

VoiceCon Spring 2007

Elements of a Vulnerability Assessment

**Llewellyn Derry - CISSP, CISM, CHSP
Director - Security Solutions
NEC Unified Solutions
March 7, 2007**

Key Questions

- What are the steps involved in putting together --- and following through on --- a vulnerability assessment for your enterprise?
- Who should lead an IP Telephony Vulnerability Assessment : Telecom/IT Team or the network security team?
- What are the best outside sources of information on security vulnerabilities?
- What IP Telephony elements typically present the most serious points of vulnerability and how does this relate to the existing 'legacy' data networking infrastructure?



Best Practices for Securing “any” Network :

- Disabling unnecessary services running call control software
- Run all Traffic (including VoIP) through your firewall and IPS
- Control Access to your IP PBX by access list and rate limiting
- Keep current on your software security patches and updates on “all” IT hardware, software and server operating systems

How are Today's Calls Completed?

- Layer 2 Network (MPLS, Frame Relay, ATM)
- Layer 3 VPN
- Toll/TDM
- Internet

Targeted VoIP Attacks are Rare...



- Registration and Session Hijacking
- Eavesdropping
- Vendor Specific Denial of Service (DOS)

Key Questions

- **What are the steps involved in putting together --- and following through on --- a vulnerability assessment for your enterprise?**
- Who should lead an IP Telephony Vulnerability Assessment : Telecom/IT Team or the network security team?
- What are the best outside sources of information on security vulnerabilities?
- What IP Telephony elements typically present the most serious points of vulnerability and how does this relate to the existing 'legacy' data networking infrastructure?

What are the Steps...

- Know Your Enterprise Network
 - Assets/Hardware
 - Software
 - Applications
- Develop Strategy on How to Conduct a Vulnerability Assessment and How to Remediate
- Follow Through w/ VA Strategy
 - Mapping Network Assets
 - Identify Vulnerabilities
 - Quantify Vulnerabilities
 - Triage Vulnerabilities
- Remediate According to Level of Severity
- Follow up to confirm vulnerability has been remediated
- Conduct Periodic VA based upon Corporate Security Policy

Key Questions

- What are the steps involved in putting together --- and following through on --- a vulnerability assessment for your enterprise?
- **Who should lead an IP Telephony Vulnerability Assessment : Telecom/IT Team or the network security team?**
- What are the best outside sources of information on security vulnerabilities?
- What IP Telephony elements typically present the most serious points of vulnerability and how does this relate to the existing 'legacy' data networking infrastructure?

Who Should Lead...

- Security Team !!!
- It's Neither Telecom's nor IT's Responsibility
- Understand who owns and is responsible for the asset and/or data in question

Key Questions

- What are the steps involved in putting together --- and following through on --- a vulnerability assessment for your enterprise?
- Who should lead an IP Telephony Vulnerability Assessment : Telecom/IT Team or the network security team?
- **What are the best outside sources of information on security vulnerabilities?**
- What IP Telephony elements typically present the most serious points of vulnerability and how does this relate to the existing 'legacy' data networking infrastructure?

Best Outside Sources...

- Computer Emergency Response Team (CERT)
- www.cert.org
- Black Hat – www.blackhat.com
- Packet Storm – www.packetstormsecurity.nl
- Security Focus – www.securityfocus.com
- SANS – <http://www.sans.org/top20>

Key Questions

- What are the steps involved in putting together --- and following through on --- a vulnerability assessment for your enterprise?
- Who should lead an IP Telephony Vulnerability Assessment : Telecom/IT Team or the network security team?
- What are the best outside sources of information on security vulnerabilities?
- **What IP Telephony elements typically present the most serious points of vulnerability and how does this relate to the existing 'legacy' data networking infrastructure?**

What IP Telephony Elements...

- Configuration
- Network Architecture Design
- How the IP Telephony is integrated into the Legacy LAN