Securing Remote Access to IT Resources

Presented By:
Bryan Miller
Adjunct Faculty, Computer Science & Information Systems
Virginia Commonwealth University

VA SCAN 2011

Agenda

- Speaker Introduction
- Wikipedia: Remote Access Technologies
- Attack Vectors
- Audit Tools
- Mobile Device Issues
- Hardening Recommendations
- Policies & Procedures (P&P)
- Wrap-Up

VA SCAN 2011

Speaker Introduction

- B.S. Information Systems – VCU
- M.S. Computer Science – VCU
- VCU Network Engineer – 1987 – 1993
- President, Syrinx Technologies, 2007
- Adjunct Faculty Member in Information Systems and Computer Science @ VCU, FTEMS lecturer
- CISSP, former Cisco CCIE in R/S
- Published author with over 25 years in the industry

VA SCAN 2011

Wikipedia: Remote Access Technologies

VA SCAN 2011

- Dial-In/PPP – Point-to-Point Protocol – 1994
  - Layer 2 of the OSI model
  - Provides authentication, encryption & compression
  - Used by ISPs for dial-up Internet access

- PPTP - Point-to-Point Tunneling Protocol – 1999
  - Provides VPN access over GRE tunnel using PPP
  - Does not provide encryption or authentication
  - MSCHAP-v2 used for authentication is vulnerable to dictionary attacks

VA SCAN 2011

- L2TP – Layer 2 Tunneling Protocol - 1999
  - Tunneling protocol used with VPN's
  - Does not provide encryption
  - Still used today by some cable providers
- IPSec VPN
  - Site-Site
    - Dedicated VPN, typically over the Internet
    - No client configuration
  - Remote Access
    - Requires configuration of VPN client
    - Can be a challenge to update large numbers of clients
    - Configuration files must be protected!
    - Split Tunneling Issues

VA SCAN 2011

- SSL VPN
  - Browser-based access to applications
  - No VPN client to load on endpoints
  - Provides user-friendly front end with low maintenance
  - No configuration files to protect
- Single Sign On (SSO)
  - One password to rule them all
  - Various authentication methods
    - Kerberos, smart card, two-factor, Windows AD integration, LDAP
  - Often provides web-based front-end to common applications

VA SCAN 2011

- Authentication Options
  - RADIUS – Remote Authentication Dial-In User Service
    - Implements "AAA" – Authentication, Authorization & Accounting
    - Client-server protocol over UDP
    - Used in VPNs, Wireless, 802.1x, etc.
  - TACACS(+) – Terminal Access Controller Access-Control System (Plus)
    - Cisco proprietary protocol using TCP
    - Access control for networking devices

VA SCAN 2011

- 802.1x
  - IEEE standard for port-based, Network Access Control (NAC)
  - Provides authentication mechanisms for devices wishing to connect to a LAN or WLAN
  - Typically requires an authentication server running RADIUS
  - Most modern operating systems support 802.1x, including iPhone and iPod Touch
  - Vulnerable to MITM attacks

VA SCAN 2011

- Network Access Control (NAC)
  - Technology which restricts access to the network based on identity or security posture
  - To confuse the issue, Cisco's NAC product is actually known as Network Admission Control
  - Can be used to force clients to conform to security policies before granting network access
    - A/V
    - Patches
    - Registry Settings
  - Can be difficult to implement in "legacy" networks

VA SCAN 2011

Attack Vectors

VA SCAN 2011

- Dial-In
  - Yes, this still works!
  - Automated program dials 1000's of phone numbers per day
  - Usually finds "forgotten" out-of-band modem
- Wireless
  - Please don't use WEP, no longer compliant with PCI
  - Rogue APs are still a problem – make sure your P&P documents address this
  - Watch those hotspots!
- Extranet
  - Mutual protection is the only way to go!

VA SCAN 2011

- VPN
  - Protect those configuration files (try Google)
  - Use appropriate complexity for PSKs
- SSL in web sites
  - Test the cipher strengths – applicable to PCI
  - Disable the weak ones
- Outdated out-of-band management tools
  - Are you still using Telnet?

VA SCAN 2011

Audit Tools

VA SCAN 2011

- Web Proxy
  - Burp Suite
  - Paros
- IPSec Configuration
  - IPSecScan
  - IKE-Scan

IKE-Scan Output:

192.168.1.254 Aggressive Mode Handshake

HDR=(CKY-R=509ca66bcabbcc3a)
SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
VID=12f5f2887f768a9702d9fe274cc0100
VID=afcad713a12d96b8696fc77570100
VID=a55b0176cabacc3a52207fea2babaa9
VID=0900299bcfd6b712 (XAUTH)
KeyExchange(128 bytes)
ID(Type=ID_IPV4_ADDR, Value=192.168.1.254)
Nonce(20 bytes)
Hash(20 bytes)

VA SCAN 2011

- SSL Cipher Strength
  - THCSSLCheck
  - SSLDigger
  - OpenSSL
- Web Servers
  - Nikto
  - Nessus

SSLDigger Output:

192.168.1.1:

EXP-RC2-CBC-MD5 – (40)
EXP-RC4-MD5 – (40)
EXP1024-DES-CBC-SHA – (56)
EXP1024-RC4-SHA – (56)
DES-CBC-SHA – (56)

() – Number of bits of encryption

This tool is great for checking PCI compliance!

VA SCAN 2011

- Dial-In
  - PhoneSweep
- PPTP
  - asleap
- Wireless
  - 802.11
    - Aircrack-ng
    - NetStumbler
  - Bluetooth
    - Bluesnarf
    - BlueAuditor

```
File  Edit  View  Terminal  Go  Help
thallium asleap $ time ./asleap -r leap.dump -f dict.dat -n dict.idx
asleap 2.1 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>

Captured LEAP exchange information:
        username:           jwright
        challenge:          ceb69885c656590c
        response:           7279f65aa49870f45822c89dcbdd73c1b89d377844caead4
        hash bytes:         586c
        NT hash:            8846f7eaee8fb117ad06bdd830b7586c
        password:           password

real    0m0.178s
user    0m0.175s
sys     0m0.003s
thallium asleap $
```

```
File  Edit  View  Terminal  Go  Help
thallium asleap $ ./asleap -C 07:86:AE:A0:21:5B:C3:0A -R 7F:6A:14:F1:1E:EB:98:0F
:DA:11:BF:83:A1:42:A8:74:4F:00:68:3A:D5:BC:5C:B6 -f dict.dat -n dict.idx
asleap 2.1 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
        hash bytes:         4a39
        NT hash:            a1fc198bdbf5833a56fb40cdd1a64a39
        password:           qaleap
thallium asleap $
```

From: http://www.willhackforsushi.com/Asleap.html

VA SCAN 2011

- Port Scanners
  - nMap
  - SuperScan 4
  - RAPS (Remote Access Perimeter Scanner)

RAPS Output:

192.168.0.187 Port 5900 - VNC, Version 3.8
192.168.0.9 Port 3389 - Terminal Server
192.168.10.57 Port 5631 - pcAnywhere, Host: A1
192.168.10.56 Port 1720 - NetMeeting
10.2.0.139 Port 1494 – Citrix Server
10.2.1.20 Port 6000 – X Server, Version 11.0
10.2.1.21 Port 6000 – X Server, NO LOGIN REQUIRED, Version 11.0

What's the difference between 10.2.1.20 and 10.2.1.21?

Mobile Device Issues

VA SCAN 2011

- Who owns the device
- Are employee-owned devices allowed
- Applications
- Email sync
- VPN configurations
- Encryption

VA SCAN 2011

- Security settings
- Backup/restore issues
- Profile management
- Management/Reporting
- Wireless/Bluetooth issues
- E-discovery
- What happens if the device is lost/stolen?
  - Remote wipe?

VA SCAN 2011

Hardening Recommendations

VA SCAN 2011

- Laptops
  - At a minimum, encrypt the hard drive
    - TrueCrypt
    - PGP Disk
    - BitLocker
  - Biometrics
- Wireless
  - Two-factor authentication
  - 802.1x
  - VPN

VA SCAN 2011

- Labs, public access
  - Network Access Control (NAC)
  - 802.1x
- Remote Devices
  - Use SSH instead of Telnet for out-of-band access
    - Limit source IP address whenever possible
  - Always require HTTPS when available
  - Change all default SNMP community strings and other passwords
  - Don't allow access to common remote control programs from the outside
    - Citrix, VNC, PCAnywhere, DameWare, Terminal Services

VA SCAN 2011

- General Recommendations
  - Make sure you have secure build configurations for all infrastructure devices
  - Whenever possible, limit the source of resource requests to the smallest number possible
    - SNMP, SSH
  - With VPNs, configure access lists to limit exposure

VA SCAN 2011

- General Recommendations
  - With VPNs, configure access lists to limit exposure
    - Don't allow free range of internal networks
  - Identify the user as soon as possible and apply access policies
  - Remove all unnecessary protocols, apps, etc.
  - Perform periodic penetration tests to ensure that all low hanging fruit have been removed

VA SCAN 2011

Policies & Procedures (P&P)

VA SCAN 2011

- Be sure to start with documented, enforceable policies
- Without upper management buy-in, don't bother trying to enforce the policies
- Make sure you have a mobile device management policy
- Update and re-educate every year

VA SCAN 2011

Wrap-Up

VA SCAN 2011

- Remote access is one of the oldest IT technologies in use today
- It is well understood -- but occasionally implemented without security in mind
- Be sure to test often and update configurations and P&P documents as necessary
- Remember there are more potential attackers outside your security perimeter than inside

VA SCAN 2011

Q&A