

# Appendix G

## PENETRATION TESTING TEMPLATE



### Arhont Ltd Wireless Network Security and Stability Audit Checklist Template

---

Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

Customer: \_\_\_\_\_

#### 1 Reasons for an audit:

---

- |                        |                          |                           |                          |
|------------------------|--------------------------|---------------------------|--------------------------|
| network design         | <input type="checkbox"/> | network operations issues | <input type="checkbox"/> |
| preventive / hardening | <input type="checkbox"/> | suspected intrusion       | <input type="checkbox"/> |
- 

Appendix G appears in the book "Wi-Foo: The Secrets of Wireless Hacking," ISBN 0321202171, copyright 2004. All rights reserved. This content is reprinted with permission from Addison-Wesley Professional.





**Appendix G • Penetration Testing Template**

**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 <input type="checkbox"/>	802.11 FHSS <input type="checkbox"/>
	802.11b DSSS <input type="checkbox"/>	802.11a DSSS <input type="checkbox"/>
	802.11g DSSS <input type="checkbox"/>	802.15 Bluetooth <input type="checkbox"/>
	802.16 Broadband <input type="checkbox"/>	HomeRF <input type="checkbox"/>

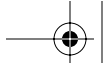
other: \_\_\_\_\_

network structure	Infrastructure/Managed <input type="checkbox"/>	Independent/Ad-Hoc <input type="checkbox"/>
	Other _____	

network topology	point-to-multipoint <input type="checkbox"/>	point-to-point <input type="checkbox"/>
------------------	--	---

Appendix G appears in the book "Wi-Foo: The Secrets of Wireless Hacking," ISBN 0321202171, copyright 2004. All rights reserved. This content is reprinted with permission from Addison-Wesley Professional.





**Appendix G • Penetration Testing Template**

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 \_\_\_\_\_

Appendix G appears in the book "Wi-Foo: The Secrets of Wireless Hacking," ISBN 0321202171, copyright 2004. All rights reserved. This content is reprinted with permission from Addison-Wesley Professional.



**Appendix G • Penetration Testing Template**

802.11 layer 2 traffic baselining

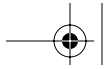
beacons per min	___	probe requests	
		per min	___
probe responses per min	___	deassociate frames per min	___
Deauthenticate frames		reassociate frames per min	___
per min	___		
authenticate frames		ATIM frames per min	___
per min	___		
data packets per min (peak)	___	802.11 frame size (bytes)	___
Fragments 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   

Appendix G appears in the book "Wi-Foo: The Secrets of Wireless Hacking," ISBN 0321202171, copyright 2004. All rights reserved. This content is reprinted with permission from Addison-Wesley Professional.



Appendix G • Penetration Testing Template

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

Appendix G appears in the book "Wi-Foo: The Secrets of Wireless Hacking," ISBN 0321202171, copyright 2004. All rights reserved. This content is reprinted with permission from Addison-Wesley Professional.



**Appendix G • Penetration Testing Template**

Centralized authentication implemented

- |                     |                          |        |                          |
|---------------------|--------------------------|--------|--------------------------|
| Kerberos v4         | <input type="checkbox"/> | RADIUS | <input type="checkbox"/> |
| Kerberos v5         | <input type="checkbox"/> | TACACS | <input type="checkbox"/> |
| TACACS version ____ |                          |        |                          |

Layer 3 VPN implemented

VPN type and mode \_\_\_\_\_

key exchange

- |                    |                          |                      |                          |
|--------------------|--------------------------|----------------------|--------------------------|
| asymmetric crypto  | <input type="checkbox"/> | shared secret        | <input type="checkbox"/> |
| X.509 certificates | <input type="checkbox"/> | DH asymmetric crypto | <input type="checkbox"/> |
|                    |                          | other                | <input type="checkbox"/> |

ciphers used

- |                |      |             |      |
|----------------|------|-------------|------|
| message digest | ____ | symmetric   | ____ |
|                |      | assymmetric | ____ |
| key size       |      | symmetric   | ____ |
| message digest | ____ | assymmetric | ____ |

tunneling implemented

- |       |                          |           |                          |
|-------|--------------------------|-----------|--------------------------|
|       |                          | IPSec AH  | <input type="checkbox"/> |
| PPTP  | <input type="checkbox"/> | IPSec ESP | <input type="checkbox"/> |
| L2F   | <input type="checkbox"/> | L2TP      | <input type="checkbox"/> |
| CIPE  | <input type="checkbox"/> | GRE       | <input type="checkbox"/> |
| IP-IP | <input type="checkbox"/> | VTP       | <input type="checkbox"/> |
| DVS   | <input type="checkbox"/> | ATMP      | <input type="checkbox"/> |
| Other | ____                     | MIN-IP-IP | <input type="checkbox"/> |



### Appendix G • Penetration Testing Template

Higher layers security protocols used

SSHv1	<input type="checkbox"/>
S/MIME	<input type="checkbox"/>
SCP	<input type="checkbox"/>
Other	_____

SSHv2	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>
PGP/GNUPG	<input type="checkbox"/>

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 is enabled   
 restricted  disabled

Connections between wireless peers denied \_\_\_\_\_  
 Wireless peers have firewalling capability \_\_\_\_\_

Wireless IDS present      IDS type      \_\_\_\_\_  
 Remote sensors present      Sensor type      \_\_\_\_\_  
    Number of sensors      \_\_\_\_\_

Appendix G appears in the book "Wi-Foo: The Secrets of Wireless Hacking," ISBN 0321202171, copyright 2004. All rights reserved. This content is reprinted with permission from Addison-Wesley Professional.



### Appendix G • Penetration Testing Template

#### 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 \_\_\_\_\_



### Appendix G • Penetration Testing Template

---

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 <input type="checkbox"/>
	unknown <input type="checkbox"/> unintentional <input type="checkbox"/>

---



**Appendix G • Penetration Testing Template**

---

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 \_\_\_\_\_

---

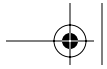
Out of sequence frames present (amount/time) \_\_\_\_\_/\_\_\_\_\_  
Excessive Deassociate/deauthenticate frames  
time \_\_\_\_\_ amount \_\_\_\_\_  
channel \_\_\_\_\_  
Excessive RF noise strength \_\_\_\_\_  
channel \_\_\_\_\_

Rogue DHCP servers present  
IP \_\_\_\_\_ MAC \_\_\_\_\_

---

Appendix G appears in the book "Wi-Foo: The Secrets of Wireless Hacking," ISBN 0321202171, copyright 2004. All rights reserved. This content is reprinted with permission from Addison-Wesley Professional.





### Appendix G • Penetration Testing Template

---

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

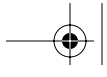
Comments \_\_\_\_\_

Attempts to send SPAM

Comments \_\_\_\_\_

---





**Appendix G • Penetration Testing Template**

## 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) \_\_\_\_\_





### Appendix G • Penetration Testing Template

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  Telnet

SMTP  FTP

IMAP  HTTP

NNTP  Instant messengers

IRC  SQL

PAP  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 \_\_\_\_\_

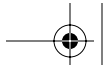
username/password \_\_\_\_\_

username/password \_\_\_\_\_

username/password \_\_\_\_\_

Appendix G appears in the book "Wi-Foo: The Secrets of Wireless Hacking," ISBN 0321202171, copyright 2004. All rights reserved. This content is reprinted with permission from Addison-Wesley Professional.





### Appendix G • Penetration Testing Template

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 \_\_\_\_\_

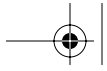
ICMP type 9/10 implem.       RIPv1 running

#### Unauthenticated routing protocols over wireless network

RIPv2	<input type="checkbox"/>	OSPF	<input type="checkbox"/>
IGRP	<input type="checkbox"/>	EIGRP	<input type="checkbox"/>
IS-IS	<input type="checkbox"/>	IPX RIP	<input type="checkbox"/>
NLSP	<input type="checkbox"/>	Other _____	
Unauthenticated NTP traffic	<input type="checkbox"/>	SNMP traffic	<input type="checkbox"/>
SNMP communities found	_____	SNMP version	_____
NetBIOS over IPX traffic	<input type="checkbox"/>	AppleTalk traffic	<input type="checkbox"/>
DecNet traffic	<input type="checkbox"/>	Banyan Vines traffic	<input type="checkbox"/>
SNA traffic	<input type="checkbox"/>	Other _____	<input type="checkbox"/>
Unencrypted remote administration traffic			
VNC	<input type="checkbox"/>	PCAnywhere	<input type="checkbox"/>
Webmin	<input type="checkbox"/>	Other _____	<input type="checkbox"/>
Remote X Server cookies	<input type="checkbox"/>		
Syslog traffic	<input type="checkbox"/>	over UDP	<input type="checkbox"/>
		over TCP	<input type="checkbox"/>

Appendix G appears in the book "Wi-Foo: The Secrets of Wireless Hacking," ISBN 0321202171, copyright 2004. All rights reserved. This content is reprinted with permission from Addison-Wesley Professional.





### Appendix G • Penetration Testing Template

---



---

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 \_\_\_\_\_

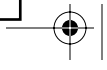
attack/host/result \_\_\_\_\_

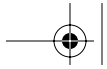
Egress filtering firewall testing from the wireless site  
\_\_\_\_\_

Physical security issues discovered \_\_\_\_\_

---

Appendix G appears in the book "Wi-Foo: The Secrets of Wireless Hacking," ISBN 0321202171, copyright 2004. All rights reserved. This content is reprinted with permission from Addison-Wesley Professional.





---

**Appendix G • Penetration Testing Template**

---

## **7 Final recommendations:**

---

---

---

---

---

---

---

---

---

---

Network Security Consultant  
Network Security Consultant  
Network Security Consultant

---



Appendix G appears in the book "Wi-Foo: The Secrets of Wireless Hacking," ISBN 0321202171, copyright 2004. All rights reserved. This content is reprinted with permission from Addison-Wesley Professional.

