


Toolkit 1

 On-line demo:
http://buchananweb.co.uk/adv_security_and_network_forensics/toolkit01/toolkit01.htm

The objective of this series of labs is to build an integrated toolkit. Open up the following

<http://buchananweb.co.uk/toolkit.zip>

and extract to a local folder. Next open up toolkit.sln, and double click on client.cs.

- 1.1 Select the [Network] table, and double click on the “netstat -a” button, and add the code:

```
runProgram("netstat", "-a");
```

and test the program.

- 1.2 Select the [Network] table, and complete the rest of the buttons (netstat -a, “arp -a”, “nbstat -n”, “systeminfo”, “ipconfig”, “ipconfig /all”, “route print” and “net view|”). See Figure L1.4.

For Audit Policy add:

```
runProgram("Auditpol", "/get /category:*");
```

For Clear ARP add:

```
runProgram("netsh", "interface ip delete arpcache");
```

For Add Firewall Rule:

```
runProgram("netsh", "advfirewall firewall add rule name=\"NetworkSims Rule\" dir=in action=allow protocol=TCP localport=65000");
```

For Add ICMP Rule:

```
runProgram("netsh", "advfirewall firewall add rule name=\"NetworkSims Rule\" protocol=icmpv4:8,any dir=in action=allow");
```

For Delete Rule:

```
runProgram("netsh", "advfirewall firewall delete rule name=\"NetworkSims Rule\" dir=in");
```

For Show Rules:

```
runProgram("netsh", "advfirewall firewall show rule name=\"Networksims Rule\"");
```

1.3 Now add three buttons, and three text boxes (tbPing, tbTracert and tbTracert) and add a ping, tracert and nslookup button. Next add the code to each of the buttons:

```
runProgram("ping", tbPing.Text);
runProgram("tracert", tbTracert.Text);
runProgram("nslookup", tbTracert.Text);
```

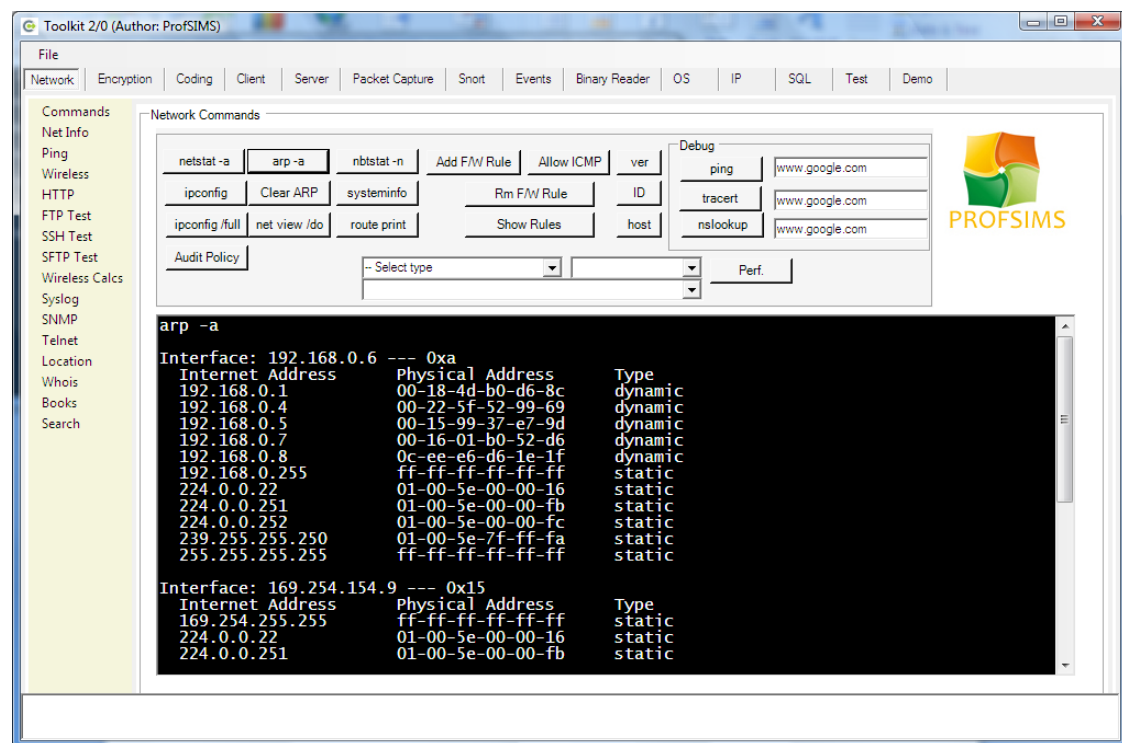


Figure 1.4 Buttons to add