WIRELESS NETWORK SECURITY

SUMMARY AND CONCLUSIONS

AGENDA

- [ ] REVEIW
- [ ] RECOMMENDATIONS
- [ ] COMMENTS

REVIEW

REVIEW

- [ ] WIRELESS
  - [ ] RADIO FREQUENCY SPECTRUM
  - [ ] PROPERTIES OF RADIO WAVES
  - [ ] 802.11 STANDARDS, A/B/G, WIMAX
  - [ ] POINT-TO-POINT NETWORKS
  - [ ] MESH NETWORKS

REVIEW

- [ ] ACCESS POINTS TO BUILD WIRELESS NETWORKS
  - [ ] CONFIGURATION ACCESS POINTS
  - [ ] ESSID, MODE, CHANNELS, SNMP
  - [ ] ACCESS-POINT MODE V. "STATION"/CLIENT MODE
  - [ ] POWER SETTINGS
  - [ ] BRIDGING
  - [ ] WPA2 POINT-TO-POINT LINKS
  - [ ] UBIQUITI ACCESS POINTS

REVIEW

- [ ] EXTENDING WIRELESS NETWORKS
  - [ ] ADDING ADDITIONAL ACCESS POINTS
  - [ ] SITE DEPLOYMENT ISSUES
  - [ ] POWER/ENVIRONMENTAL CONCERNS
- [ ] CAPTIVE PORTAL APPROACHES
  - [ ] USING MONOWALL OR NOCAT TO SECURE A WIRELESS NETWORK

REVIEW

- [ ] MONOWALL
  - [ ] A GUI-BASED CAPTIVE PORTAL/FIREWALL SOLUTION
  - [ ] INEXPENSIVE (FREE!)
  - [ ] SUITABLE FOR WIRELESS CAPTIVE PORTALS
  - [ ] RUNS ON INEXPENSIVE HARDWARE

REVIEW

- NETWORK PROTOCOLS
  - THE MAC LAYER, "LAYER2" IS SIMILAR IN BOTH WIRED AND WIRELESS NETWORKS
  - THERE IS NO SECURITY BUILT INTO THE ETHERNET OR MAC LAYER
  - BECAUSE OF THIS, ARP MECHANISMS ARE SUBJECT TO TAMPERING, POISONING, MASQUERADING ATTACKS

REVIEW

- TCP/IP
  - SIMILARLY, TCP/IP HAS NO SECURITY BUILT INTO THE PROTOCOLS
  - BECAUSE OF THAT IP ADDRESSES ARE ALSO SUBJECT TO FORGERY. TCP/IP CAN ALSO BE TAMPERED WITH, ESPECIALLY FOR DENIAL OF SERVICE ATTACKS
  - LEARNED UNIX TOOLS FOR NETWORK CONFIGURATION: IFCONFIG, NETSTAT, ARP, ARPING, PING, TRACEROUTE, MTR, TCPTRACEROUTE

REVIEW

- [ ] BACKTRACK
  - [ ] LEARNED ABOUT LIVE-CD DISTRIBUTIONS
  - [ ] LOTS OF TOOLS ON THE BACKTRACK LIVE-CD
  - [ ] INSTALLING BACKTRCK ON USB
  - [ ] WIRELESS CONFIGURATION TOOLS: IFCONFIG, IWCONFIG, IWLIST, DHCPCD

REVIEW

- NETWORK DESIGN
  - ADDING WIRELESS NETWORKS AND ADDITIONAL SECURITY SYSTEMS WILL REQUIRE NETWORK DESIGN
  - THIS REQUIRES CAREFUL CONSIDERATION OF THE TOPOLOGY OF THE EXISTING NETWORK
  - IT ALSO REQUIRES UNDERSTANDING WHAT THE GOAL IS FOR THE NEW DESIGN

REVIEW

- NETWORK DESIGN (CONTINUED)
  - SECURITY "ZONES" CAN BE CREATED, OUTSIDE, IN A DMZ, OR INSIDE OF NETWORKS. EX: GUEST V. INTERNAL
  - CAPTIVE PORTALS (AUTHENTICATION GATEWAYS) CAN BE USED TO CREATE THE EDGE OF A SECURITY ZONE
  - ACCOUNT MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL ARE CRITICAL COMPONENTS IN A CAPTIVE PORTAL (AUTHENTICATION GATEWAY)

REVIEW

- [ ] WIRELESS SECURITY STANDARDS
  - [ ] OLDER WIRELESS ENCRYPTION STANDARDS HAVE NOT PERFORMED WELL
  - [ ] WEP IS CRACKABLE USING A NUMBER OF TOOLS
  - [ ] WPA2 APPEARS TO BE THE BEST OF THE CURRENTLY AVAILABLE STANDARDS
  - [ ] WPA2 MAY NOT BE SUPPORTED ON ALL OF YOUR CLIENT MACHINES
  - [ ] A CERTIFICATE/PKI SYSTEM MAY PROVIDE ADDITIONAL SUPPORT FOR AN IMPLEMENTATION

REVIEWS

- TRAFFIC ANALYSIS
  - A NUMBER OF FREE TOOLS ARE AVAILABLE
  - THESE CAN BE USED TO MONITOR THE CONDITION OF YOUR NETWORK
  - THEY CAN ALSO BE USED TO DO FORENSICS AFTER A BREAKIN HAS OCCURRED
  - FLOWTOOLS, WIRESHARK, AND NTOP ARE COMMONLY USED BY MANY NETWORK ENGINEERS

REVIEW

- ☐ WIRELESS TOOLS
- ☐ NETSTUMBLER CAN BE USED TO MAP OUT THE STATE OF THE WIRELESS NETWORK
- ☐ KISMET CAN BE USED TO ANALYZE THE WIRELESS TRAFFIC IN MORE DETAIL
- ☐ INEXPENSIVE SPECTRUM ANALYSIS TOOLS, SUCH AS WISPY, CAN BE USED TO ANALYZE RADIO ISSUES

REVIEW

- [ ] UBUNTU
  - [ ] POPULAR, EASY-TO-USE LINIX DISTRIBUTION
  - [ ] PACKAGE MANAGEMENT USING: APT-GET, APT-CACHE, DPKG
  - [ ] USE OF THE ROOT ACCOUNT USING: SUDO, SUDO -S
  - [ ] START/STOP SERVICE USING: /ETC/INIT.D/

REVIEW

- ☐ INFORMATION SECURITY CONCEPTS
- ☐ INFORMATION SECURITY RESOURCES
- ☐ NETWORK SECURITY
- ☐ NETWORK ACCESS CONTROL

REVIEW

- NETWORK ACCESS CONTROL
  - NAC SYSTEMS ARE STARTING TO APPEAR THAT BUILD COMPLEX ACCESS CONTROL MECHANISMS
  - SIMPLER ACCESS CONTROL MECHANISMS ARE POSSIBLE
  - PROXIES, SSL VPNS, AND IPSEC VPNS ARE A SIMPLE SOLUTION TO THIS PROBLEM IN SOME CASES
  - CAPTIVE PORTALS (AUTHENTICATION GATEWAYS) PROVIDE MOST OF THE BENEFITS OF NAC, WITHOUT THE HIGH COSTS AND COMPLEXITY

REVIEW

- [ ] NETWORK ATTACKS
  - [ ] ATTACK RESOURCES: CONFERENCES, WEBSITES, MAGAZINES
  - [ ] ATTACK TYPES
    - [ ] DENIAL OF SERVICE
    - [ ] ARP SPOOFING
    - [ ] MAN-IN-THE-MIDDLE
    - [ ] PHISHING ATTACKS
  - [ ] ATTACK TOOLS: DSNIFF, ETTERCAP, AIRCRACK, AIREPLAY

REVIEW

- ☐ NMAP, NESSUS, AND SNORT
  - ☐ VULNERABILITY ANALYSIS CONCEPTS
  - ☐ INTRUSION DETECTION CONCEPTS
  - ☐ THE USE OF OPEN-SOURCE TOOLS

RECOMMENDATIONS

RECOMMENDATIONS

- ☐ MONITOR YOUR NETWORK
  - ☐ MANAGE YOUR ACCESS POINTS
  - ☐ GRAPH NETWORK STATISTICS
  - ☐ DEPLOY A FLOWTOOLS OR MONITORING STATION

RECOMMENDATIONS

- [ ] APPLY ACCESS CONTROLS WHERE NECESSARY
  - [ ] CAPTIVE PORTALS WORK WELL TO SECURE OPEN WIRELESS NETWORKS

RECOMMENDATIONS

- ☐ MONITOR YOUR WIRELESS ENVIRONMENT
  - ☐ LOOK FOR ROGUE ACCESS POINTS WITH NETSTUMBLER
  - ☐ WATCH OUT FOR ROGUE DHCP SERVERS
  - ☐ ADDRESS ROGUE AP ISSUES QUICKLY

RECOMMENDATIONS

- [ ] ENCRYPTION
  - [ ] USE ENCRYPTION WHERE IT MAKES SENSE
  - [ ] USE WPA2 OR SIMILAR SOLUTIONS
  - [ ] USE SSL-VPN AND IPSEC VPNS, AND SSH
  - [ ] USE END-TO-END ENCRYPTION, AND PAY ATTENTION TO DATA SECURITY: PGP, AND OTHER TOOLS

RECOMMENDATIONS

- [ ] ADVANCED NETWORK SETTINGS
  - [ ] USE VLANS TO SEGMENT SUBNETS
  - [ ] ENABLE "ARP INSPECTION" OR "PORT-SECURITY" ON CHALLENGING SUBNETS
  - [ ] ENABLE "DHCP SNOOPING" TO LIMIT THE DAMAGE FROM ROGUE DHCP SYSTEMS
  - [ ] STATIC ARP ON SOME CRITICAL DEVICES

RECOMMENDATIONS

- ☐ VULNERABILITY SCANNING
  - ☐ PERORM REGULAR SCANS OF YOUR NETWORK
  - ☐ APPLY PATCHES
  - ☐ SUPPORT ANTI-VIRUS FIREWALL SOFTWARE
  - ☐ USE IDS TO DETECT RECENT KNOWN ATTACKS
  - ☐ EDUCATE YOUR USERS

COMMENTS

- ☐ FEEDBACK IS WELCOME
- ☐ MORE LAB TIME?
- ☐ MORE TIME ON SITE PLANNING AND DEPLOYMENT LABS?
- ☐ MORE TIME ON MESH NETWORKING?
- ☐ OTHER TYPES OF WIRELESS TECHNOLOGY?
- ☐ MORE TIME ON DEMONSTRATING CAPTIVE PORTALS?

COMMENTS

THANK YOU!