Hacking Exposed 7
Network Security Secrets & Solutions

Chapter 7 Remote Connectivity and VoIP Hacking

Remote Connectivity and VoIP Hacking

- Dial-up Hacking
- PBX (Private Branch Exchange) Hacking
- Voicemail Hacking
- Virtual Private Network (VPN) Hacking
- Voice Over IP (VoIP) Attacks

Dial-up Hacking

Preparing to Dial up

- Many companies still use dial-up connections
  - Connecting to old servers, network devices, Industrial control system (ICS)
- Dial-up hacking process is similar to other hacking
  - Footprint, scan, enumerate, exploit
  - Automated by tools: wardialer or demo dialer
- Phone number footprinting: identify blocks of phone numbers to load into a wardialer
  - Phone directories, target websites, Internet name registration database, manual dialing, etc.
  - Countermeasures: require a password to make account inquiries; sanitize sensitive information; educate employees

Dial-up Hacking
Wardialing

- Hardware
  - Important as the software, greatly affect efficiency
    - The number of modems, high-quality modems
- Legal issues
  - Laws about wardialing activities
    - Identify phone lines, record calls, spoof phone numbers, etc.
- Peripheral costs
  - Long distance, international or nominal charges
- Software
  - Automated scheduling, ease of setup, and accuracy
  - Tools: WarVOX, TeleSweep, PhoneSweep

Dial-up Hacking

Brute-Force Scripting - The Homegrown way

- Categorize the connections into *penetration domains*
  - Based on wardialing results
  - Experience with a large variety of dial-up servers and OS
- Brute-force scripting attack: ZOC, Procomm Plus, and ASPECT scripting language

Domains	Attacking remarks
Low Hanging Fruit	Easily guessed or commonly used passwords
Single Authentication, Unlimited Attempts	ONE type of authentication (password or ID) NOT disconnect after a number of failed attempts
Single Authentication, Limited Attempts	ONE type of authentication (password or ID) Disconnect after a number of failed attempts
Dual Authentication, Unlimited Attempts	TWO type of authentication (password and ID) NOT disconnect after a number of failed attempts
Dual Authentication, Limited Attempts	TWO type of authentication (password and ID) Disconnect after a number of failed attempts

Dial-up Hacking

Dial-up Security Measures

1. Inventory existing dial-up lines
2. Consolidate all dial-up connectivity to a central modem bank
   - Position as an untrusted connection off the internal network
3. Make analog lines harder to find
4. Verify that telecommunications equipment closets are physically secure
5. Regularly monitor existing log features within dial-up software
6. For business serving lines, do not disclose any identifying information
7. Require multi-factor authentication systems for all remote access
8. Require dial-back authentication
9. Ensure the corporate help desk is aware of the sensitivity of giving out or resetting remote access credentials
10. Centralize the provisioning of dial-up connectivity
11. Establish firm policies
12. Back to step 1

PBX (Private Branch Exchange) Hacking

- Dial-up connections to PBXes still exist
  - Managing method, especially by PBX vendors
- Hacking PBXes takes the same route as typical dial-up hacking

PBX Systems	Attacking remarks
Octel Voice Network Login	Password is a number; by default 9999
Williams/Northern Telecom PBX	Require a user number/ four-digit numeric-only access code
Meridian Links	There are some default user IDs/passwords (e.g. maint/maint)
Rolm PhoneMail	There are some default user IDs/passwords (e.g. sysadmin/sysadmin)
PBX Protected by RSA SecurID	Take a peek and leave; cannot defeat

- Countermeasures: reduce the time when modems turned on; deploy multiple forms of authentication

Voicemail Hacking

- Brute-force Voicemail Hacking
  - In similar fashion to dial-up hacking methods
  - Required components: phone number to access voicemail; target voicemail box (3~5 digits); educated guess about voicemail box password (typically only numbers)
  - Tools: Voicemail Box Hacker 3.0 and VrACK 0.51 (for old/less-secure system), ASPECT scripting language
- Countermeasures: deploy a lockout on failed attempts; log/observe voicemail connections

VPN Hacking

Google Hacking for VPN

- VPN has replaced dial-up as the remote access mechanism
- Google hacking
  - Using filetype:pcf to find profile setting files for Cisco VPN client (PCF file)
  - Download, import the file; connect to target network, launch further attacks
  - Passwords stored in PCF file can be used for password reuse attacks (tools: Cain, etc.)
  - Countermeasures: user awareness; sanitize sensitive information on websites; use Google Alerts service

VPN Hacking

Probing IPsec VPN Servers

- Check if service's corresponding port is available (UDP 500)
- Perform IPsec VPN identification and gateway fingerprinting
- Identify the IKE Phase 1 mode and remote server hardware
- Tools: Nmap, NTA Monitor, IKEProber
- Countermeasures: cannot do much to prevent the attack

VPN Hacking

Attacking IKE Aggressive Mode

- IKE Phase 1-Aggressive mode does not provide a secure channel
  - Eavesdropping attacks to authentication information
- First, identify whether target server supports aggressive mode (tool: IKEProbe)
- Then, initiate connection and capture authentication messages (tool: IKECrack, Cain)
- Countermeasures: discontinue IKE Aggressive mode use; use token-based authentication scheme

VPN Hacking

Hacking the Citrix VPN Solution

- Client-to-site VPN solution provides access to remote desktops and applications
  - A full-fledged remote desktop (Microsoft Windows)
  - Commercial off-the-shelf (COTS) application
  - Custom application
- Typical attack is to spawn to another process in a remote Citrix environment (i.e. explorer.exe, cmd.exe, PowerShell, etc.)
- Ten most popular categories for attacking published applications: Help, Microsoft Office, Internet Explorer, Microsoft Games and Calculator, Task Manager, Printing, Hyperlinks, Internet Access, EULAs Text Editor, Save As/File System Access
- Countermeasures: place Citrix instance into segmented, monitored and limited environment; multifactor authentication; assess the system

VoIP Attacks
SIP Scanning

- The transport of voice on top of an IP network
  - Signaling protocols: H.323 and SIP
- SIP scanning: discover SIP proxies and other devices
  - Tools: SiVuS, SIPVicious
  - Countermeasures: network segmentation between VoIP network and user access segment

VoIP Attacks

Pillaging TFTP for VoIP Treasures

- Many SIP phones rely on a TFTP server to retrieve configuration settings
  - May contain user name/password for administrative functionality
- Firstly, locate TFTP server (tools: Nmap)
- Then, attempt to guess the configuration file's name (tools: TFTP brute-force)
- Countermeasures: access restriction to TFTP

VoIP Attacks

Enumerating VoIP Users

- Traditional manual and automated wardialing methods
- Observe servers' responses
  - SIP is a human-readable protocol
- Cisco Directory Services
- Automated user enumeration tools: SIPVicious (svwar.py), SIPScan, Sipsak
- Countermeasures: segmenting VoIP and user networks; deploy IDS/IPS systems

VoIP Attacks

Interception Attack

- First, intercept the signaling protocol (SIP, SKINNY, UNIStim) and media RTP stream
  - ARP spoofing attack (tools: dsniff, arp-sk)
  - Sniff VoIP datastream (tools: tcpdum, Wireshark)
- Next, identify the codec (Payload Type field or Media Format field)
- Then, convert datastream to popular file types (tools: vomit, scapy)
- GUI and all-in-one tools: UCSniff
- Offline analysis and attack tools: Wireshark (RTP, Cisco's SKINNY dissectors), SIPdump and SIPcrack

VoIP Attacks

Denial of Service

- DoS the infrastructure or a single phone
  - Sending a large volume of fake call setup signaling traffic (SIP INVITE)
  - Flooding the phone with unwanted traffic (unicast or multicast)
- Tools: Inviteflood, hack_library
- Countermeasures: network segment between voice and data VLANs; authentication and encryption for all SIP communication; deploy IDS/IPS system

Summary

- Remote access security tips:
  - Password policy is even more critical
  - Consider two-factor authentication
  - Develop provisioning policies for any type of remote access
  - Eliminate unsanctioned use of remote control software
  - Be aware PBXes, fax servers, voicemail systems, etc., besides modems
  - Educate support personnel and end users
  - Be extremely skeptical of vendor security claims
  - Develop a strict use policy and audit compliance

Exercises

1. Google and download a PCF file. Then, use Cain for password decoding attack. Screen dump results and explain.
2. Use Nmap, NTA Monitor, IKEProbe to identify whether a target VPN server supports Aggressive mode. Screen dump “useful” results and explain.
3. Use SiVuS, SIPVicious to scan a public SIP server. Screen dump “useful” results and explain.