Johnson, Darren

From: OG150 Device[redacted]
Sent: Monday, 13 May 2013 8:23 PM
To: OG150-DISTRIBUTION-LIST
Subject: OG150 Security Report.

The OG150 has completed several automated tests that will provide the user with useful information that could be used to launch an attack against the IT infrastructure. The results of this penetration test is detailed within this Security Report.

Each test will be documented using the format shown below;

TITLE
DESCRIPTION
VULNERABILITY
EXPLOIT
COUNTERMEASURE
TEST RESULTS

A brief description of the key terms used within this Security Report are provided below for reference.

VULNERABILITY:
A vulnerability is a software, hardware or procedural weakness that may provide an attacker the open door he is looking for to enter a computer/network and have unauthorised access to resources within the environment.

EXPLOIT:
An exploit is a piece of software or sequence of commands that takes advantage of a vulnerability in order to cause unintended or unanticipated behaviour to occur on computer/network software or hardware. This behavior frequently includes such things as gaining control of a computer/network system or allowing privilege escalation or a denial-of-service attack.

COUNTERMEASURE:
A countermeasure may be a software configuration, a hardware device or a procedure that eliminates a vulnerability or reduces the likelihood of someone exploiting a vulnerability.

TITLE: DISPLAY OG150 IP DETAILS
DESCRIPTION: Display the IP address details assigned to the OG150 ethernet0 interface via DHCP. The IP address, Subnet Mask, Default Gateway and DNS information is listed.
VULNERABILITY: This is part of the reconnaissance phase, where the attacker can identify information such as the IP subnet, the default gateway and DNS configuration for the local network.
EXPLOIT: Although there is not a direct exploit for this vulnerability, the information yielded can be used in more advanced tests later.
COUNTERMEASURE: To prevent an unauthorised device from receiving DHCP assigned IP address information, the best countermeasure is to use IEEE 802.1x port authentication. Other, less desirable, options include shutting down the switch interface or disabling DHCP services.
TEST RESULTS:

```
eth0      Link encap:Ethernet  HWaddr 14:CF:92:[redacted]
inet addr:192.168.11.49  Bcast:192.168.11.255  Mask:255.255.255.0
```

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.11.1    0.0.0.0         UG    0      0        0 eth0

DNS Server: 8.8.8.8 DNS Server: 8.8.4.4 Domain Name: [redacted]
```

TITLE: VERIFY ICMP CONNECTIVITY TO THE INTERNET
DESCRIPTION: The OG150 will try to ping www.google.com. This will ascertain if the firewall permits ICMP pings to the Internet.
VULNERABILITY: If ICMP (ping) traffic is permitted, the user could leverage this ‘security hole’ to launch additional attacks.
EXPLOIT: The user can send IP traffic hidden inside an ICMP tunnel. The firewall will only see ICMP traffic and the user can launch all kinds of attacks which the firewall has no visibility of.
COUNTERMEASURE: ICMP pings are commonly used to troubleshoot connectivity to the Internet. It is advisable to configure the firewall to ONLY permit ICMP pings from pre-defined devices, for example devices used by the IT team. This facilitates troubleshooting by the IT team, whilst denying everyone else ICMP access to the Internet.
TEST RESULTS:

```
PING www.google.com (74.125.237.145): 56 data bytes
64 bytes from 74.125.237.145: seq=0 ttl=52 time=46.640 ms
64 bytes from 74.125.237.145: seq=1 ttl=52 time=47.063 ms
64 bytes from 74.125.237.145: seq=2 ttl=52 time=46.643 ms
64 bytes from 74.125.237.145: seq=3 ttl=52 time=46.580 ms
64 bytes from 74.125.237.145: seq=4 ttl=53 time=48.421 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max =
46.580/47.069/48.421 ms
```

TITLE: TRACEROUTE TO THE INTERNET
DESCRIPTION: The OG150 will attempt to traceroute to www.google.com.
VULNERABILITY: This is a form of reconnaissance that allows the user to map out the network topology inside the target infrastructure.
EXPLOIT: Although there is not a direct exploit for this vulnerability, the information yielded can be used in more advanced tests later. An understanding of the target network topology will allow more focussed attacks against the IT infrastructure.
COUNTERMEASURE: It is difficult to prevent traceroute within the internal network without using IEEE 802.1x port authentication or ACLs (Access Control Lists) on the routers and/or switches. To prevent traceroute traffic that traverses the firewall you should note that, by default, UDP port 33434 is used as the base port number. Each additional routing hop increments the UDP port by +1 – therefore routing hop 2 uses UDP port 33435, routing hop 3 uses UDP port 33436, etc. Although firewall rules can be configured to restrict this access based on the UDP information provided, the default port(s) can be easily changed by the user.
TEST RESULTS:

```
traceroute to www.google.com (74.125.237.147), 30 hops max, 38 byte packets
1  [redacted] ([redacted])  0.842 ms  0.872 ms  0.795 ms
2  [redacted] ([redacted])  30.532 ms  30.519 ms  31.065 ms
3  172.18.69.98 (172.18.69.98)  30.802 ms  30.803 ms  31.325 ms
4  172.18.241.101 (172.18.241.101)  39.472 ms  34.166 ms  34.889 ms
5  bundle-ether10.cha45.brisbane.telstra.net (203.45.53.237)  38.568 ms  34.476 ms  33.665
ms
6  bundle-ether2.cha-core4.brisbane.telstra.net (203.50.44.13)  32.735 ms  30.269 ms
32.054 ms
```

```
7  bundle-ether11.ken-core4.sydney.telstra.net (203.50.11.72)  47.702 ms  50.164 ms
47.608 ms
8  bundle-ether1.ken39.sydney.telstra.net (203.50.6.146)  58.364 ms  58.342 ms  47.964 ms
9  72.14.198.54 (72.14.198.54)  169.053 ms  164.672 ms  156.541 ms
10  66.249.95.226 (66.249.95.226)  47.661 ms  46.984 ms  47.000 ms
11  72.14.237.137 (72.14.237.137)  46.377 ms  47.336 ms  49.065 ms
12  syd01s13-in-f19.1e100.net (74.125.237.147)  48.575 ms  *  49.320 ms
```

TITLE: DISCOVER HOSTS AND SERVICES ON THE LOCAL NETWORK USING NMAP
DESCRIPTION: The OG150 will perform an NMAP ‘Quick Scan’ against the OG150s local (ethernet0) IP subnet.
VULNERABILITY: This information yields extremely useful information about the users and devices that reside on the same IP subnet as the OG150 (ethernet0 interface). Please Note: Although this test is restricted to the OG150s local IP subnet, this test can easily be scaled to scan additional networks as required.
EXPLOIT: Although there is not a direct exploit for this vulnerability, the user can use this information to target specific users and/or devices. The user may notice a specific service operating on a device and attempt to compromise that device using a known vulnerability associated with that service. An additional attack vector may include using ARP poisoning against a local server to capture passwords in a classic MITM (Man In The Middle) style attack.
COUNTERMEASURE: The best way to prevent NMAP scanning within the internal network is to use using IEEE 802.1x port authentication. An alternative, less desirable, option is to use Private VLANs.
TEST RESULTS:

```
Starting Nmap 6.01 ( http://nmap.org ) at 2013-05-13 20:14 EST Nmap scan report for
192.168.11.1 Host is up (0.0016s latency).
Not shown: 97 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
443/tcp open  https
MAC Address: 58:BC:27:D2:29:92 (Cisco Systems) Device type: WAP
Running: Cisco IOS 12.X
OS CPE: cpe:/h:cisco:aironet_ap1241n cpe:/o:cisco:ios:12.4 OS details: Cisco Aironet AIR-
AP1141N WAP (IOS 12.4) Network Distance: 1 hop

Nmap scan report for 192.168.11.44
Host is up (0.00028s latency).
All 100 scanned ports on 192.168.11.44 are filtered MAC Address: 5C:26:0A:2C:D4:98 (Dell)

Nmap scan report for 192.168.11.49
Host is up (0.00036s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
Device type: storage-misc|WAP|media device|general purpose|webcam|router Running (JUST
GUESSING): LaCie Linux 2.6.X (96%), Netgear embedded (96%), Western Digital embedded
(96%), Linux 2.6.X|3.X|2.4.X (96%), AXIS Linux 2.6.X (95%), Linksys embedded (94%), Nokia
Linux 2.6.X (92%) OS CPE: cpe:/o:lacie:linux:2.6 cpe:/o:linux:kernel:2.6
cpe:/o:axis:linux:2.6 cpe:/h:linksys:wrv54g cpe:/o:linux:kernel:3 cpe:/h:linksys:rv042
cpe:/o:linux:kernel:2.6.21 cpe:/o:linux:kernel:2.4 Aggressive OS guesses: LaCie d2 NAS
device (Linux 2.6) (96%), Netgear DG834G WAP or Western Digital WD TV media player (96%),
Linux 2.6.17 - 2.6.28 (96%), Linux 2.6.22 (Ubuntu 7.10) (96%), Linux 2.6.24 (95%), AXIS
211A Network Camera (Linux 2.6) (95%), AXIS 211A Network Camera (Linux 2.6.20) (95%),
Linksys WRV54G WAP (94%), Linux 2.6.16 (94%), Linux 2.6.32 - 3.0 (94%) No exact OS matches
for host (test conditions non-ideal).
Network Distance: 0 hops

Warning: 192.168.11.248 giving up on port because retransmission cap hit (2).
Warning: 192.168.11.247 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.11.247
Host is up (0.0019s latency).
Not shown: 57 closed ports, 40 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
443/tcp open  https
MAC Address: 00:00:5E:00:01:01 (USC Information Sciences Inst) Device type: router|WAP
Running: Cisco IOS 12.X|15.X
OS CPE: cpe:/h:cisco:836_router cpe:/h:cisco:890_router cpe:/h:cisco:1751_router
cpe:/o:cisco:ios:12 cpe:/h:cisco:1841_router cpe:/o:cisco:ios:15
cpe:/h:cisco:aironet_ap1241n cpe:/o:cisco:ios:12.4 OS details: Cisco 836, 890, 1751, 1841,
or 2800 router (IOS 12.4 - 15.1), Cisco Aironet AIR-AP1141N WAP (IOS 12.4) Network
Distance: 1 hop

Nmap scan report for 192.168.11.248
Host is up (0.0018s latency).
Not shown: 72 closed ports
PORT      STATE    SERVICE
9/tcp     filtered discard
22/tcp    open     ssh
23/tcp    open     telnet
26/tcp    filtered rsftp
79/tcp    filtered finger
119/tcp   filtered nntp
389/tcp   filtered ldap
443/tcp   open     https
444/tcp   filtered snpp
465/tcp   filtered smtps
544/tcp   filtered kshell
631/tcp   filtered ipp
873/tcp   filtered rsync
1027/tcp  filtered IIS
1900/tcp  filtered upnp
2121/tcp  filtered ccproxy-ftp
3000/tcp  filtered ppp
5000/tcp  filtered upnp
5009/tcp  filtered airport-admin
5190/tcp  filtered aol
5357/tcp  filtered wsdapi
5432/tcp  filtered postgresql
7070/tcp  filtered realserver
8000/tcp  filtered http-alt
8081/tcp  filtered blackice-icecap
9999/tcp  filtered abyss
32768/tcp filtered filenet-tms
49153/tcp filtered unknown
MAC Address: 00:00:0C:07:AC:01 (Cisco Systems) Device type: router|WAP
Running: Cisco IOS 12.X|15.X
OS CPE: cpe:/h:cisco:836_router cpe:/h:cisco:890_router cpe:/h:cisco:1751_router
cpe:/o:cisco:ios:12 cpe:/h:cisco:1841_router cpe:/o:cisco:ios:15
cpe:/h:cisco:aironet_ap1241n cpe:/o:cisco:ios:12.4 OS details: Cisco 836, 890, 1751, 1841,
or 2800 router (IOS 12.4 - 15.1), Cisco Aironet AIR-AP1141N WAP (IOS 12.4) Network
Distance: 1 hop
```

```
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 65.18 seconds
```

TITLE: CDP (Cisco Discovery Protocol) SNOOPING

DESCRIPTION: The OG150 will listen, capture and display any CDP (Cisco Discovery Protocol) announcements. The test will run for 60 seconds based on the default hello timer for CDP. Please Note: If no CDP messages were received during this interval, there will be no output displayed below.

VULNERABILITY: The information contained within CDP announcements leaks important detail relating to the Cisco network devices being deployed. Network devices may include Cisco switches, wireless access-points and routers.

EXPLOIT: Although there is not a direct exploit for this vulnerability, the user now has possession of very sensitive information relating to the Cisco network devices, such as the hardware model, software version in use, IP addresses being used, etc. Armed with this information, the user can launch attacks. For example, the user can research vulnerabilities relating to the software version advertised by CDP and launch attacks to compromise the network device.

COUNTERMEASURE: CDP is a useful tool, however the default settings leak sensitive information. The best countermeasure for this is to disable CDP on all user facing switch interfaces - in other words CDP is only enabled on interfaces that connect to other network devices such as switch-to-switch uplinks.

TEST RESULTS:

```
20:15:54.632382 CDPv2, ttl: 180s, checksum: 692 (unverified), length 354 Device-ID (0x01),
length: 19 bytes: '[redacted]'
Version String (0x05), length: 247 bytes:
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(24)T, RELEASE
SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2009
by Cisco Systems, Inc.
Compiled Wed 25-Feb-09 15:36 by prod_rel_team Platform (0x06), length: 10 bytes: 'Cisco
1841'
Address (0x02), length: 22 bytes: IPv4 (2) [redacted] IPv4 (1) [redacted] Port-ID (0x03),
length: 15 bytes: 'FastEthernet0/0'
Capability (0x04), length: 4 bytes: (0x00000029): Router, L2 Switch, IGMP snooping VTP
Management Domain (0x09), length: 0 bytes: ''
```

TITLE: FHRP (First Hop Redundancy Protocol) SNOOPING

DESCRIPTION: The OG150 will listen, capture and display FHRP (First Hop Redundancy Protocol) messages. FHRP’s provide redundancy for the default gateway on a LAN or VLAN. HSRP (Hot Standby Router Protocol) and VRRP (Virtual Router Redundancy Protocol) are commonly used FHRP’s used in enterprises. The test will run for 10 seconds based on the default HSRP and VRRP timers. Please Note: If no FHRP messages were received during this interval, there will be no output displayed below.

VULNERABILITY: The presence of FHRPs creates an opportunity for the user to implement FHRP related attacks.

EXPLOIT: The OG150 supports a VRRP daemon that allows it to participate in VRRP - if VRRP was detected during the test. The OG150 can be configured with a high VRRP priority to ensure it becomes the ‘active’ default gateway on the LAN or VLAN. Once this is achieved, the user can launch a DOS (Denial of Service) attack on the LAN or VLAN by black-holing all traffic or it can perform a MITM (Man In The Middle) attack, whereby all user traffic on the LAN or VLAN is routed across it (the OG150 is the default gateway and see’s all user traffic).

COUNTERMEASURE: The use of FHRP’s is common and considered good practise. To countermeasure this attack, both HSRP and VRRP support an MD5 Authentication feature which generates an Message Digest 5 (MD5) digest for the HSRP and VRRP messages. If a FHRP message is received that has not been encrypted with the same authentication key, the message is discarded. Configuring authentication for FHRP messages will prevent the OG150 from implementing this exploit.

TEST RESULTS:

```
20:16:50.963482 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112),
length 40)
192.168.11.1 > vrrp.mcast.net: vrrp 192.168.11.1 > vrrp.mcast.net: VRRPv2, Advertisement,
vrid 1, prio 99, authtype none, intvl 1s, length 20, addrs: 192.168.11.247
20:16:51.847446 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112),
length 40)
192.168.11.1 > vrrp.mcast.net: vrrp 192.168.11.1 > vrrp.mcast.net: VRRPv2, Advertisement,
vrid 1, prio 99, authtype none, intvl 1s, length 20, addrs: 192.168.11.247
20:16:52.719339 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112),
length 40)
192.168.11.1 > vrrp.mcast.net: vrrp 192.168.11.1 > vrrp.mcast.net: VRRPv2, Advertisement,
vrid 1, prio 99, authtype none, intvl 1s, length 20, addrs: 192.168.11.247
20:16:52.875314 IP (tos 0xc0, ttl 1, id 0, offset 0, flags [none], proto UDP (17), length
48)
192.168.11.1.1985 > all-routers.mcast.net.1985: HSRPv0-hello 20: state=active group=1
addr=192.168.11.248 hellotime=3s holdtime=10s priority=100 auth="cisco^@^@^@"
20:16:53.587249 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112),
length 40)
192.168.11.1 > vrrp.mcast.net: vrrp 192.168.11.1 > vrrp.mcast.net: VRRPv2, Advertisement,
vrid 1, prio 99, authtype none, intvl 1s, length 20, addrs: 192.168.11.247
20:16:54.435171 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112),
length 40)
192.168.11.1 > vrrp.mcast.net: vrrp 192.168.11.1 > vrrp.mcast.net: VRRPv2, Advertisement,
vrid 1, prio 99, authtype none, intvl 1s, length 20, addrs: 192.168.11.247
20:16:55.339136 IP (tos 0xc0, ttl 1, id 0, offset 0, flags [none], proto UDP (17), length
48)
192.168.11.1.1985 > all-routers.mcast.net.1985: HSRPv0-hello 20: state=active group=1
addr=192.168.11.248 hellotime=3s holdtime=10s priority=100 auth="cisco^@^@^@"
20:16:55.363067 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112),
length 40)
192.168.11.1 > vrrp.mcast.net: vrrp 192.168.11.1 > vrrp.mcast.net: VRRPv2, Advertisement,
vrid 1, prio 99, authtype none, intvl 1s, length 20, addrs: 192.168.11.247
20:16:56.347065 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112),
length 40)
192.168.11.1 > vrrp.mcast.net: vrrp 192.168.11.1 > vrrp.mcast.net: VRRPv2, Advertisement,
vrid 1, prio 99, authtype none, intvl 1s, length 20, addrs: 192.168.11.247
20:16:57.286916 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112),
length 40)
192.168.11.1 > vrrp.mcast.net: vrrp 192.168.11.1 > vrrp.mcast.net: VRRPv2, Advertisement,
vrid 1, prio 99, authtype none, intvl 1s, length 20, addrs: 192.168.11.247
20:16:57.882897 IP (tos 0xc0, ttl 1, id 0, offset 0, flags [none], proto UDP (17), length
48)
192.168.11.1.1985 > all-routers.mcast.net.1985: HSRPv0-hello 20: state=active group=1
addr=192.168.11.248 hellotime=3s holdtime=10s priority=100 auth="cisco^@^@^@"
20:16:58.274837 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112),
length 40)
192.168.11.1 > vrrp.mcast.net: vrrp 192.168.11.1 > vrrp.mcast.net: VRRPv2, Advertisement,
vrid 1, prio 99, authtype none, intvl 1s, length 20, addrs: 192.168.11.247
20:16:59.206769 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112),
length 40)
192.168.11.1 > vrrp.mcast.net: vrrp 192.168.11.1 > vrrp.mcast.net: VRRPv2, Advertisement,
vrid 1, prio 99, authtype none, intvl 1s, length 20, addrs: 192.168.11.247
20:17:00.178713 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112),
length 40)
192.168.11.1 > vrrp.mcast.net: vrrp 192.168.11.1 > vrrp.mcast.net: VRRPv2, Advertisement,
vrid 1, prio 99, authtype none, intvl 1s, length 20, addrs: 192.168.11.247
```

TITLE: DYNAMIC ROUTING PROTOCOL SNOOPING
DESCRIPTION: The OG150 will listen, capture and display dynamic routing protocol messages. This test supports OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol) and RIP (Routing Information Protocol) which are commonly used dynamic routing protocols used within enterprises. The test will run for 60 seconds based on default routing protocol timers. Please Note: If no dynamic routing protocol messages were received during this interval, there will be no output displayed below.
VULNERABILITY: The presence of dynamic routing protocols creates an opportunity for the user to implement dynamic routing protocol related attacks.
EXPLOIT: The OG150 supports ‘Quagga’ which is a routing protocol software suite. ‘Quagga’ allows the OG150 to participate in dynamic routing protocols such as OSPF, RIP and BGP. The OG150 can use ‘Quagga’ to manipulate the routing tables on adjacent routers, ensuring traffic is routed to it. Once this is achieved, the user can launch a DOS (Denial of Service) attack by black-holing all traffic it receives or it can perform a MITM (Man In The Middle) attack, whereby user traffic is routed across it (the OG150 is a transit router and see’s all user traffic).
COUNTERMEASURE: All dynamic routing protocols support authentication and this should be enabled for security reasons. If a dynamic routing protocol message is received that has not been encrypted with the same authentication key, the message is discarded. Configuring authentication for routing protocol messages will prevent the OG150 from implementing this exploit.
TEST RESULTS:

```
20:17:15.941244 IP 192.168.11.1 > ospf-all.mcast.net: OSPFv2, Hello, length 56
20:17:25.148255 IP 192.168.11.1 > ospf-all.mcast.net: OSPFv2, Hello, length 56
20:17:34.531251 IP 192.168.11.1 > ospf-all.mcast.net: OSPFv2, Hello, length 56
20:17:44.494217 IP 192.168.11.1 > ospf-all.mcast.net: OSPFv2, Hello, length 56
20:17:54.105289 IP 192.168.11.1 > ospf-all.mcast.net: OSPFv2, Hello, length 56
20:18:03.708287 IP 192.168.11.1 > ospf-all.mcast.net: OSPFv2, Hello, length 56
```

TITLE: NBTSCAN (NETBIOS SCAN)
DESCRIPTION: The NBTscan software can scan IP networks for Microsoft Windows NetBIOS name information. The OG150 will implement an NBTscan against the OG150 local subnet (eth0) - 192.168.11.0/24. Please Note: Although this test is restricted to the OG150s local IP subnet, this test can easily be scaled to scan additional networks as required.
VULNERABILITY: This scan yields important information related to users/devices and is the first step in finding open file shares.
EXPLOIT: A user could use the scan results to view open file shares that contain sensitive information. In addition, the user can use the scan results to target specific users and/or devices in later attacks. For example, if a specific employee is a target, the scan results usually indicate the user’s name. This allows the user to carry out direct attacks against that specific employee.
COUNTERMEASURE: The best way to prevent NBTscan within the network is to use IEEE 802.1x port authentication. It is also considered good practise to routinely scan the network and shut down any open file shares and educating users about the risks of using open file shares.
TEST RESULTS:

```
Doing NBT name scan for addresses from 192.168.11.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.11.49    <unknown>                  <unknown>
```

TITLE: WIRELESS NETWORK SCANNING

DESCRIPTION: The OG150 will listen for wireless beacons that advertise the presence of wireless networks. Please Note: The OG150 has a 2.4Ghz radio and will detect 802.11b/g/n wireless networks.

VULNERABILITY: This scan yields important information relating wireless networks detected in the target environment. The OG150 will detail the security settings associated with each wireless network that is detected.

EXPLOIT: A user could use the scan results to perform all kinds of attacks against the wireless infrastructure. For example, if the OG150 detects the presence of an SSID using PSK (Pre Shared Key) security, the OG150 can be used to try and crack the PSK which would allow the OG150 to decrypt wireless user traffic.

COUNTERMEASURE: One way to prevent this scan from detecting your wireless networks is to disable beacons on your SSIDs. However, there are other methods to detect SSIDs such as listening to wireless probe requests/responses. A wireless network using WPA2 EAP-TLS authentication with rogue access-point detection, provides a high level of wireless security.

TEST RESULTS:

```
Cell 01 - Address: C8:4C:75:19:4D:A0
Channel:5
Frequency:2.432 GHz (Channel 5)
Quality=69/70  Signal level=-41 dBm
Encryption key:on
ESSID:"og150-test"
Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
11 Mb/s; 12 Mb/s; 18 Mb/s
Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
Extra: Last beacon: 0ms ago
IE: IEEE 802.11i/WPA2 Version 1
Group Cipher : CCMP
Pairwise Ciphers (1) : CCMP
Authentication Suites (1) : PSK
```

TITLE: PUBLIC IP ADDRESS INFORMATION

DESCRIPTION: The OG150 will attempt to connect to the Internet and provide information regarding to the Public IP address that it is using. Please Note: If this content is blank, the connection to the Internet was probably blocked by a firewall.

VULNERABILITY: This test yields important information relating to the Internet connection used by the target infrastructure.

EXPLOIT: A user could use the test results to try and attack the target infrastructure ‘from’ the Internet. For example, assume that this test shows that the target infrastructure is using public IP address [redacted]. The user can, from anywhere on the Internet, attempt to penetrate the target infrastructure by focusing attacks on IP address [redacted].

COUNTERMEASURE: For this test, the OG150 attempts to access a website on the Internet using TCP port 80 (HTTP). To prevent this type of attack consider using a web proxy to secure Internet access. The firewalls should permit the web proxies access to the Internet, whilst denying all other users access to the Internet on known website ports such as TCP port 80 (HTTP).

TEST RESULTS:

```
IP Address: 121.[redacted]
Hostname: CPE-121-[redacted].lnse1.cha.bigpond.net.au
```

TITLE: REMOTE ACCESS STATUS

DESCRIPTION: The OG150 will, if configured, attempt to establish a reverse SSH tunnel to the users SSH server. If the SSH tunnel successfully connects, the user has remote access

to the target network infrastructure from any location with Internet access. This test will confirm the status of the reverse SSH tunnel.
VULNERABILITY: Remote access to the target network is extremely dangerous and allows the user to control the OG150 to launch further attacks against the target.
EXPLOIT: Once remote access has been established, a large list of attacks can be launched by the user. The attacks that can be launched are only limited by the software packages supported by the OG150. There are currently over 2000 packages supported by the OG150, providing a huge number of attack vectors. For example, the OG150 can perform an ARP spoof (using Dsniff), followed by an SSLStrip (using SSLStrip) attack to capture a users banking credentials.
COUNTERMEASURE: The OG150, by default, attempts to access the users SSH server using TCP port 22. To prevent this type of attack consider blocking TCP port 22 on the firewalls. This will prevent the OG150 from establishing a reverse SSH tunnel. Please Note: The default TCP port used for the reserve SSH tunnel can be changed by the user.
TEST RESULTS:

OG150 has NOT established remote access. This may be due to a number of reasons, such as it is not configured or a firewall has denied access.

Thank you for using the OG150, please visit www.og150.com for further information.

Darren Johnson