Appendix G

PENETRATION TESTING TEMPLATE

Arhont Ltd Wireless Network Security and Stability Audit Checklist Template

Date: _____/______/_______
Customer: ___________________

1 Reasons for an audit:

network design ❑

preventive / hardening ❑

network operations issues ❑

suspected intrusion ❑

2 Preliminary investigations:

network administrator: ______________________________

familiarity with wireless networking	□	familiarity with wireless security	□
presence of wireless security policy	□	presence of overall security policy	□
wireless network position information found online	□	security officer or security system administrator present	□

resource: ______________________________

3 Wireless site survey:

network type	802.11 DSSS	□	802.11 FHSS	□
	802.11b DSSS	□	802.11a DSSS	□
	802.11g DSSS	□	802.15 Bluetooth	□
	802.16 Broadband	□	HomeRF	□

other: __________________________

network structure	Infrastructure/ Managed	□	Independent/ Ad-Hoc	□

Other __________________________

network topology	point-to-multipoint	□	point-to-point	□

Highest Fresnel zone diameter (if applicable)_______

Estimated power output IR _____ EIRP _____

Network coverage zone mapping

See the included/ signed map

Point-to-point link distance ___

Antenna types deployed _________________________

Antenna polarization Vertical ❑ Horizontal ❑

SNR / signal strength value

point-to-point bridge___

typical clients position ___

Peak usage network bandwidth

point-to-point bridge ___

typical clients position___

DSSS network frequencies / channels _____

Number of access points deployed _____

Access points make __________________

Number of wireless hosts present _____

802.11 layer 2 traffic baselining

beacons per min ___ probe requests per min ___

probe responses per min ___ deassociate frames per min ___

Deauthenticate frames per min ___ reassociate frames per min ___

authenticate frames per min ___ ATIM frames per min ___

data packets per min (peak)___ 802.11 frame size (bytes) ___

Fragments per minute ___ Collisions per minute ___

rants per minute ___ giants per minute ___

RTS/CTS present ___ PCF present / superframes ___

IAPP running ___

Network ESSIDs present:

ESSID ____________________ Channel

ESSID ____________________ Channel

ESSID ____________________ Channel

Miscs. Host roaming enabled □ Load balancing enabled □

4 Network security features present:

Close ESSIDs □

MAC filtering □ explicit deny □
explicit allow □

Protocol filtering □
filtered protocols ____________________________

WEP
key size ___ static or dynamic ___
key rotation frequency ___ TKIP implemented ___
other WEP enhancements ______________________________

Authentication system open □
mixed □ close □

802.1x authentication
EAP type ____________________________
User database type ____________________________
802.1x-based WEP key rotation □
ESSID/MAC EAP authentication □

Centralized authentication implemented

Kerberos v4 □   RADUIS □

Kerberos v5 □   TACACS □

TACACS version ___

Layer 3 VPN implemented □

VPN type and mode ______________________________

---

key exchange   shared secret □

asymmetric crypto □   DH asymmetric crypto □

X.509 certificates □   other □

---

ciphers used   symmetric ___

message digest ___   assymmetric ___

key size   symmetric ___

message digest ___   assymmetric ___

---

tunneling implemented   IPSec AH □

PPTP □   IPSec ESP □

L2F □   L2TP □

CIPE □   GRE □

IP-IP □   VTP □

DVS □   ATMP □

Other ___   MIN-IP-IP □

Higher layers security protocols used

S/MIME □

SCP □

Other ___

SSHv1 □

SSHv2 □

HTTPS □

PGP/GNUPG □

Wireless authentication gateway ______________________________

gateway type ______________________________

Proper wired/wireless network separation

Type of the gateway/firewall ______________________________

Gateway malware filtering present □ Gateway SPAM filtering present □

Access points management from the wireless side isenabled□

restricted □ disabled □

Connections between wireless peers deniedWireless peers have firewalling capability

---

Wireless IDS present

Remote sensors present

IDS type ________________

Sensor type ________________

Number of sensors ___

Centralized logging present

Logging is done over UDP □ TCP □

Log review frequency ___

Wired IDS present □ IDS type _______________

Remote sensors present □ Sensor type _______________

Number of sensors___

Honeypots deployed

wireless □ wired □

comments ______________________________

5 Network problems / anomalies detected:

connection loss □ excessive collisions □

common RF issues near/far problem □

hidden node □ interference □

interference type narrowband □

wideband □ channel overlapping □

interference source ______________________________

abnormal frames ______________________________

excessive amount of management / control frames

excessive frame type ___ excessive frame structure ___ rogue Aps AP1________________________

AP3________________________ AP2________________________

rogue APs MACs AP1________________________

AP3________________________ AP2________________________

rogue ApsIPs AP1________________________

AP3________________________ AP1________________________

rogue APs channels AP1________________________

AP3________________________ AP2________________________

rogue APs ESSIDs AP1________________________

AP3________________________ AP2________________________

rogue APs location AP1________________________

AP3________________________ AP2________________________

rogue AP signal strength AP1________________________

AP3________________________ AP2________________________

rogue APs use WEP AP1________________________

AP3________________________ AP2________________________

rogue APs WEP keys AP1________________________

AP3________________________ AP2________________________

rogue APs origin intentional □

unknown □ unintentional □

rogue access points have associated hosts ❑

hosts associated (IP/MAC) ____________________________

____

other rogue wireless hosts detected ❑

number of hosts___

MAC __________________ IP ___________________

physically discovered rogue wireless devices PCMCIA client card ❑

USB wireless client ❑ CF client card ❑

other________________________________

Known signatures of wireless attack tools (version)

Netstumbler ___ Dstumbler ___

Windows XP scan ___ Wellenreiter ___

Airjack ___ Fata_jack ___

Man-in-the-middle attacks signs (Double MAC / IP addresses)

MiM1 ________________________ MiM2 _____________________

MiM3 _____________________ MiM4 _____________________

Out of sequence frames present (amount/time) _____/_____

Excessive Deassociate/deauthenticate frames

time ___ amount ___

channel ___

Exsessive RF noise strength ___

channel ___

Rogue DHCP servers present

IP ____________________ MAC _____________________

Atypical route advertisement (type/comments)

Type ____________________ Comments _______________

Type __________________ Comments _______________

Wireless DoS attack signs Management / control frames flood❑

frame types _______________ origin MAC ________________

Out-of-sequence frames

origin MAC __________________________

Excessive RF noise channel___

jamming device discovered ___ strength ___

comments ______________________________

Higher layer DoS attacks

Comments ____

Higher layer DoS attacks

Comments

Attacks against the access point detected

Comments ____

DoS attacks

Comments ____

brute-forcing attacks via SNMP ___

via SSH ___ via telnet ___

via other means ___ via Web interface___

Attacks against wireless hosts detected

Comments ____

Attacks directed at the wired hosts from the WLAN

Comments ____

Attacks directed at the hosts on the Internet

Comments ____

Attempts to send SPAM

Comments ____

6 Wireless Penetration Testing Procedure Outline

Maximum network discovery and fingerprinting distance with:

Built-in client card antenna ___ 2 dBi omnidirectional ___

15 dBi Yagi ___ 9 dBi directional ___

ESSID security

default ❑ company name ❑

closed ❑ address ❑

other relevant information ________________________________

Bypassing closed ESSID

closed ESSID value ________________________________

Bypassing MAC filtering

success with MAC ________________________________

Cracking WEP keys

key 1 ________________________________

key 2 ________________________________

key 3 ________________________________

key 4 ________________________________

cracking time ___ cracking tool ___

WEP cracking acceleration ❑ time saved ___

traffic injection tool ___ type of traffic injected ___

Brute-forcing 802.1x access

password guessed ________________________________

Wireless man-in-the-middle attacks ❑ Tool: ________________

layer 1 attack (comments) ________________________________

layer 2 attack (comments) ________________________________

DoS attack resilience / detection (comments)

wlan_jack ______________________________

fata_jack ______________________________

HostAP beacon flood ______________________________

Other attacks ______________________________

Wireless traffic interception / analysis

packets per minute ___

plaintext & plaintext authentication protocols detected

POP3 ☐

SMTP ☐

IMAP ☐

NNTP ☐

IRC ☐

PAP ☐

Telnet ☐

FTP ☐

HTTP ☐

Instant messengers ☐

SQL ☐

LDAP ☐

Other ______________________________

passwords/user credentials collected

username/password ______________________________

username/password ______________________________

username/password ______________________________

username/password ______________________________

weak encryption/vulnerable protocols detected

LM/ NTLMv1 SSHv1

Other ______________________________

passwords cracked

username/password ______________________________

username/password ______________________________

username/password ______________________________

username/password ______________________________

UNIX remote services ___ type ___

SMB/Windows shares on a wireless LAN________________________________

NFS shares detected ________________________________

DHCP traffic detected ________________________________

HSRP/VRRP traffic detected ________________________________

HSRP password ________________________________

VRRP authentication ________________________________

VRRP password ________________________________

CDP traffic detected ________________________________

CDP data gathered ________________________________

ICMP type 9/10 implem. □ RIPv1 running □

Unauthenticated routing protocols over wireless network

RIPv2 □ OSPF □

IGRP □ EIGRP □

IS-IS □ IPX RIP □

NLSP □ Other ________________________

Unauthenticated NTP traffic □ SNMP traffic □

SNMP communities found ___ SNMP version ___

NetBIOS over IPX traffic □ AppleTalk traffic □

DecNet traffic □ Banyan Vines traffic □

SNA traffic □Other _________________ □

Unencrypted remote administration traffic

VNC □ PCAnywhere □

Webmin □Other _________________ □

Remote X Server cookies □

Syslog traffic □ over UDP □

over TCP □

Passive OS fingerprinting ______________________________

Gateway discovery (IP) ______________________________

IDS host discovery ______________________________

ARP spoofing man-in-the-middle attack ______________________________

Switch CAM table flooding ______________________________

Route injection attacks ______________________________

ICMP route redirection ______________________________

DNS cache poisoning ______________________________

DHCP DoS attacks ______________________________

Tunneling protocols attack ______________________________

VPN enumeration ______________________________

VPN related attacks ______________________________

Active OS fingerprinting (nmap, xprobe, other) fingerprinted hosts (IP:OS)

____

Discovered backdoors / backchannel traffic______________________________

Banner grabbing and host penetration -penetrated hosts ()

IP/hostname:vulnerability ______________________________

IP/hostname:vulnerability ______________________________

IP/hostname:vulnerability ______________________________

Network / host DoS resilience testing

attack/host/result ______________________________

attack/host/result ______________________________

attack/host/result ______________________________

Egress filtering firewall testing from the wireless site

____

Physical security issues discovered ______________________________

7 Final recommendations:

Network Security Consultant
Network Security Consultant
Network Security Consultant