



Elements of a Vulnerability Assessment

Ken Agress, Senior Consultant

PlanNet Consulting, LLC.



Agenda

- **Defining a Vulnerability Assessment**
- **Types of Vulnerability Assessments**
- **Are You Ready for an Assessment?**
- **What Should a Technical Assessment Look At?**
- **Getting Valuable Results**



Defining a Vulnerability Assessment

- A “vulnerability” is a software, hardware, or procedural weakness that may provide a means to compromise an asset
- A Vulnerability Assessment is a project undertaken to identify these items in your environment
- A Vulnerability Assessment may or may not include:
 - Penetration Testing
 - Social Engineering
 - Port Scanning
 - Session Hijacking
 - Packet Capture



What Types of Assessments are There?

- **Technical Assessment**
 - Focuses on hardware and software
 - Looks for “known issues”
 - Identifies “inappropriate services”
- **Organizational Assessment**
 - Examines security procedures within organization
 - May include social engineering efforts
 - May evaluate your ability to detect attempts to exploit systems
- **Physical Assessment**
 - Examines physical access to assets and personnel
 - Includes reviewing physical security procedures
 - Isolates issues created by direct access to assets
- **Compliance Assessment (HIPPA, SOX, GLBA)**

For this discussion, we’re limiting the topic to Technical Assessments...



Are You Ready For An Assessment?

- **Many of our clients request assessments when...**
 - They haven't put Security Policies, Standards, or Guidelines in place
 - Are looking for a "feel good" verification of their environment
 - Cannot describe what "adequate security" means to their organization
- **Before you ask for an assessment...**
 - Understand the limitations if you don't have a benchmark to compare against
 - Remember that assessments "go stale" quickly and aren't a substitute for a more comprehensive approach
 - Keep in mind that you may not like the results if you haven't "done your homework" first



What Should An Assessment Look At

Core Pieces Of Infrastructure

- **Servers (general or otherwise)**
 - “Listening ports”
 - Login restrictions and abilities
 - Session security
 - Enforcement of policy
- **Key services**
 - DHCP and DHCP attacks
 - DNS and DNS hijacking
 - TFTP services and posture
- **Critical infrastructure**
 - Routers
 - Switches
 - Wireless Access Points
 - Firewalls



What Should An Assessment Look At

**Appropriate
Traffic**

- **Segregation of traffic**
 - Is Voice in its own VLAN?
 - Is Data in its own VLAN?
 - If they do mix, is it appropriate?
- **Network access**
 - Enforcement of security rules and restrictions
 - Network authentication requirements
 - Automated VLAN assignments
 - Network admission requirements
- **Common attacks**
 - Detection and reaction to DoS attacks
 - DHCP re-direction
 - Man-in-the-middle issues



What Should An Assessment Look At

Other Important Items

- **Determine if packet capture is possible**
- **Identify if session encryption policies are in place and enforced**
- **Call signaling (visibility and verification)**
- **Public Key Infrastructure (if present)**
- **Quality of Service**
 - “Hijacking”
 - Enforcement
 - Preservation
- **Known bugs and issues**



Systems You Don't Want To Miss...

- **IP Telephony systems**
 - Call processing servers
 - Gateways
 - SIP proxies (if present)
 - Call accounting systems
- **Core infrastructure**
- **Key IT assets**
 - Domain controllers
 - LDAP servers
 - Critical servers and services
 - DHCP, DNS
- **Remember to look from multiple perspectives and places in your environment!**



Getting Valuable Results

- **Don't accept a list of open ports**
 - Get some idea of the degree of vulnerability
 - Understand if the issue is a “well known problem”
 - Require that “phantom” vulnerabilities are weeded out
- **Require that the results map against your existing policies and procedures**
- **While an assessment is under way, determine:**
 - If you can detect the activities that are occurring
 - If you can respond appropriately to the activities
 - If your automated systems are responding correctly
- **Comments on procedure and policy issues**



Final Thoughts

- **Before approaching any security effort, remember that security is a process and not a technology**
 - Your posture will need to change as technology changes
 - Your vulnerabilities will change over time
 - Your people will always be the primary link in keeping any system secure
- **Without strong policies and processes, security will be questionable in any organization**
- **Remember that any vulnerability assessment will “go stale” quickly; plan on an iterative process**