



Faculty of Information Technology

Milestone 8

BI3 Ethical Hacking Challenge 2011

Team – BI3EHC11-117:

Joshua Stennett

Thomas Ujszaszi

BI3 Ethical Hacking Challenge 2011

Milestone 8

Develop a TAIS Beta Environment Exploit

Virtual Machine Environment

Current Setup:

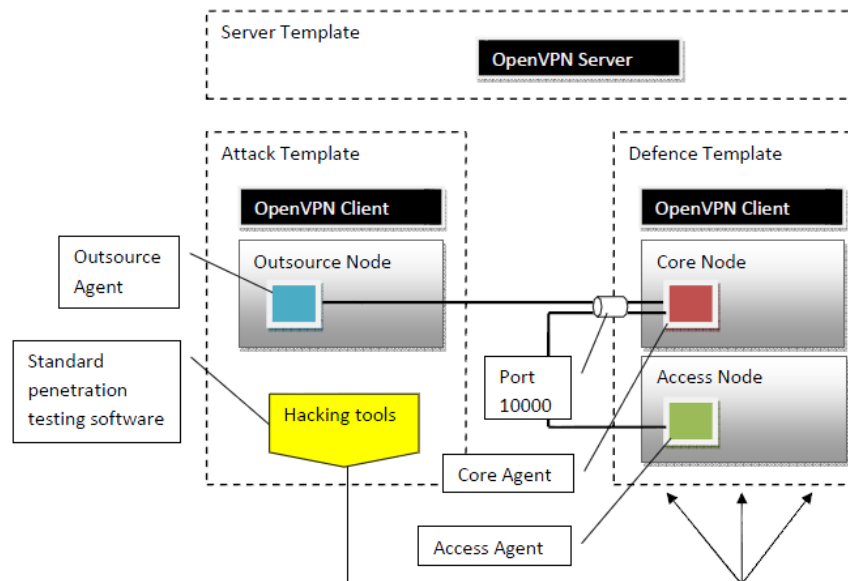


Figure 1: Test VM Environment.

Virtual Machine Environment			
Component	Network	Mask	Notes
Server Template (OpenVPN Server)			
VM Host Only Network	192.168.56.0/24	255.255.255.0	DHCP Allocated – eth5 (192.168.56.101)
Dynamic Pool	5.5.0.0/20	255.255.240.0	VPN Tun GW – 5.5.0.1
Reserved	5.6.0.0/20	255.255.240.0	VPN Tun GW – 5.6.0.1
Attack Template			
VM Host Only Network	192.168.56.0/24	255.255.255.0	DHCP Allocated – eth7 (192.168.56.103)
Tunnel Interface	5.6.0.0/20	255.255.240.0	VPN tun0 – 5.6.0.3
Defence Template			
VM Host Only Network	192.168.56.0/24	255.255.255.0	DHCP Allocated – eth5 (192.168.56.102)
Tunnel Interface	5.6.0.0/20	255.255.240.0	VPN tun0 – 5.6.0.2

Table 1: Virtual Machine IP Address Allocation Tables.

Defence Template (Modifications)

The Defence template was hardened to Linux server administration best practices. Not due to any known insecurities within the Bluebrick implementation, but to limit any potential vulnerability in the underlying substrate.

Firewall

The firewall was disabled temporarily to allow for a number of the below changes, most notably updating and patching of the substrate. Care was taken to re-enable the firewall after all changes were made, as this is the first line of network defence.

SSHD

For ease of performing administrative management tasks, SSH was installed and enabled for remote shell access. The SSH daemon service was removed after all hardening was completed for completeness.

System Upgrade

All currently installed packages were upgraded to the latest release. The kernel was also upgraded to the latest version, at the time (*Linux blueicon-VirtualBox 2.6.38-10-generic #46-Ubuntu SMP Tue Jun 28 15:05:41 UTC 2011 i686 i686 i386 GNU/Linux*).

Recommendations:

- Compiling a custom kernel to further minimise surface area of attack.

Services

All currently installed services were analysed for their usefulness within the scope of just running Bluebrick. Any default services were disabled and removed from the substrate.

Recommendations:

- For non-user interactive builds, remove Xwindows from the substrate to make the server headless. This reduces OS complexity and restricts access to CLI tools only, thus reducing potential vulnerabilities that may be introduced via the GUI.
- Restrict physical access to device: Eg. Disable USB ports, physically lock device if possible (if a server), etc.
- Enable filesystem encryption. The Bluebrick implementation may be theoretically secure however, if the device is physically seized then its contents can be copied and data extracted.

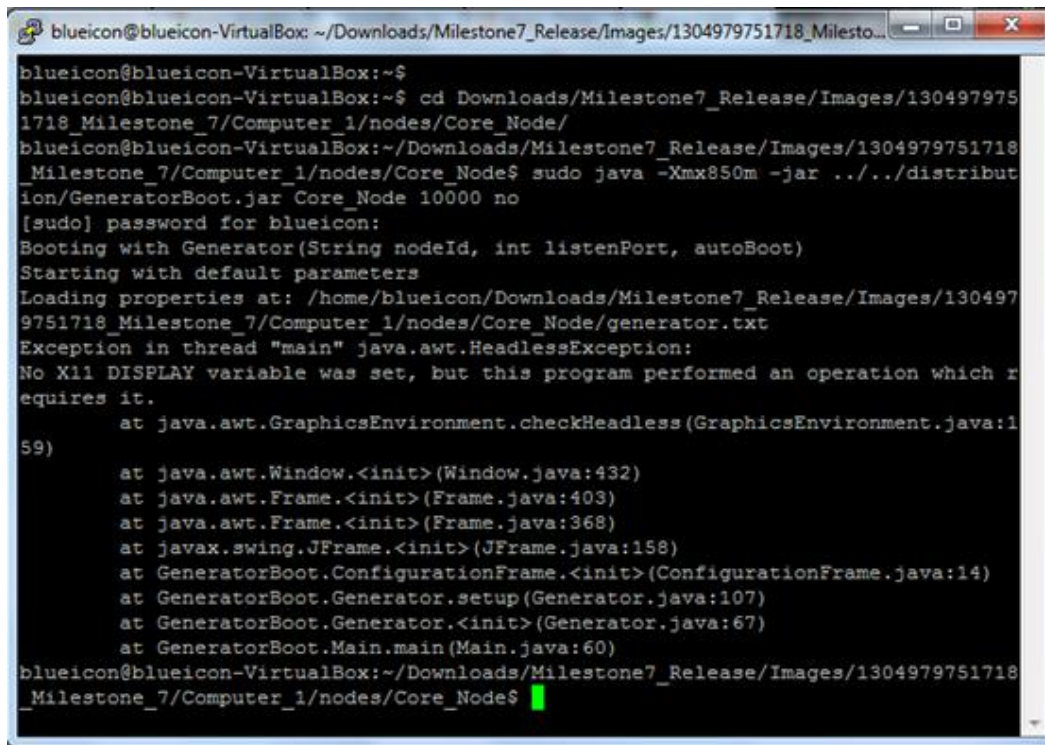
OpenVPN Service

OpenVPN was added to rc.d for service auto start. The configuration to allow an automatic tunnel to be created does involve hardcoding credentials into an auth file in plain text. While this does open up a security concern, the attacker would have to have gained root on the substrate of which still needs to compromise Bluebrick to gain any meaningful access to content.

Bluebrick Service

Attempts to automate the agent load process were unsuccessful as the Xwindows service is required (**Figure 2**). Automating the Bluebrick initial load would add convenience and an additional layer of security as it would make it more difficult to compromise the system when Bluebrick is running.

This issue should be reviewed by the developers as the Bluebrick Service should have the capacity to load independent of Xwindows.



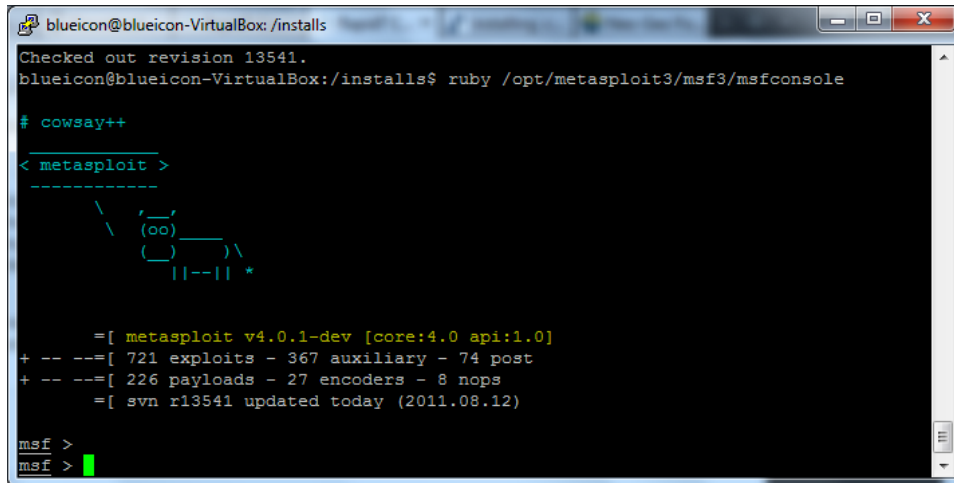
```
blueicon@blueicon-VirtualBox: ~/Downloads/Milestone7_Release/Images/1304979751718_Milesto...
blueicon@blueicon-VirtualBox:~$
blueicon@blueicon-VirtualBox:~$ cd Downloads/Milestone7_Release/Images/1304979751718_Milestone7/Computer_1/nodes/Core_Node/
blueicon@blueicon-VirtualBox:~/Downloads/Milestone7_Release/Images/1304979751718_Milestone7/Computer_1/nodes/Core_Node$ sudo java -Xmx850m -jar ../../distribution/GeneratorBoot.jar Core Node 10000 no
[sudo] password for blueicon:
Booting with Generator(String nodeId, int listenPort, autoBoot)
Starting with default parameters
Loading properties at: /home/blueicon/Downloads/Milestone7_Release/Images/1304979751718_Milestone7/Computer_1/nodes/Core_Node/generator.txt
Exception in thread "main" java.awt.HeadlessException:
No X11 DISPLAY variable was set, but this program performed an operation which requires it.
    at java.awt.GraphicsEnvironment.checkHeadless(GraphicsEnvironment.java:159)
    at java.awt.Window.<init>(Window.java:432)
    at java.awt.Frame.<init>(Frame.java:403)
    at java.awt.Frame.<init>(Frame.java:368)
    at javax.swing.JFrame.<init>(JFrame.java:158)
    at GeneratorBoot.ConfigurationFrame.<init>(ConfigurationFrame.java:14)
    at GeneratorBoot.Generator.setup(Generator.java:107)
    at GeneratorBoot.Generator.<init>(Generator.java:67)
    at GeneratorBoot.Main.main(Main.java:60)
blueicon@blueicon-VirtualBox:~/Downloads/Milestone7_Release/Images/1304979751718_Milestone7/Computer_1/nodes/Core_Node$
```

Figure 2: Trying to run the agent from a terminal session to automate.

Attack Template (Modifications)

Attack template ha, to add more flexibility to analyse the effectiveness of the Defence template:

- **Software Upgrade** – Upgrade all current packages on Attack template.
- **Nmap** (Network Mapper) – Security port scanner.
- **Ncat** – Flexible networking tool.
- **Wireshark / tcpdump** – Packet sniffing and analysis.
- **Metasploit** – Penetration testing framework solution.
- **Nessus** – Vulnerability scanner.



```
blueicon@blueicon-VirtualBox: /installs
Checked out revision 13541.
blueicon@blueicon-VirtualBox:/installs$ ruby /opt/metasploit3/msf3/msfconsole

# cowsay++

< metasploit >
-----
      \
      (oo)_____)
      ( )       )\/
      ||--|| *

=[ metasploit v4.0.1-dev [core:4.0 api:1.0]
+ -- --[ 721 exploits - 367 auxiliary - 74 post
+ -- --[ 226 payloads - 27 encoders - 8 nops
=[ svn r13541 updated today (2011.08.12)

msf >
msf >
```

Figure 3: Metasploit console with an up-to-date database.

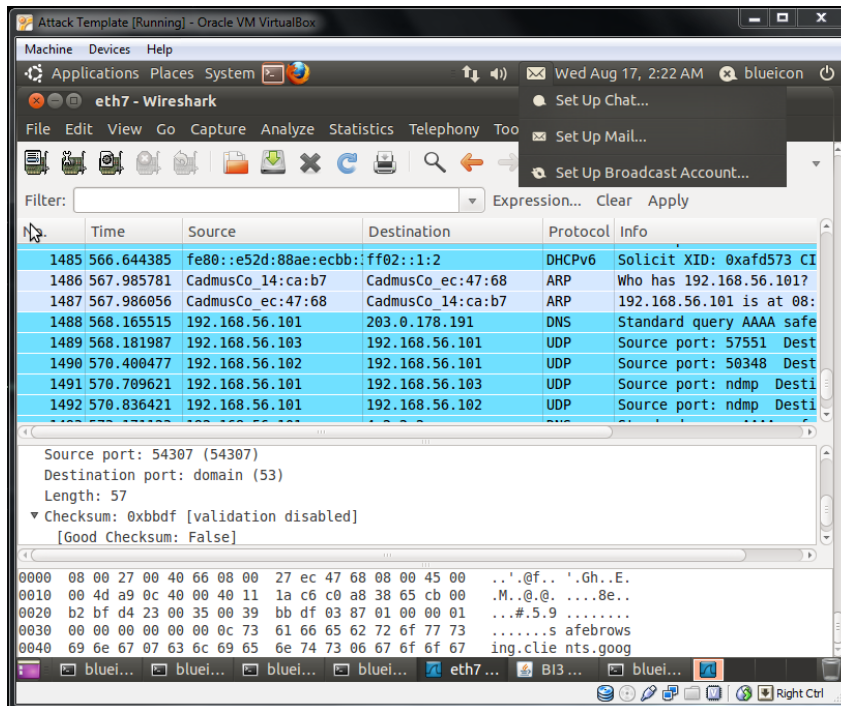


Figure 4: Wireshark packet capture mode.

Part A – Analyse of exploit options

Option A.1

In computer security, an attacker often takes the path of least resistance. An installed Bluebrick implementation may be secured however, it would likely be easier to attack the substrate, Ubuntu in this case, and try to leverage its vulnerabilities.

It is not without precedent for a Government or criminal entity to procure a zero-day exploit for a particular application or operating system. A recent widely publicised case known as the Styxnet worm utilised a number of hereto unknown vulnerabilities within the Programmable Logic Control (PLC) chips found in Siemens industrial hardware, causing significant damage.

The question poses “do you think you could develop or buy an exploit targeting Bluebrick on port 10000?” The short answer to this is no, a remote attack against Bluebrick on port 10000 does not provide much of an access vector. However, if Bluebrick was released and used extensively this answer may become *maybe*. The theory behind Bluebrick may be secure, but it is only as secure as the implementation – misconfigurations may happen, and intuitive minds may find ways to exploit these holes.

Option A.2

As suggested in A.1 above, if an attacker had full access to the source code and configuration files and given enough time and resources, it may be possible to identify an exploit due to a faulty implementation of Bluebrick.

Option A.3

As was mentioned in A.1, the very narrow attack vector where an attacker would have to identify, create and deploy an attack against a secured environment on a single unknown port would be very difficult. A proper implementation of a Bluebrick CRE should make this all but impossible.

Part B – Prepare the hack

Steps taken to prepare the environment for analysis:

- Added the Defence template from Team 115 into our VM environment.
- Attached and loaded all agents, as per Milestone 7 documentation.
- Successfully established connections between all templates, as per Milestone 7 documentation.
- Log files checked to verify correct connectivity.

Part C – Attack

The following tools were loaded in the attack template and used to scan the target for vulnerabilities:

- **Nmap** - Ran full system scan to find any open ports. (*Appendix A*)
- **Metaspolt** - Ran a full system scan checking for open ports and known attack vectors against Linux builds. (*Appendix B*)
- **Nessus** - Ran a full system scan checking for open ports and known attack vectors without specifying any special parameters. (*Appendix C*)
- **Netcat** - Used to send varying sizes of 'garbage' data to port 10000 to try to trigger a buffer overflow or other such system error.

The Outsource Node was not modified in this approach.

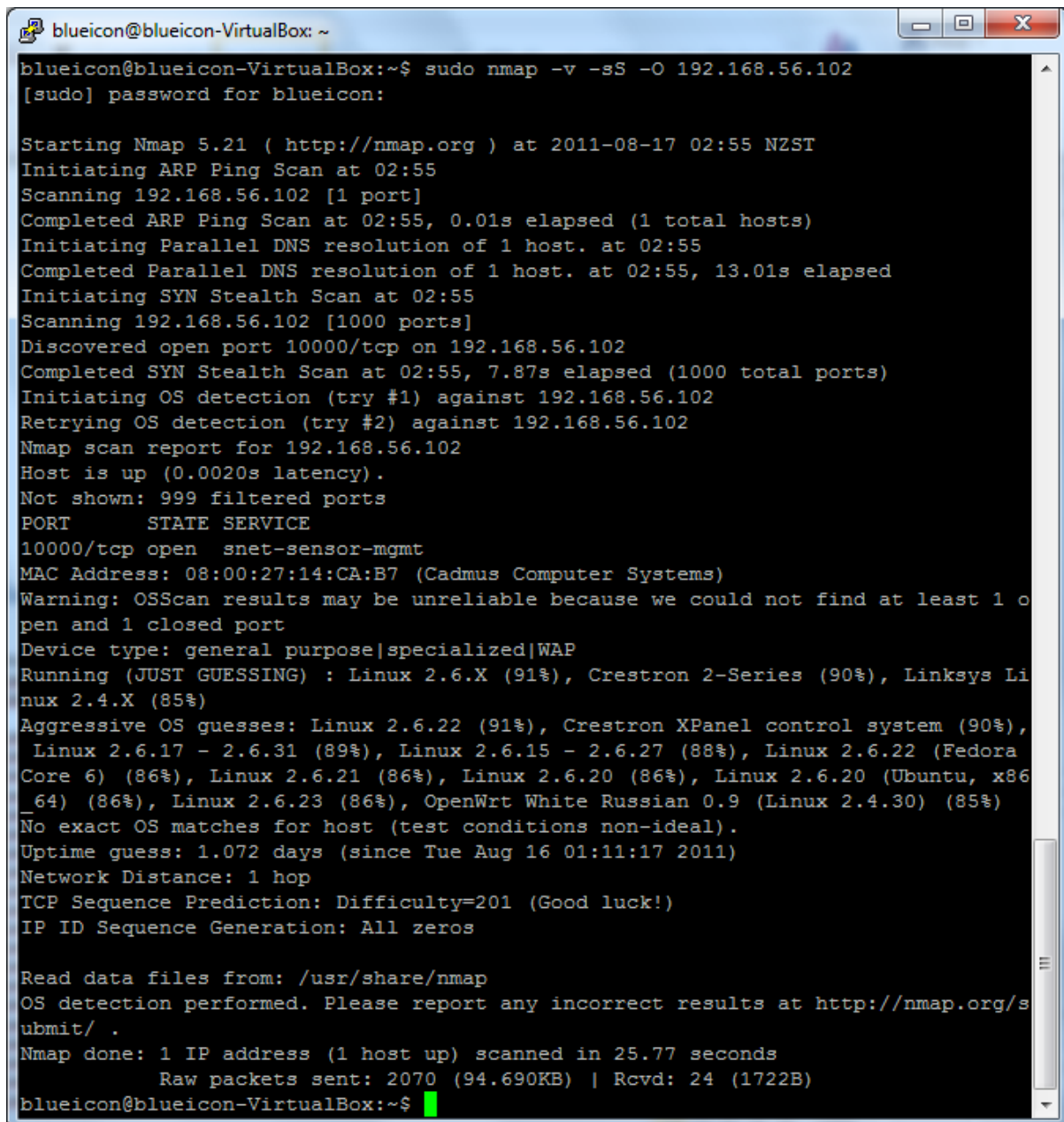
Part D – Document

Analysis of results:

1. This round of testing was unable to compromise the Team 115 defence template and our attempts were unsuccessful.
2. The theory behind Bluebrick is sound and, with a proper configuration and implementation, the deployed device would be very secure.
3. Penetration testing locally would be identical to an internet implementation therefore proving its secure locally would provide confidence moving it to an internet application. However, large scale implementation of Bluebrick on the Internet would open it up to a worldwide audience and greater scrutiny.

Appendix A

NMap Scan on Defence template



```
blueicon@blueicon-VirtualBox: ~
blueicon@blueicon-VirtualBox:~$ sudo nmap -v -sS -O 192.168.56.102
[sudo] password for blueicon:

Starting Nmap 5.21 ( http://nmap.org ) at 2011-08-17 02:55 NZST
Initiating ARP Ping Scan at 02:55
Scanning 192.168.56.102 [1 port]
Completed ARP Ping Scan at 02:55, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:55
Completed Parallel DNS resolution of 1 host. at 02:55, 13.01s elapsed
Initiating SYN Stealth Scan at 02:55
Scanning 192.168.56.102 [1000 ports]
Discovered open port 10000/tcp on 192.168.56.102
Completed SYN Stealth Scan at 02:55, 7.87s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.56.102
Retrying OS detection (try #2) against 192.168.56.102
Nmap scan report for 192.168.56.102
Host is up (0.0020s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:14:CA:B7 (Cadmus Computer Systems)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose|specialized|WAP
Running (JUST GUESSING) : Linux 2.6.X (91%), Crestron 2-Series (90%), Linksys Li
nux 2.4.X (85%)
Aggressive OS guesses: Linux 2.6.22 (91%), Crestron XPanel control system (90%),
Linux 2.6.17 - 2.6.31 (89%), Linux 2.6.15 - 2.6.27 (88%), Linux 2.6.22 (Fedora
Core 6) (86%), Linux 2.6.21 (86%), Linux 2.6.20 (86%), Linux 2.6.20 (Ubuntu, x86
_64) (86%), Linux 2.6.23 (86%), OpenWrt White Russian 0.9 (Linux 2.4.30) (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 1.072 days (since Tue Aug 16 01:11:17 2011)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.77 seconds
Raw packets sent: 2070 (94.690KB) | Rcvd: 24 (1722B)
blueicon@blueicon-VirtualBox:~$
```

Figure 5: Nmap scan on Defence template.

Appendix B

Metasploit Scan on Defence template

```
Blueicon      2011-08-14T13:31:46 Scan started by: "Blueicon" <>
Scan          2011-08-14T13:31:46 [Site: Blueicon] Initializing alerters for scan Blueicon
Scan          2011-08-14T13:31:46 [Site: Blueicon] Starting scan Blueicon (id default:1) with
scan template full-audit
Scan          2011-08-14T13:31:50 [Site: Blueicon] scan Blueicon loading plugins
Scan          2011-08-14T13:32:00 [Site: Blueicon] loading extension java/NetworkScanners
Scan          2011-08-14T13:32:01 [Site: Blueicon] loading extension java/HttpScanner
Scan          2011-08-14T13:32:02 [Site: Blueicon] loading extension java/TelnetScanner
Scan          2011-08-14T13:32:02 [Site: Blueicon] loading extension java/SshScanner
Scan          2011-08-14T13:32:03 [Site: Blueicon] loading extension java/LinuxRPMScanner
Scan          2011-08-14T13:32:03 [Site: Blueicon] loading extension java/SuseRPMScanner
Scan          2011-08-14T13:32:03 [Site: Blueicon] loading extension java/FtpScanner
Scan          2011-08-14T13:32:03 [Site: Blueicon] loading extension java/RshScanner
Scan          2011-08-14T13:32:03 [Site: Blueicon] loading extension java/TftpScanner
Scan          2011-08-14T13:32:03 [Site: Blueicon] loading extension java/RpcScanner
Scan          2011-08-14T13:32:03 [Site: Blueicon] loading extension java/NfsScanner
Scan          2011-08-14T13:32:03 [Site: Blueicon] loading extension java/LdapScanner
Scan          2011-08-14T13:32:03 [Site: Blueicon] loading extension java/CifsScanner
Scan          2011-08-14T13:32:03 [Site: Blueicon] loading extension java/GameScanner
Scan          2011-08-14T13:32:03 [Site: Blueicon] loading extension java/UnixScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/NetwareScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/NotesScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/PopScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/Db2Scanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/DceRpcScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/CvsScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/MacOSScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/TdsScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/CheckpointScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/DhcpScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/RedHatRPMScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/OracleScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/VMwarePatchScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/AIXFilesetScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/CiscoScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/SnmpScanner
Scan          2011-08-14T13:32:04 [Site: Blueicon] loading extension java/WindowsScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/SpywareScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/PostgresScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/DnsScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/FingerScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/SolarisScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/PPTPScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/MiscScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/BackdoorScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/CentOSRPMScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/SmtppScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/WindowsHotfixScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/MySQLScanner
Scan          2011-08-14T13:32:05 [Site: Blueicon] loading extension java/XwindowsScanner
Scan          2011-08-14T13:32:06 [Site: Blueicon] loading extension java/WMIScanner
Scan          2011-08-14T13:32:06 [Site: Blueicon] loading extension java/PhScanner
Scan          2011-08-14T13:32:06 [Site: Blueicon] loading extension java/AS400Scanner
Scan          2011-08-14T13:32:06 [Site: Blueicon] loading extension java/ImapScanner
Scan          2011-08-14T13:32:06 [Site: Blueicon] loading extension java/NDMPScanner
Scan          2011-08-14T13:32:06 [Site: Blueicon] loading extension java/SunPatchScanner
Scan          2011-08-14T13:32:06 [Site: Blueicon] loading extension java/RsyncScanner
Scan          2011-08-14T13:32:06 [Site: Blueicon] loading extension java/IpsecScanner
Scan          2011-08-14T13:32:11 [Site: Blueicon] scan Blueicon creating network scanning
globals...
Scan          2011-08-14T13:32:11 [Site: Blueicon] Creating default services mapper with:
default-services.properties
Scan          2011-08-14T13:32:11 [Site: Blueicon] Creating VMware update mapper with:
\usr\local\nexpose\plugins\java\1\VMwarePatchScanner\1\update-id.properties
ProtocolFper2011-08-14T13:32:12 Loaded 76 certs from keystore
\usr\local\nexpose\_jvml.6.0_25\lib\security\cacerts
Scan          2011-08-14T13:32:12 [Site: Blueicon] Scan startup took 26 seconds
Scan          2011-08-14T13:32:12 [Site: Blueicon] scan Blueicon locating live nodes...
```

```

Scan      2011-08-14T13:32:12 [Site: Blueicon] TCP port scanner is using: method[Syn]
sendDelay[0] blockSize[10] blockDelay[10] retryLoops[5] connectTimeout[3000]
Scan      2011-08-14T13:32:12 [Site: Blueicon] UDP port scanner is using: sendDelay[0]
useRaw[false] retryLoops[5]
Scan      2011-08-14T13:32:12 [Site: Blueicon] Starting ping sweep...
Scan      2011-08-14T13:32:13 [Site: Blueicon] Pinger is using: icmp[on]
tcp[21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080]
udp[53,67,68,69,123,135,137,138,139,161,162,445,500,514,520,631,1434,1900,4500,49152]
sendDelay[5] retries[4] responseWait[1000]
Scan      2011-08-14T13:32:13 [Site: Blueicon] Pinger is using: icmp[on]
tcp[21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080]
udp[53,67,68,69,123,135,137,138,139,161,162,445,500,514,520,631,1434,1900,4500,49152]
sendDelay[5] retries[4] responseWait[1000]
Scan      2011-08-14T13:32:13 [Site: Blueicon] Pinger is using: icmp[on]
tcp[21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080]
udp[53,67,68,69,123,135,137,138,139,161,162,445,500,514,520,631,1434,1900,4500,49152]
sendDelay[5] retries[4] responseWait[1000]
Scan      2011-08-14T13:32:13 [Site: Blueicon] Pinger is using: icmp[on]
tcp[21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080]
udp[53,67,68,69,123,135,137,138,139,161,162,445,500,514,520,631,1434,1900,4500,49152]
sendDelay[5] retries[4] responseWait[1000]
Scan      2011-08-14T13:32:13 [Site: Blueicon] Pinger is using: icmp[on]
tcp[21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080]
udp[53,67,68,69,123,135,137,138,139,161,162,445,500,514,520,631,1434,1900,4500,49152]
sendDelay[5] retries[4] responseWait[1000]
Scan      2011-08-14T13:32:13 [Site: Blueicon] Pinger is using: icmp[on]
tcp[21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080]
udp[53,67,68,69,123,135,137,138,139,161,162,445,500,514,520,631,1434,1900,4500,49152]
sendDelay[5] retries[4] responseWait[1000]
Scan      2011-08-14T13:32:13 [Site: Blueicon] Pinger is using: icmp[on]
tcp[21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080]
udp[53,67,68,69,123,135,137,138,139,161,162,445,500,514,520,631,1434,1900,4500,49152]
sendDelay[5] retries[4] responseWait[1000]
Scan      2011-08-14T13:32:13 [Site: Blueicon] Pinger is using: icmp[on]
tcp[21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080]
udp[53,67,68,69,123,135,137,138,139,161,162,445,500,514,520,631,1434,1900,4500,49152]
sendDelay[5] retries[4] responseWait[1000]
Scan      2011-08-14T13:32:15 [Site: Blueicon] [192.168.56.102] ALIVE
Scan      2011-08-14T13:32:15 [Site: Blueicon] Scan Blueicon finished locating 1 live nodes
in 2 seconds
Scan      2011-08-14T13:32:15 [Site: Blueicon] Queued live nodes for scanning: 1
Nexpose   2011-08-14T13:32:15 0 nodes completed, 1 active, 0 pending.
Nexpose   2011-08-14T13:32:15 [192.168.56.102] starting node scan
Scan      2011-08-14T13:32:16 [Site: Blueicon] [192.168.56.102] Resolving additional DNS
records
Scan      2011-08-14T13:32:21 [Site: Blueicon] [192.168.56.102] Finished resolving DNS
records
Scan      2011-08-14T13:32:21 [Site: Blueicon] [192.168.56.102] Queueing UDP port scan
Scan      2011-08-14T13:32:21 [Site: Blueicon] [192.168.56.102] Queueing TCP port scan
Scan      2011-08-14T13:32:21 [Site: Blueicon] [192.168.56.102] Scanning 49 UDP ports
Scan      2011-08-14T13:32:21 [Site: Blueicon] [192.168.56.102] Scanning 1328 TCP ports
Scan      2011-08-14T13:32:31 [Site: Blueicon] [192.168.56.102] Completed TCP port scan (No
open ports): 9 seconds
Scan      2011-08-14T13:33:11 [Site: Blueicon] [192.168.56.102] Completed UDP port scan (No
open ports): 50 seconds
Scan      2011-08-14T13:33:11 [Site: Blueicon] [192.168.56.102] No open TCP ports, IP
fingerprinting cannot be performed
Scan      2011-08-14T13:33:22 [Site: Blueicon] [192.168.56.102] generic-icmp-timestamp (net-
icmp-timestamp-request) - NOT VULNERABLE
Scan      2011-08-14T13:33:32 [Site: Blueicon] [192.168.56.102] generic-icmp-netmask (net-
icmp-netmask-request) - NOT VULNERABLE
Nexpose   2011-08-14T13:33:32 [192.168.56.102] Freeing vulnerability data...
Nexpose   2011-08-14T13:33:32 [192.168.56.102] Freeing node cache data...
Nexpose   2011-08-14T13:33:32 [192.168.56.102] Freeing resources for active services...
Scan      2011-08-14T13:33:36 [Site: Blueicon] Scan [Blueicon] completed in 1 minute 49
seconds
Scan      2011-08-14T13:33:38 [Site: Blueicon] Scan [Blueicon] discovered 1 live devices, 0
vulnerabilities.

```

Appendix C

Nessus Scan on Defence template



PLUGIN IDS	ISSUES
35716	1
19506	1

PLUGIN IDS	SEVERITY	# OF ISSUES	SYNOPSIS
35716	Low	1	Ethernet Card Manufacturer Detection The manufacturer can be deduced from the Ethernet OUI.
19506	Low	1	Nessus Scan Information Information about the Nessus scan.

172.30.10.20

Scan Time

Start time: Wed Aug 17 23:51:30 2011
End time: Thu Aug 18 00:22:33 2011

Number of vulnerabilities

High 0
Medium 0
Low 2

Remote Host Information

MAC address: 08:00:27:dc:f1:64