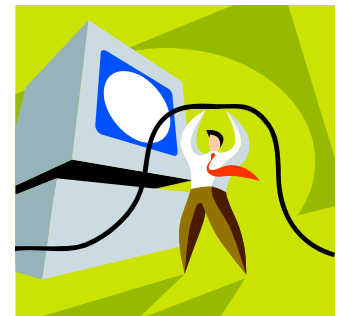
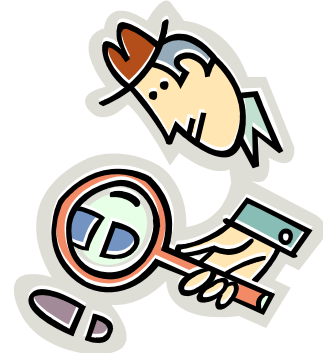
Scanning



Enumeration



Exploiting the Network





# Footprinting



Public Web site research

Google hacking

WHOIS and DNS analysis



# Unearthing Information

## Information includes:

Organizational structure and corporate locations

Help and tech support

Job listings

Domain name lookup

Phone numbers and extensions

VoIP vendor press releases and case studies

Resumes

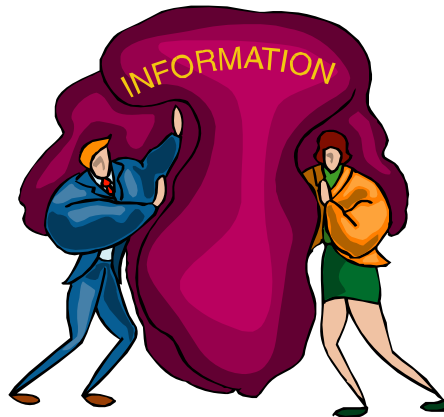
Mailing lists and local user group postings

Web-based VoIP logins

# Organizational Structure and Corporate Locations

Hacker can guess names of employees working in an organization

Check for the location information for branch offices and corporate headquarters to know the traffic flow between two VoIP call participants



Check the sites that hold information from the help desks:

- Phone type
- Default PIN numbers for voicemail
- Links to web administration



Corporate web sites open up Job listings that include the information on the technologies used within an organization



# Phone Numbers and Extensions

Identify internal workings numbers and extensions



VoIP vendor sites consists of case studies that gives you a detailed information about products and versions and so on



## Resumes provide information such as:

- Designed and set up a sophisticated SIP-based VoIP production Asterisk PBX with headsets and X-Lite softphones
- "Provided security consulting, VPN setup, and VoIP assistance including CallManager installation with Cisco 7920 IP Phones"





# WHOIS and DNS Analysis

DNS is the distributed database system used to map IP addresses to hostnames

Every organization with an online presence relies on DNS in order to route website visitors and external email to the correct places

WHOIS search reveals the IP address ranges that an organization owns

Based on this information, hackers can determine which servers are running DNS and SMTP services

# Steps to Perform Footprinting

Find companies' external and internal URLs

Perform whois lookup for personal details

Extract DNS information

Mirror the entire website and look up names

Extract archives of the website

Google search for company's news and press releases

Use people search for personal information of employees

Analyze company's infrastructure details from job postings





# Scanning

# Host/Device Discovery

First step of scanning is to collect an active target list and figure out what devices are accessible on the network

Ping large number of IP addresses and check for any responses

Methods to ping IP addresses:

ICMP ping sweeps

ARP pings

TCP ping scans

SNMP sweeps



# ICMP Ping Sweeps

Easy way to identify active hosts by sending ICMP ECHO REQUEST packets

Send ICMP ECHO REPLAY packets if ICMP is unblocked by firewalls

## Tools for ICMP Ping Sweeps:

- fping
- Nmap
- super scan
- Nessus
- Ping and port sweep utility



# ARP Pings

ARP ping requests MAC address through a large range of IP addresses

It identifies live hosts on the network

## Tools:

- Arping
- MAC address discovery tool



# TCP Ping Scans

Sends TCP SYN or ACK flagged packets to TCP port on the target host

RST packet that comes as a response indicate that a host is alive

## Tools:

- Nmap
- hping2



Scan to return sensitive information because the default “public” community string is always used

Tools:

SNS Scan

snmpwalk

Nomad

Cheops

snmpenum

snmp-audit





# Port Scanning and Service Discovery

Technique of connecting TCP and UDP ports on target to search for active services

Determines the vulnerabilities present on the target host or devices

Method to scan active services:

- TCP Scan
- UDP scan



# TCP SYN Scan



Sends a TCP SYN packet to a specific port to establish a TCP connection

A returned SYN/ACK-flagged TCP packet indicates the port is open

RTP packet indicates a closed packet

Sends an empty UDP header to each UDP port on the target

If it responds, it indicates an active service is listening

It is unused, if you get an ICMP port unreachable error



# Host/Device Identification

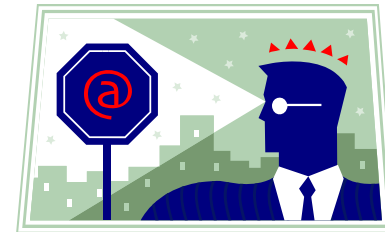
Determines the type of devices, hosts by OS and firmware types

## Method to identify the host/device:

- Stack Fingerprinting:
  - A technique for further identifying the innards of a target host or device

## Tools used to identify host or devices

- Nmap
- Xprobe2
- Arkin
- Queso
- Snacktime





# Enumeration

# Steps to Perform Enumeration

1

- Extract user names using win 2k enumeration

2

- Gather information from the host using null sessions

3

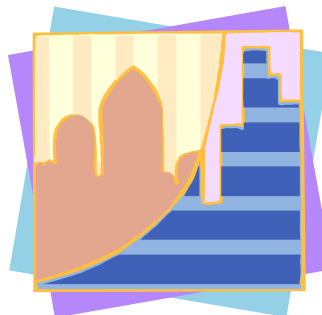
- Perform Windows enumeration using the tool Super Scan4

4

- Get the users' account using the tool GetAcct

5

- Perform an SNMP port scan using the tool SNScan V1.05



# Banner Grabbing with Netcat

Banner grabbing is a method where a port is connected to remote target to gather information of associated services running on it

It is the first step implicated in enumerating VoIP network

## Types of banner grabbing:

- Manual Banner grabbing
  - It can be accomplished easily using command-line tool NETCAT
- Automated Banner grabbing
  - In this type, fingerprinting tool SMAP analyzes SIP message response to determine the device it is probing



# SIP User/Extension Enumeration

Provides some valid username or extensions of SIP phones

Easy way to glean user registration

## Methods of Enumeration:

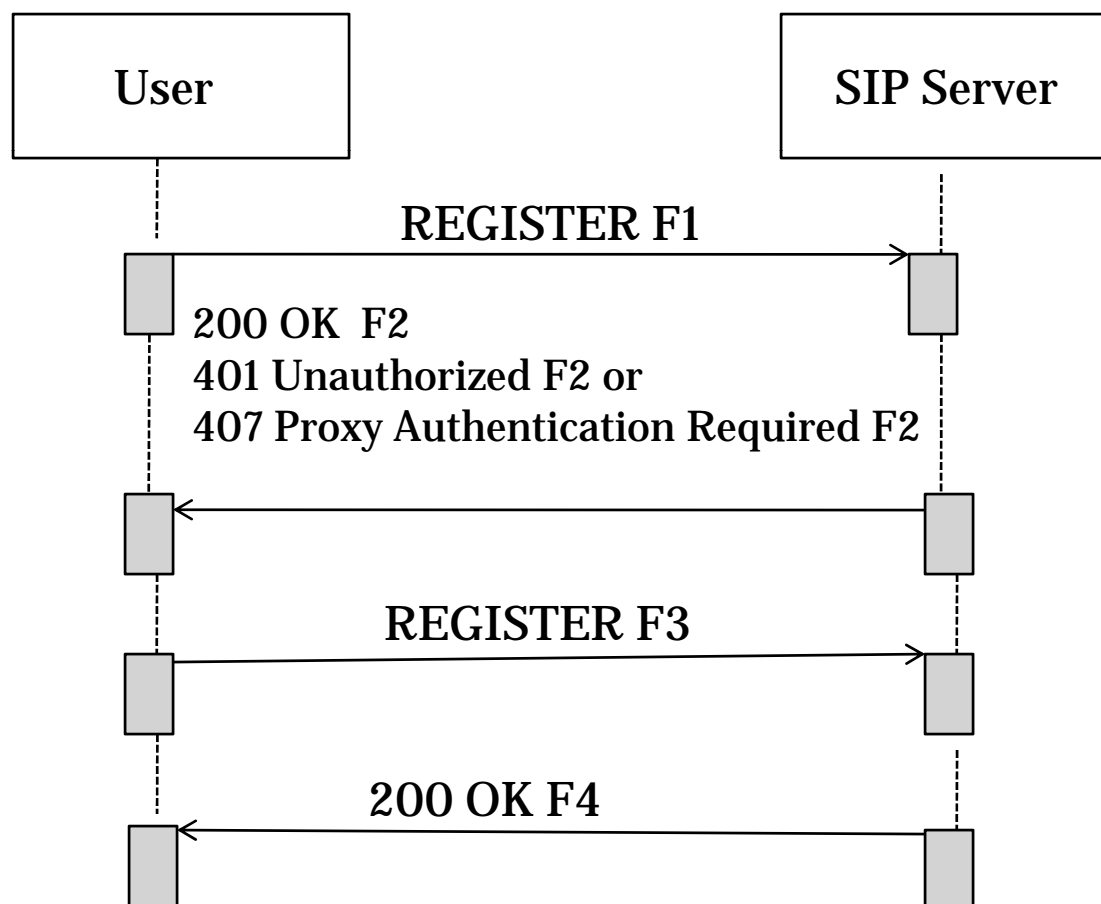
- REGISTER Username Enumeration
- INVITE Username Enumeration
- OPTIONS Username Enumeration
- Automated OPTIONS Scanning with sipsak
- Automated REGISTER, INVITE and OPTIONS Scanning with SIPSCAN Against SIP server
- Automated OPTIONS Scanning Using SIPSCAN Against SIP Phones





# REGISTER Username Enumeration

SIP REGISTER call flow from phone to registration servers



# INVITE Username Enumeration

INVITE Username Enumeration provides track back evidence as:

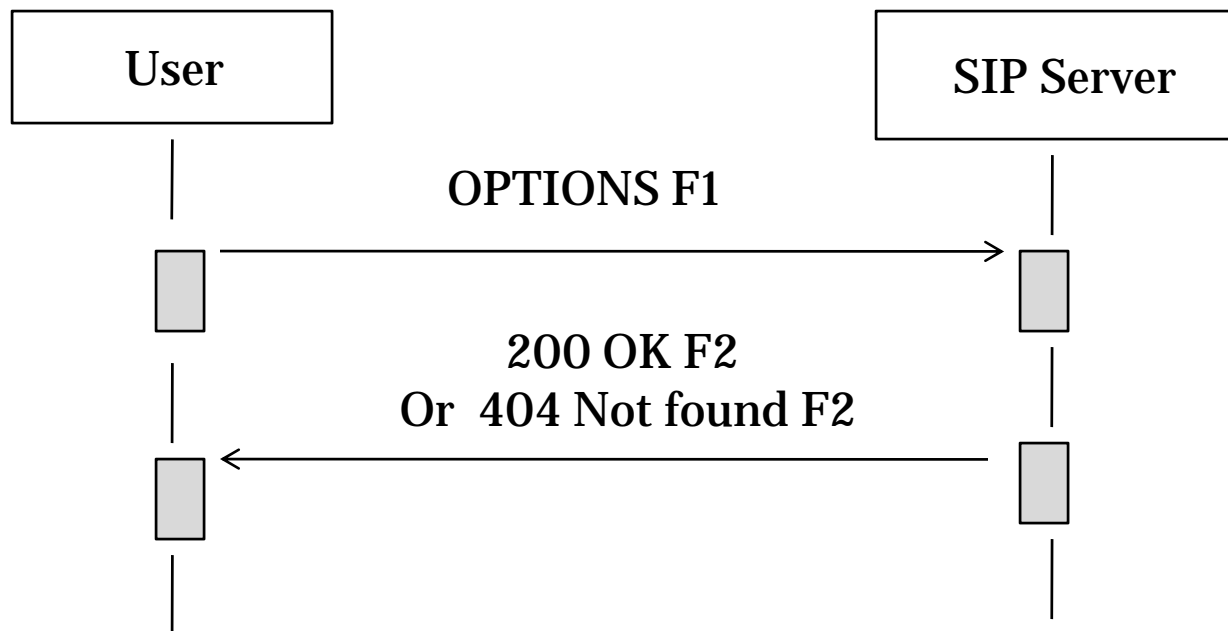
- It involves ringing the target's phone
- Missed calls logged on the phones and on SIP proxy



# OPTIONS Username Enumeration

A stealthy method for enumerating SIP users

It supports all SIP services and user agents



# Automated OPTIONS Scanning with sipsak



For OPTIONS scanning, command-line tool sipsak is used  
(<http://sipsak.org>)

It is useful in stress testing and  
diagnosing SIP service issues

# Automated REGISTER, INVITE and OPTIONS Scanning with SIPSCAN against SIP Server

Use SIPSCAN  
([www.hackingvoip.com](http://www.hackingvoip.com))

It returns the live SIP  
extensions/users



# Automated OPTIONS Scanning Using SIPSCAN against SIP Phones

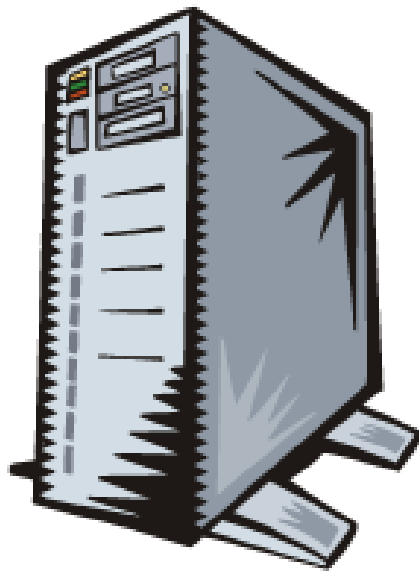
With this method, you can identify exact extension that the phone uses to log in to the SIP proxy or registrar



# Enumerating TFTP Servers

Locate the server within the network

It can be done by reading the TFTP server IP address from web-based configuration



# SNMP Enumeration

SNMP listens on UDP port 162

Use Nmap to find any devices that supports it

```
• root@domain2 ] # nmap -sU
```

Provides configuring information such as:

- Vendor type used
- Operating system
- Mac address
- Ports of UDP services



# Enumerating VxWorks VoIP Devices

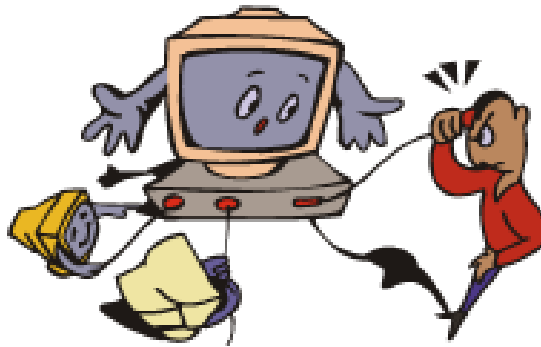
Many IP Phones are developed on VxWorks embedded operating system

Vendors forget to turn off the remote debugging feature that allows for administrative debugging access to the device

VxWorks debugger listens on UDP or TCP port 17185

It allows connection from remote debugging client

Visit [www.vxworks.com](http://www.vxworks.com)



# Exploiting The Network

# Steps to Exploit the Network

1

- Launch various attacks based on the vulnerability existing

2

- Compromise a network node

3

- Gain access to the network

4

- Now access the network and start sniffing

5

- Intercept through VoIP Signaling Manipulation to Insert Rogue Applications

# Denial-of-Service (DoS)

DoS attacks occurs when a large volume of packets are sent towards the victim's computer with or without involvement of the attacker directly

## Attack occurs:

- When data packets flood the target network from multiple external sources causing Distributed Denial-of-Service (DDoS) attack
- When devices within the internal network are targeted by a flood of packets causing Internal DoS Attack
- When viruses and worms in infected network systems generate false network traffic
- By infiltrating a hidden control program into network-attached computers

# Denial-of-Service (DoS) (cont'd)

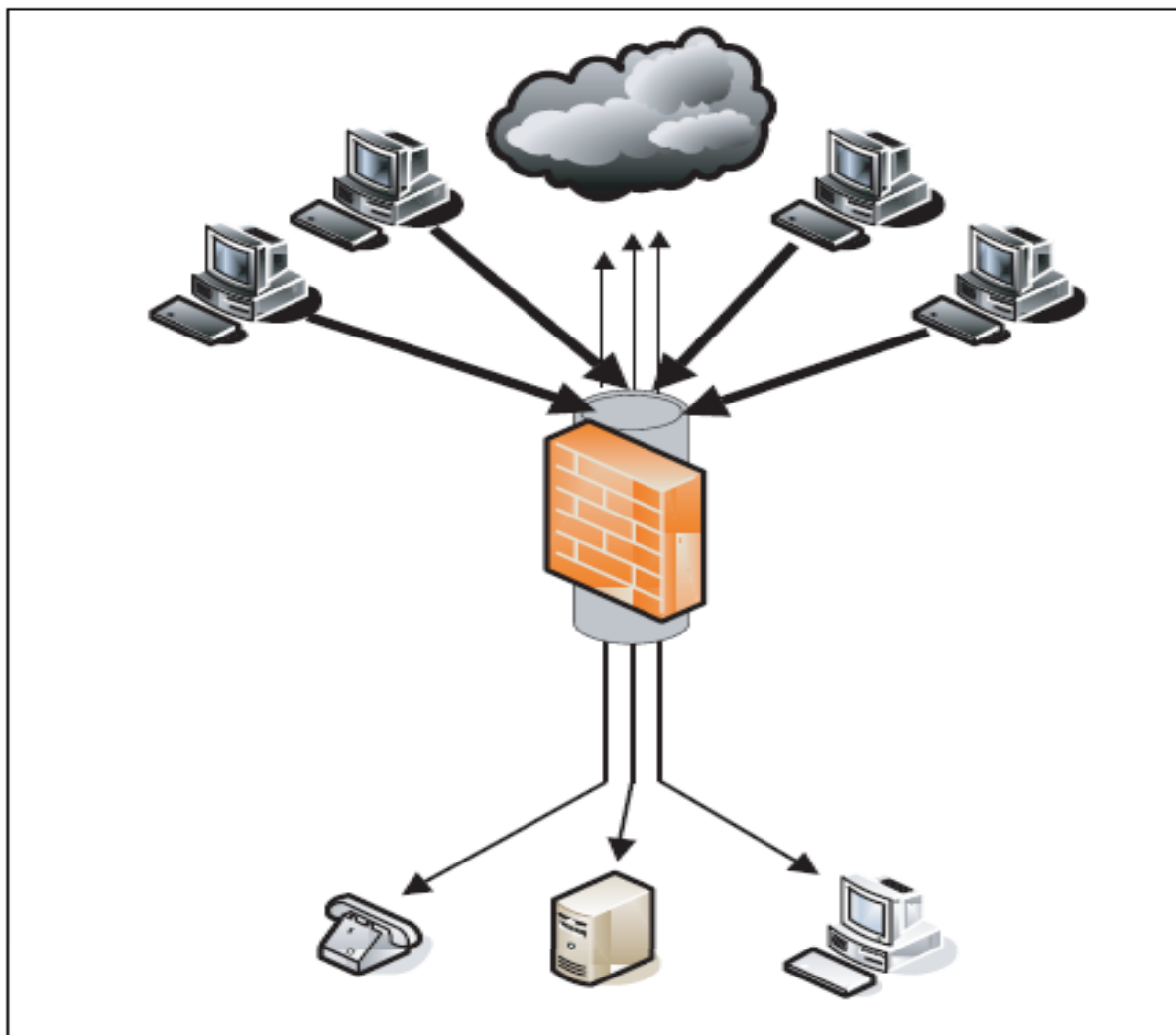
## Effects on VoIP

- Service degradation or disruption leads to resource depletion
- Bandwidth and CPU resource starvation

## It disrupts VoIP service by

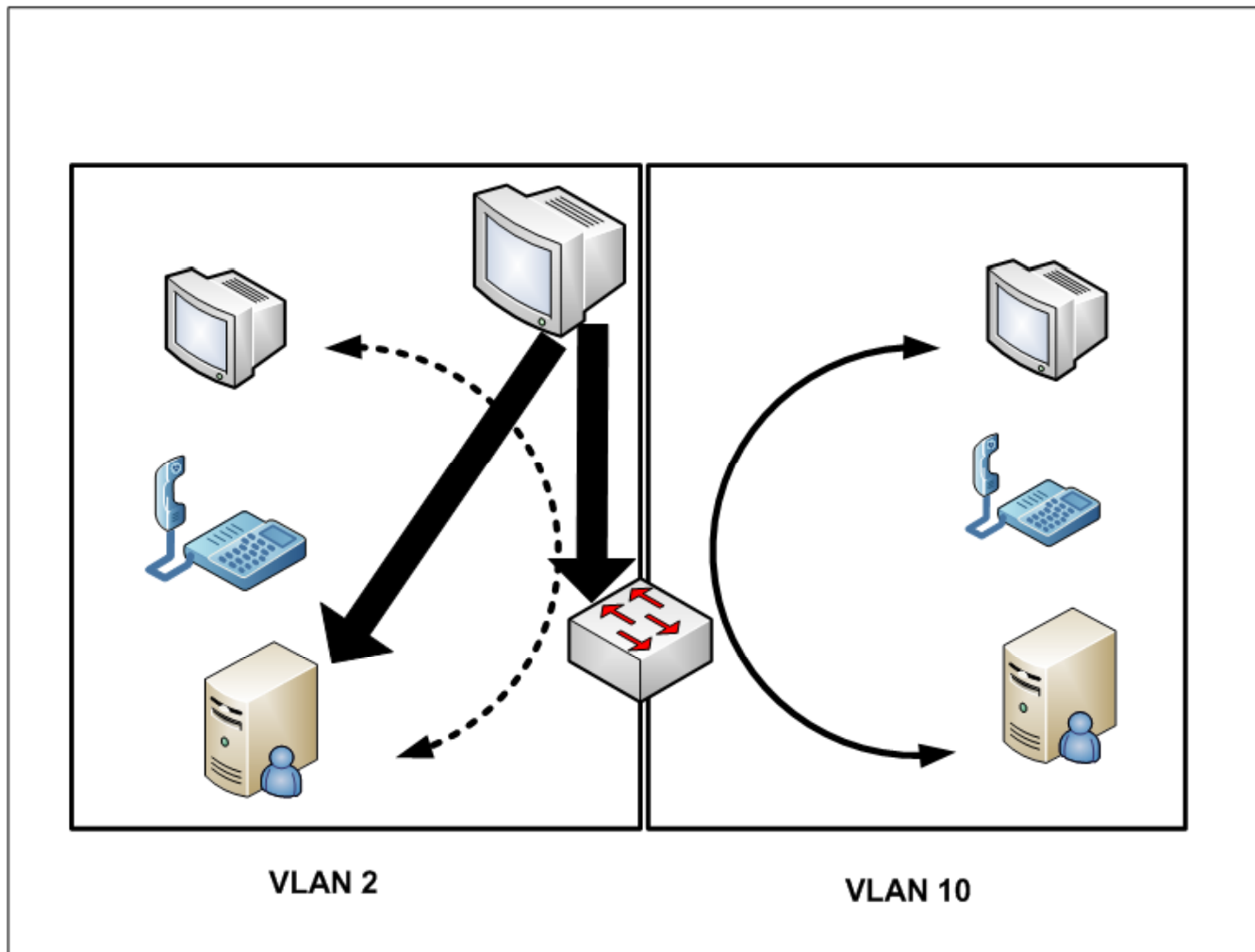
- Preventing successful call placement (including emergency/911)
- Disconnecting existing calls, or preventing use of related services like voicemail
- Overloading call control servers and gateways

# Distributed Denial-of-Service (DDoS) Attack



# Internal Denial-of-Service Attack

An Internal Denial-of-Service Attack



# DoS Attack Scenarios

## TLS Connection Reset

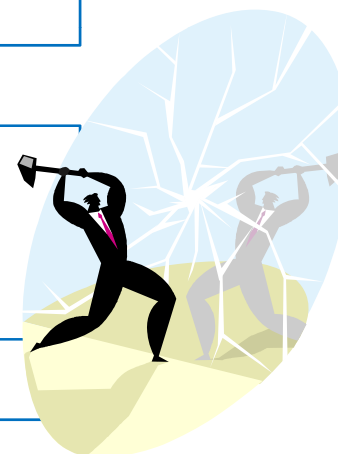
- It sends junk packet and the TLS connection resets, interrupting the signaling channel between the phone and call server

## VoIP Packet Replay Attack

- It captures and resends out-of-sequence VoIP packets adding delay to the call and degrades the call quality

## Wireless DoS

- Initiates a DoS attack against wireless VoIP endpoints by sending 802.11 or 802.1X frames that causes network disconnection





# DoS Attack Scenarios (cont'd)

## QoS Modification Attack

- Modifies non-VoIP-specific protocol control information fields in VoIP data packets to and from endpoints to degrade voice service

## VoIP Packet Injection

- It sends forged VoIP packets to endpoints, injecting speech, or noise or gaps into active call

## Bogus Message DoS

- It sends VoIP servers or endpoints valid-but-forged VoIP protocol packets to cause call disconnection



# DoS Attack Scenarios (cont'd)

## DoS against Supplementary Services

- Initiates a DoS attack against other network services upon which the VoIP service depends

## Control Packet Flood

- Attacker's intent is to deplete/exhaust device, system, or network resources to the extent that VoIP service is unusable

## Invalid Packet DoS

- It sends VoIP servers or endpoints invalid packets that exploit device OS and TCP/IP



# Eavesdropping

Attack that allows to capture the data stream among VoIP endpoints without altering the data

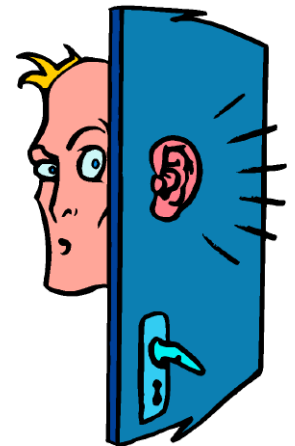
Eavesdropping is used for:

## Call Pattern Tracking

- An illegal data traffic produced by the node or nodes on the network that includes theft and deceiving activities like phishing

## Traffic Capture

- It is an unauthorized way of recording data traffic



# Eavesdropping (cont'd)

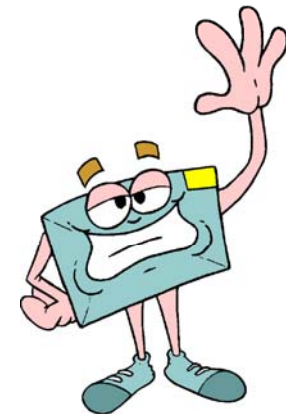
## Number Harvesting

- It is an unauthorized capturing of numbers and email addresses



## Voicemail Reconstruction

- It is an unauthorized monitoring, recording, recognition, interpretation, and translation of any voice mail message



## Fax Reconstruction

- It is the illegal interpretation, translation, and feature extraction of any document image



# Eavesdropping (cont'd)

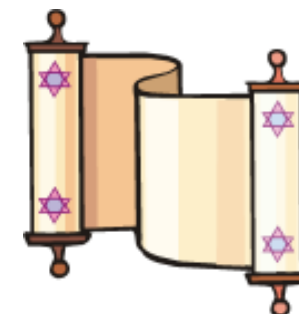
## Video Reconstruction

- It is the unauthorized recording, storage, interpretation, and feature extraction of moving images



## Text Reconstruction

- It is the unlawful monitoring, storage, recognition, translation and feature extraction of text in containing identity, presence or status



## Conversation Reconstruction

- It is the illegal recording, storage, recognition, interpretation, and feature extraction of voice portion communication system



# Packet Spoofing and Masquerading

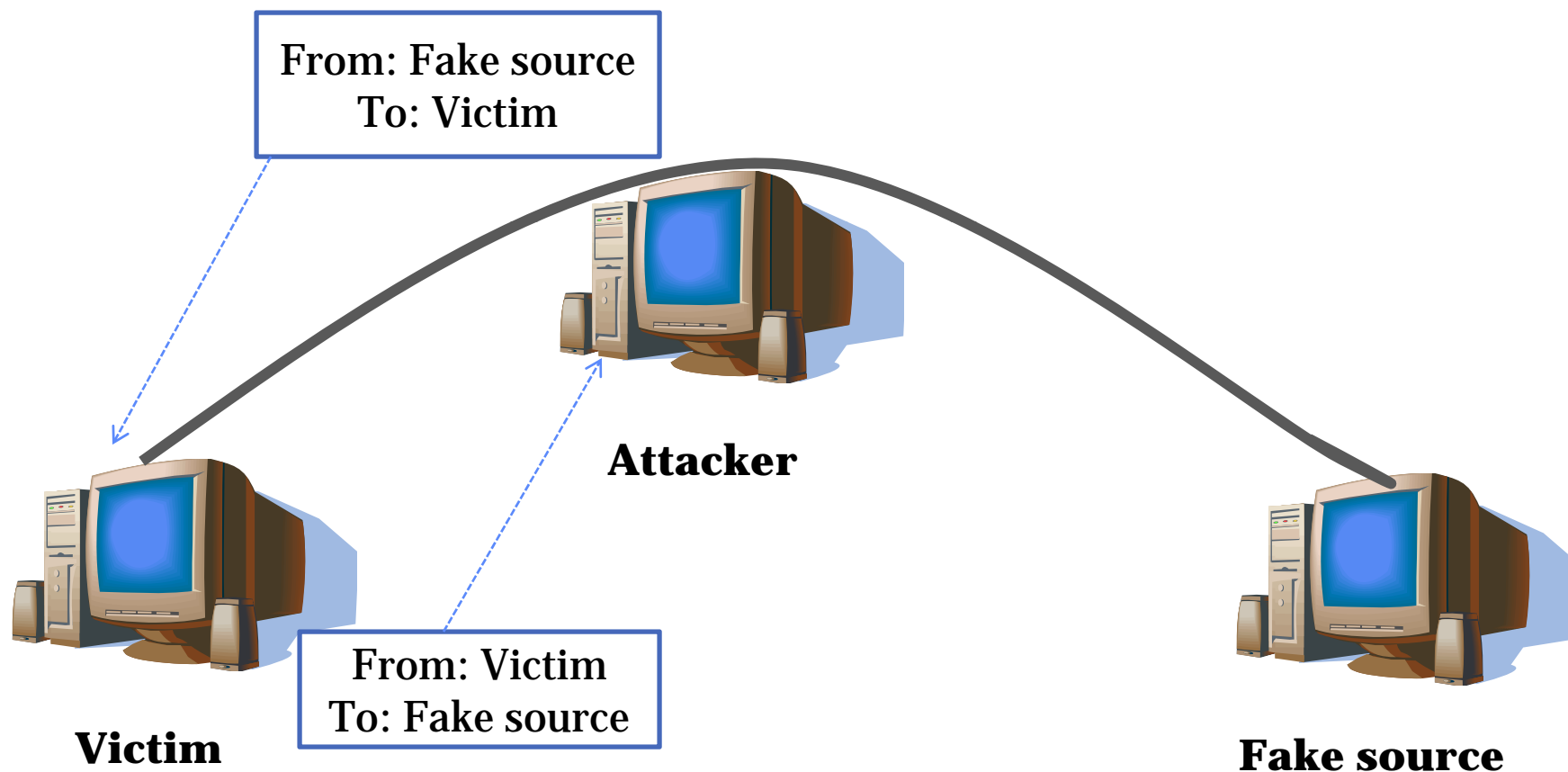
Packet Spoofing and Masquerading is sending the IP packets with fake source addresses

Packet Spoofing and Masquerading is used to:

- Misconfigure the origin of the packet while attacking
- Connect as another system as the attack originator
- Masquerade as a trusted system by manipulating of Caller ID or Call Line Identification (CLID)
- Intercept or hijack network traffic
- Direct response to another system and
- Perform “man-in-the-middle” spoofing attacks



# Packet Spoofing and Masquerading (cont'd)



# Replay Attack

Replay Attack captures a valid packet with the intent of replaying in the network

Attackers can use replay attacks for:

- Capturing the entry point to the target network to eavesdrop or other attack purposes
- Packet spoofing and masquerading

VoIP network is prone to such attacks if no message integrity checking is conducted





# Call Redirection and Hijacking

In call redirection and hijacking, an attacker redirects a call intended for a user



## Attack Scenarios

- **Registration Hijacking**
  - It occurs when an attacker impersonates a valid UA (User Agent) to a registrar and replaces the registration with its own address
- **Proxy Impersonation**
  - It occurs when an attacker tricks a SIP UA or proxy into communicating with a rogue proxy

# Call Redirection and Hijacking (cont'd)

## Toll Fraud

- Rogue or legitimate VoIP endpoint uses a VoIP server to place unauthorized toll calls over the PSTN

## Message Tampering

- Capture, modify, and relay unauthenticated VoIP packets to/from endpoints

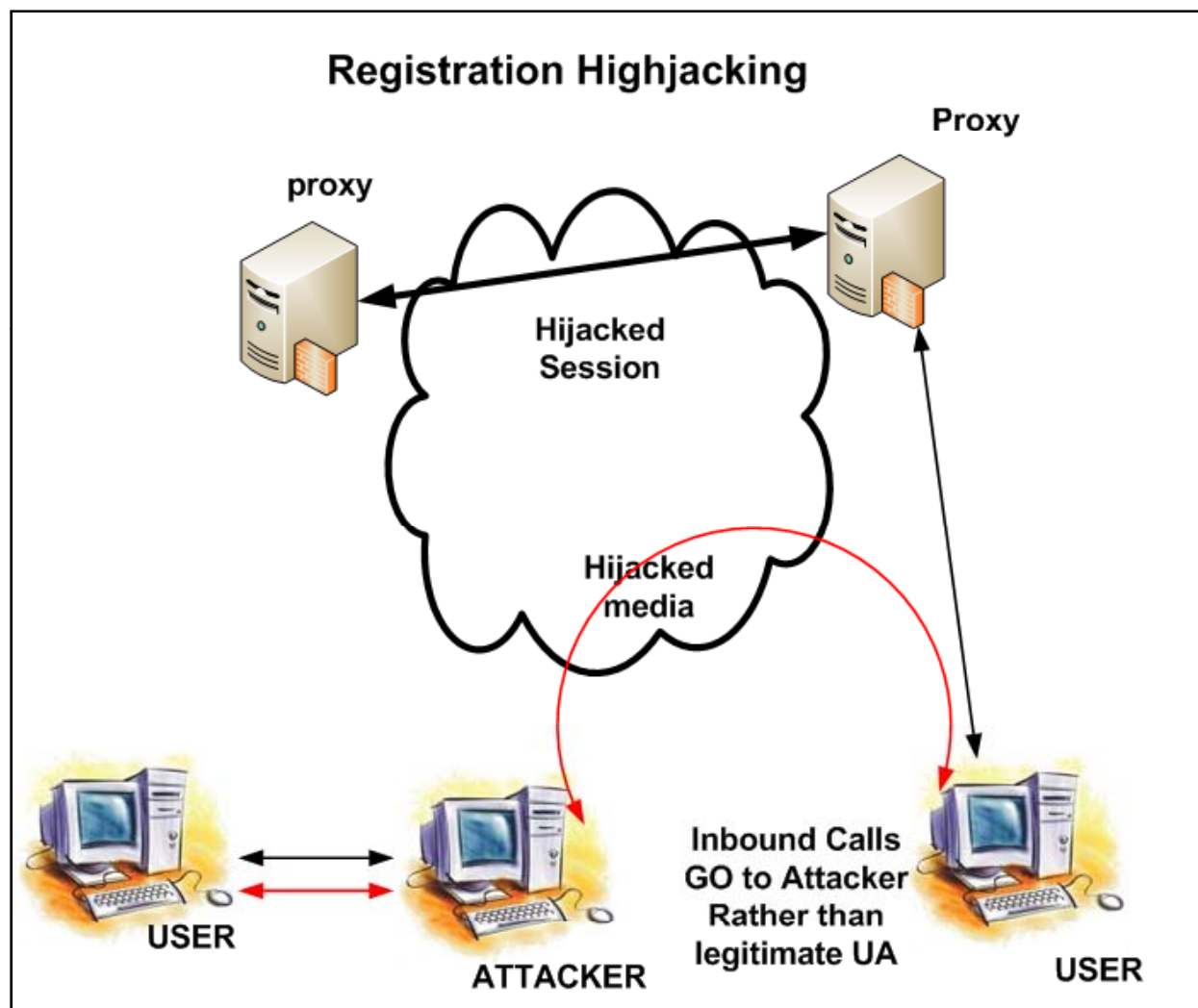
## VoIP Protocol Implementation Attacks

- Sends invalid packets to VoIP servers or endpoints

## Rogue VoIP Endpoint Attack

- Rogue IP endpoint contacts VoIP server by leveraging stolen or guessed identities, credentials, and network access

# Call Redirection and Hijacking (cont'd)



A rogue IP device can spoof a normal IP device by sending unsolicited ARP replies to a target host

Unsolicited ARP reply contains the hardware address of the normal device and the IP address of the malicious device

An attacker can use ARP Spoofing to capture, analyze, and eavesdrop into VoIP communications



# ARP Spoofing (cont'd)

## ARP redirection

- Operates bidirectionally wherein a spoofing device can insert itself in the middle of a conversation between two IP devices on a switched network

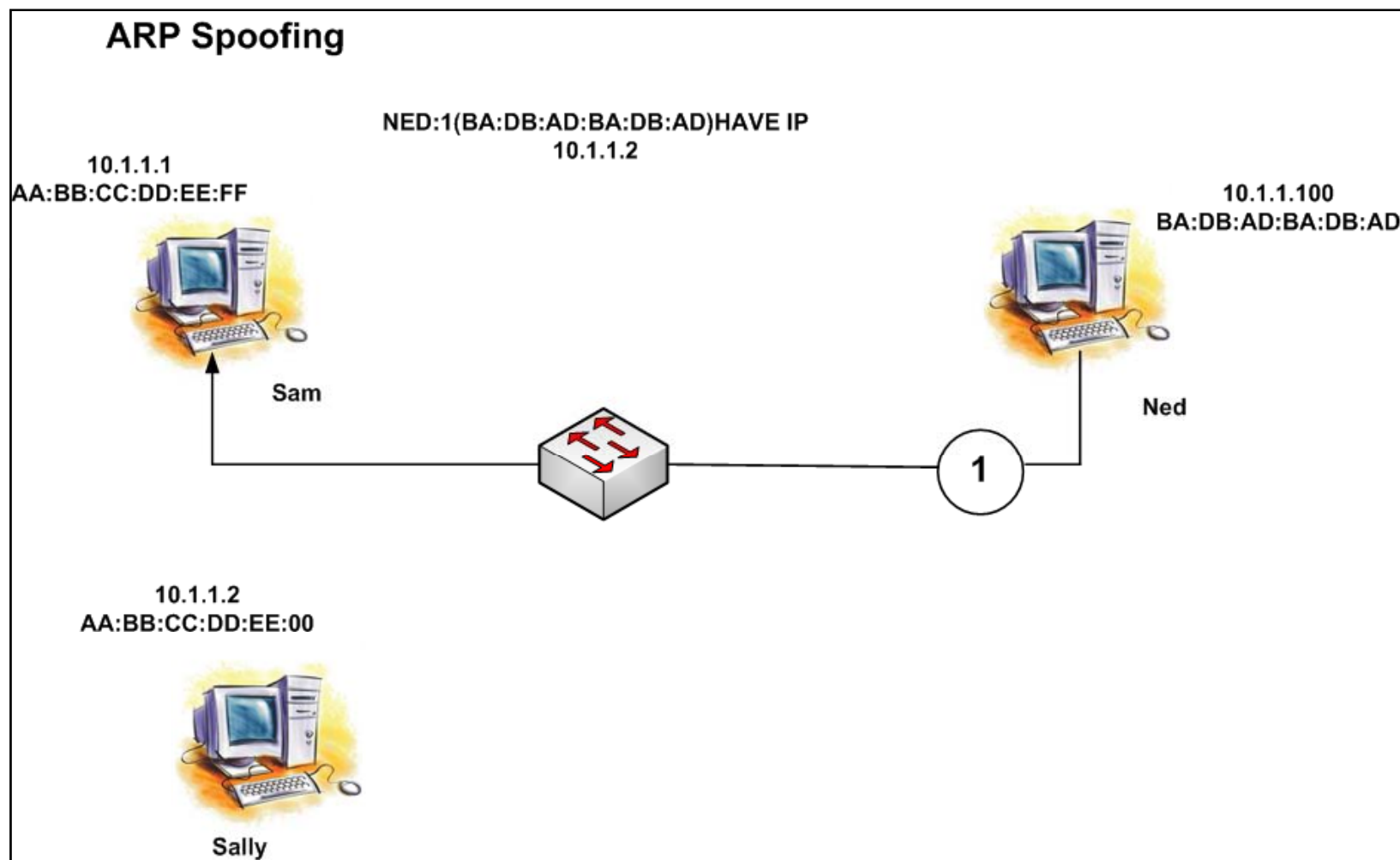


## ARP hijacking

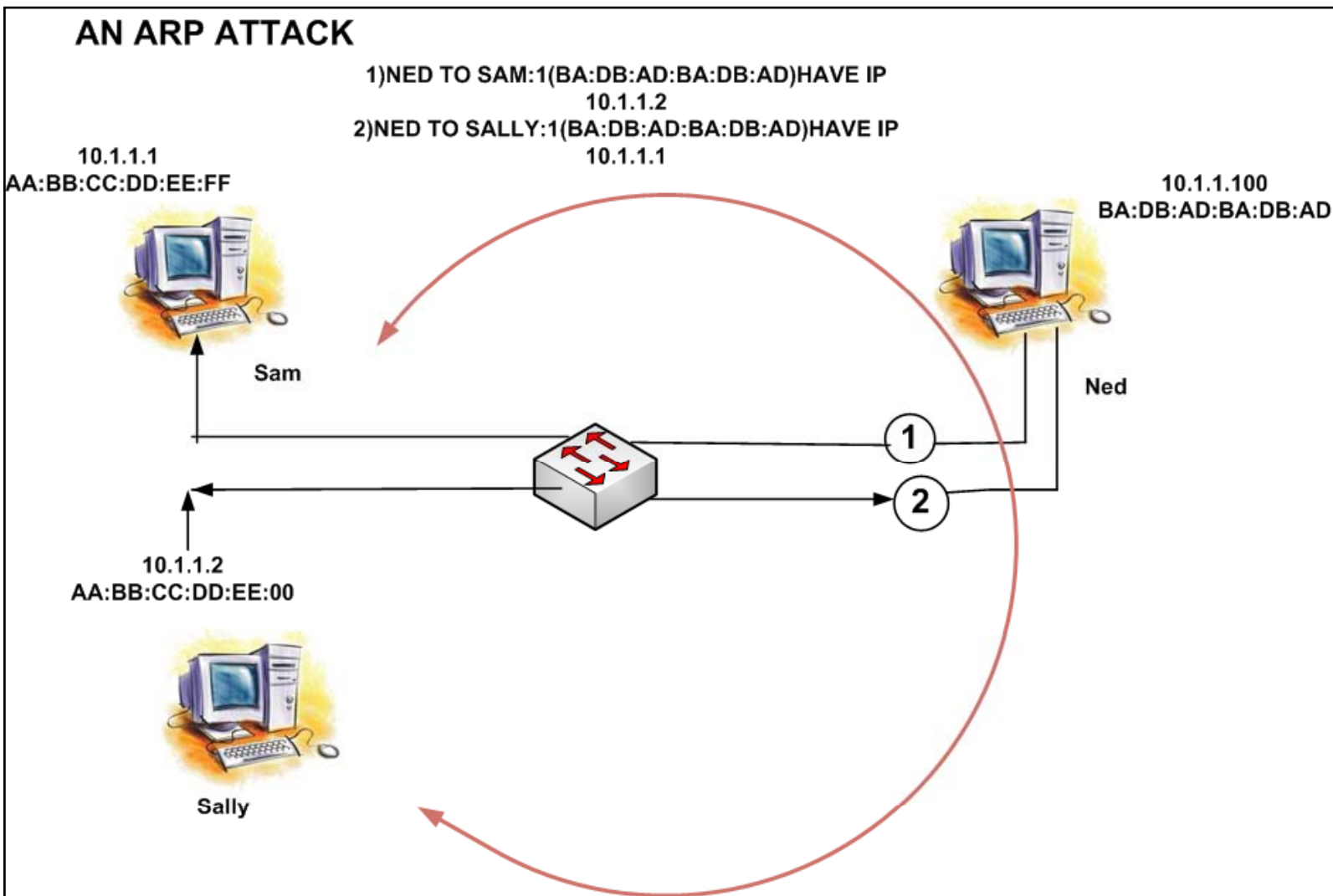
- It hijacks a user's VoIP Subscription and subsequent Voice communications traversing the internal IP network



# ARP Spoofing Attack



# ARP Spoofing Attack (cont'd)

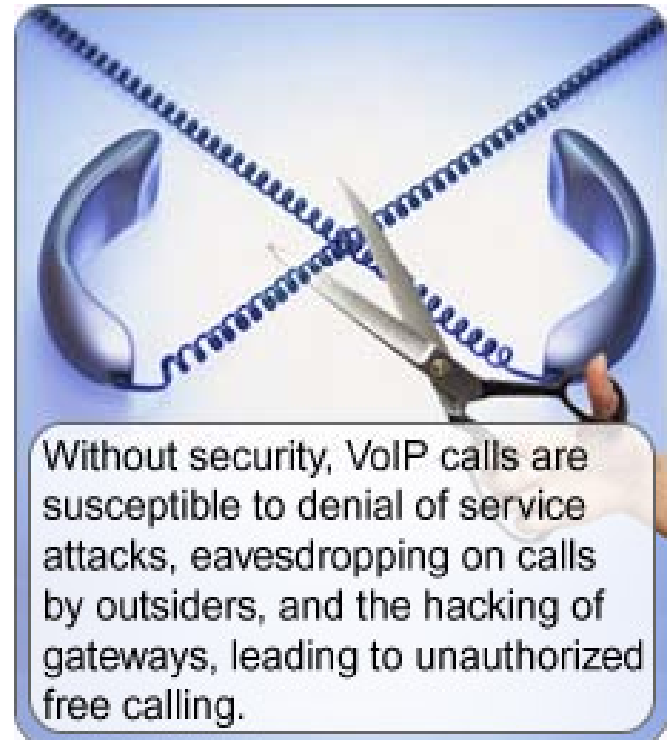


# Service Interception

Service interception is a sudden, unlawful interception of VoIP services

It occurs due to:

- Compromise of PBX hosts and voice gateways
- Poor control, detection, and management systems
- Poor security awareness and practices and
- Poor physical security



Without security, VoIP calls are susceptible to denial of service attacks, eavesdropping on calls by outsiders, and the hacking of gateways, leading to unauthorized free calling.



# Service Interception (cont'd)

Threats include:

Attacks against VoIP devices operating systems

Configuration weaknesses in VoIP devices

VoIP protocol implementation vulnerabilities



# H.323-Specific Attacks

Implementation of H.323 message parsers results in security vulnerabilities in the H.323 suite



# SIP Security Vulnerabilities

SIP is an unstructured text-based protocol and prone to Vulnerabilities identified in:

- INVITE message used by two SIP endpoints
- SSL implementation in SIP proxy server is vulnerable to an ASN.1 BER decoding error



## Registration Hijacking

- An attacker sniffs a REGISTER message from a valid user and modifies it with its own address as the contact address

## IP Spoofing/Call Fraud

- An attacker impersonates another valid user with spoofed ID and sends an INVITE or REGISTER message
- If SIP messages are sent in clear text, it is difficult to block IP spoofing

# SIP Attacks (cont'd)

## Weakness of Digest Authentication

- Since it is based on MD5 digest algorithm being weak, it cannot provide high security

## INVITE Flooding

- An attacker sends INVITE messages with a fake address and paralyzes the user terminal or SIP proxy server

## BYE Denial of Service

- An attacker sniffs valid INVITE messages to counterfeit a valid BYE message and sends it to one of the communicating parties



# SIP Attacks (cont'd)

## RTP Flooding

- An attacker makes fake RTP packets and bombards either of the ends with the fake RTP packets, resulting in quality degradation or terminal reboot

## Spam over Internet Telephony (SPIT)

- A SPIT threat sends unsolicited calls to legitimate users that contain mostly prerecorded messages



# Flooding Attacks

Flooding Attacks allows an attacker attempt to consume all available network or system resources

## UDP Flooding Attacks

- It allows an attacker to manipulate trust relationships within an organization to bypass firewalls and other filter devices

## TCP SYN flood attacks

- It subverts the TCP connection three-way handshake in order to overwhelm a target with connection management
- Attacker sends a flood of SYN packets with spoofed source IP addresses

# Flooding Attacks (cont'd)

## ICMP and Smurf Flooding Attacks

- It involves a flood of legitimate ICMP responses from the networks to the victim who was spoofed

## QoS Manipulation with Targeted Flooding

- This attack involves subverting the quality of service mechanisms within a network in order to degrade VoIP applications





# DNS Cache Poisoning

DNS cache poisoning attacks involve an attacker tricking a DNS server into believing the veracity of a fake DNS response

It is to redirect the victims dependent on that DNS server to other addresses

It has traditionally been used in phishing schemes to redirect a user trying to surf to their banking site to a fake site owned by the hacker

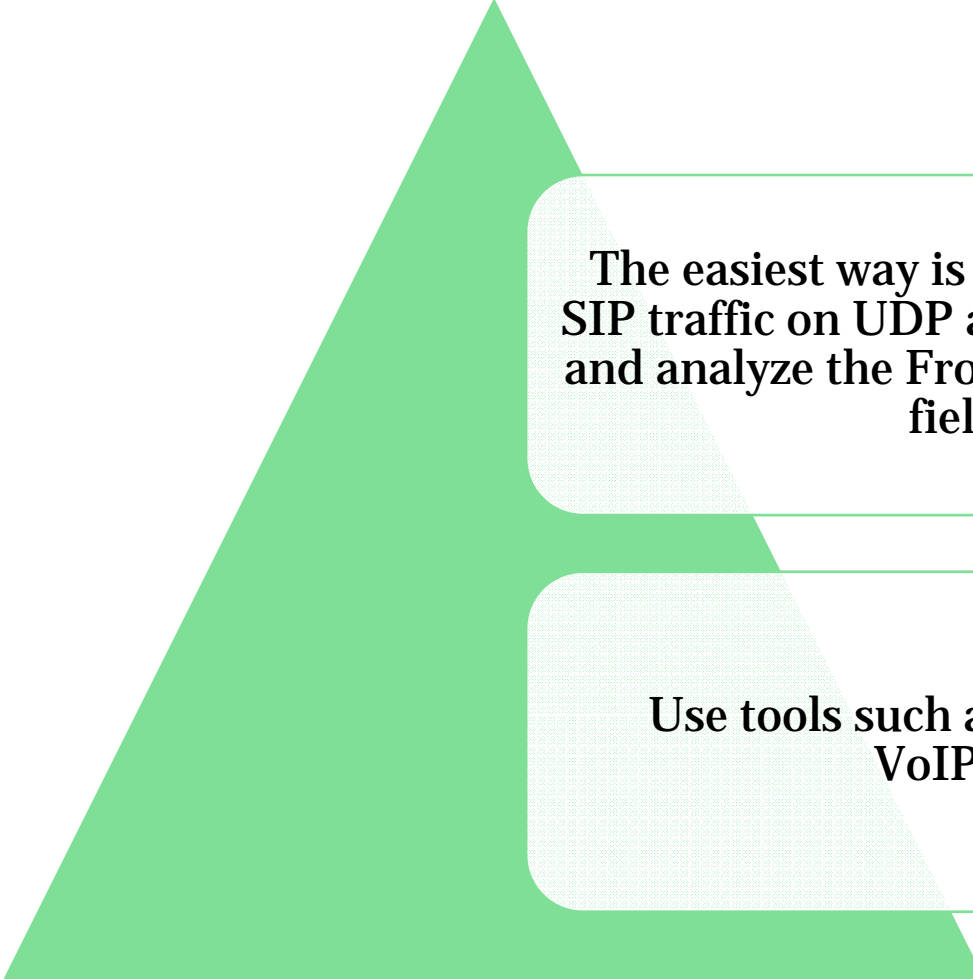


# Sniffing TFTP Configuration File Transfers

Sniffing for TFTP configuration files traveling across the network is as easy as simply watching for any and all traffic on UDP port 69 using Tcpdump or Ethereal



# Performing Number Harvesting and Call Pattern Tracking



The easiest way is to simply sniff all SIP traffic on UDP and TCP port 5060 and analyze the From: and To: header fields

Use tools such as ethereal and VoIPong

# Call Eavesdropping

Tools can perform call eavesdropping:

**Wireshark**

- It captures traffic normally

**Cain and Abel**

- It is a powerful sniffing and password-cracking tool

**Vomit**

- It is a utility that can be used with the sniffer tcpdump to convert RTP conversations to WAV files

**VoIPong**

- It can be configured to output WAV files for each captured conversation

**Oreka**

- It is an open-source VoIP recording toolset that runs on Windows and flavors of Linux

# Interception through VoIP Signaling Manipulation

An attacker to send spoofed or malformed signaling requests to a misconfigured or unsecured proxy in order to redirect incoming or outgoing calls to a victim



# Man-In-The-Middle (MITM) Attack

An attacker is able to insert herself between two communicating parties to eavesdrop and/or alter the data traveling between them without their knowledge

This attack can perform:

- Eavesdropping on the conversation
- Causing a denial of service by black-holing the conversation
- Altering the conversation by omitting media
- Altering the conversation by replaying media
- Altering the conversation by inserting media
- Redirecting the sending party to another receiving party

# Application-Level Interception Techniques

Assuming a SIP deployment with application-level interception, trick the SIP phone, SIP proxy into communicating with pretended legitimate SIP endpoint

## Attack Steps:

- Trick a SIP phone or SIP proxy into communicating with a rogue application
- Provide a rogue application that can properly mimic the behavior of a SIP phone and /or SIP proxy



# How to Insert Rogue Application

## Network-level MITM attacks:

- Used to trick a SIP phone or SIP proxy into communicating with a rogue application

## Registration hijacking:

- It refers to a situation where an attacker replaces legitimate registration with a false one

## Redirection response attacks:

- Can cause inbound calls to go to a rogue application rather than the legitimate SIP phone, an attacker replies to a SIP INVITE with a certain response

## SIP phone reconfiguration:

- When a user makes a call, it will communicate with the rogue application, rather than legitimate proxy

## Physical access to the network:

- If you have physical access to the wire connecting a SIP endpoint to the network switch, you can insert a PC acting as an inline bridge



# SIP Rogue Application

View and modify signaling and media by tricking SIP proxies and SIP phones into talking to rogue applications



## Rogue SIP Back-to-Back-User Agent (B2BUA):

- Performs like a user agent/SIP phone and can get between SIP proxy and SIP phone
- It is “inline” on all signalling and media

## Rogue SIP proxy:

- Performs also like a SIP proxy
- It is “inline” on all signaling exchanged with it

# Listening to/Recording Calls

Set up a test bed with two proxies, each of which served several SIP phones

To perform this attack:

- Insert sip\_rouge application in the middle
- Run the application on the hacker system and relay calls to the original intended recipient
- Commands to configure the sip\_rouge application
  - Issue<sipEndPointName> accept calls [after ringing for<number>-<number>seconds]



# Replacing/Mixing Audio

Use sip\_rogue application to insert or mix in audio

sip\_rogue application can drop and replace with the legitimate recorded one during the call

Attackers can vary the amplitude of the mixed audio causing it to “drown out” the legitimate audio or sound

Attacker can mix in noise creating a perception that VoIP system is behaving poorly

# Dropping Calls with a Rogue SIP Proxy

Configure `sip_rogue` application as a Sip proxy and insert it in the signalling stream between a SIP phone and SIP proxy

Attacker can record signalling, redirect calls, and selectively drop calls

Configure `sip_rogue` application to drop all calls

Commands required to configure `sip_rogue` application:

```
sip_rogue
telnet localhost 6060
connection 0
create sipudpport port
create sipdispatcher disp
create sipregistrar reg 10.1.101.1
issue port hold
```



# Randomly Redirect Calls with a Rogue SIP Proxy

Configure sip\_rogue application to randomly redirect calls

Commands to cause sip\_rogue application for randomly redirect calls:

```
sip_rogue  
telnet localhost 6060  
connection 0  
create sipudpport port  
create sipdispatcher disp  
create sipregistrar reg 10.1.101.1  
issue reg randomize
```



# Additional Attacks with a Rogue SIP Proxy

`sip_rogue` application can perform other attacks, when configured as a rogue SIP proxy

## Few signalling attacks:

- Sending all calls through a rogue B2BUA
- Negotiating not using media encryption
- Selectively dropping calls
- Creating a database of a key user's calling patterns
- Monitoring signaling for passwords and keys



# What is Fuzzing

Fuzzing is the method for finding bugs and vulnerabilities by creating different types of packets for the target protocol that push the protocol's specifications to the breaking point

Also known as Robustness testing or Functional protocol testing

For efficient fuzzing, create representative test cases

# Why Fuzzing

To find the security vulnerabilities and robustness of vendor's software applications

To find the exploitable problem with a potentially deployed VoIP applications

To find the common vulnerabilities such as:

- Buffer overflows
- Format string vulnerability
- Integer overflow
- Endless Loops and logic errors





# Commercial VoIP Fuzzing Tools

Codenomicon test tool (<http://www.Codenomicon.com>)

Musecurity's Mu-4000 (<http://www.Musecurity.com>)

Beyond security's BeStorm(<http://www.Beyondsecurity.com>)

Gleg.net's Proto Ver Professional(<http://www.Gleg.net/>)

Security Innovations Hydra( <http://www.Securityinnovation.com>)

Sipera systems LAVA(<http://www.Sipera.com>)

# Signaling and Media Manipulation

An attacker manipulates SIP signaling or media to hijack or otherwise manipulate calls

## Common attacks:

- Registration Removal
- Registration Addition



# Registration Removal with erase\_registrations Tool

erase\_registrations tool sends a properly crafted REGISTER request for a SIP phone to a SIP proxy

## Attacks:

### Simple Registration Removal

- erase\_registrations tool erases the registrations for one or all of the SIP phones

### Registration Removal Race Condition

- It defeats when a SIP phone re-registers itself

### Registration Removal with SiVuS

- Use SiVuS to erase registrations

# Registration Addition with add\_registrations Tool

add\_registrations tool sends a properly crafted REGISTER request, containing a new contact for a user

## Attacks:

### Annoying Users by Adding New Contacts

- It add one or more contacts for one or more SIP phones, so that when the intended user receives an inbound call, multiple SIP phones will ring

### Basic Registration Hijacking

- It can be used to add a new contact, performing a basic registration hijacking attack

### Registration Addition with SiVuS

- Use SiVuS to create a REGISTER request for the current registration while adding a new contact

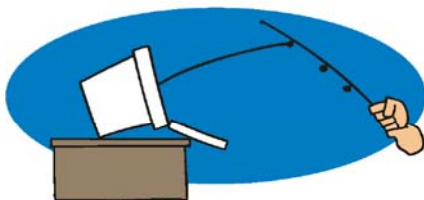
# VoIP Phishing

VoIP Phishing involves an attacker setting up a fake IVR (Interactive Voice Response) trying to glean the victims' account number

Also known as vishing

Attacker trick victims into entering sensitive information such as:

- PIN number
- Account number
- SSN





# Covering The Tracks

# Covering Tracks

Once intruders have successfully gained Administrator's access on a system, they will try to cover the detection of their presence

When all the information of interest has been stripped off from the target, the intruder installs several backdoors so that he can gain easy access in the future



Footprinting is the process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment

Hacker generally tries to gain information about the possible supporting infrastructure before launching an attack

Fuzzing is the method for finding bugs and vulnerabilities by creating different types of packets for the target protocol that push the protocol's specifications to the breaking point

VoIP Phishing involves an attacker setting up a fake IVR (Interactive Voice Response) trying to glean the victims' account number

In MITM attack, an attacker is able to insert himself/herself between two communicating parties to eavesdrop and/or alter the data traveling between them without their knowledge



DEAR, I THINK YOU'RE  
SPENDING WAAAAAY  
TOO MUCH TIME ON  
THE INTERNET.

I.COM  
AM.COM  
NOT.COM



© 2000 Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)

Copyright 2005 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“To protect our network against computer viruses,  
our IT Department has issued a ban on any use of  
e-mail attachments. For further details, please  
refer to the attached document.”**