

SECURE DATA STORAGE, SECURE DATA TRANSMISSION AND FOR CREATING DIGITAL SIGNATURES (GNUPG)

AIM:

Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG).

INTRODUCTION:

- Here's the final guide in my PGP basics series, this time focusing on Windows
- The OS in question will be Windows 7, but it should work for Win8 and Win8.1 as well
- Obviously it's not recommended to be using Windows to access the DNM, but I won't go into the reasons here.
- The tool we'll be using is GPG4Win

INSTALLING THE SOFTWARE:

1. Visit www.gpg4win.org. Click on the "Gpg4win 2.3.0" button

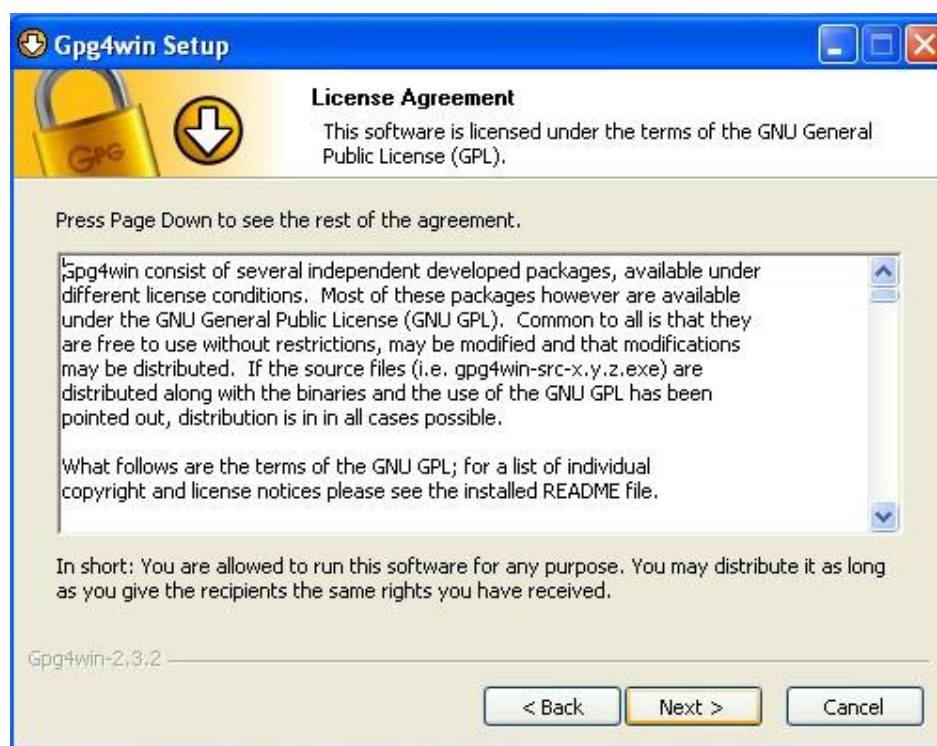
2. On the following screen, click the “Download Gpg4win” button.



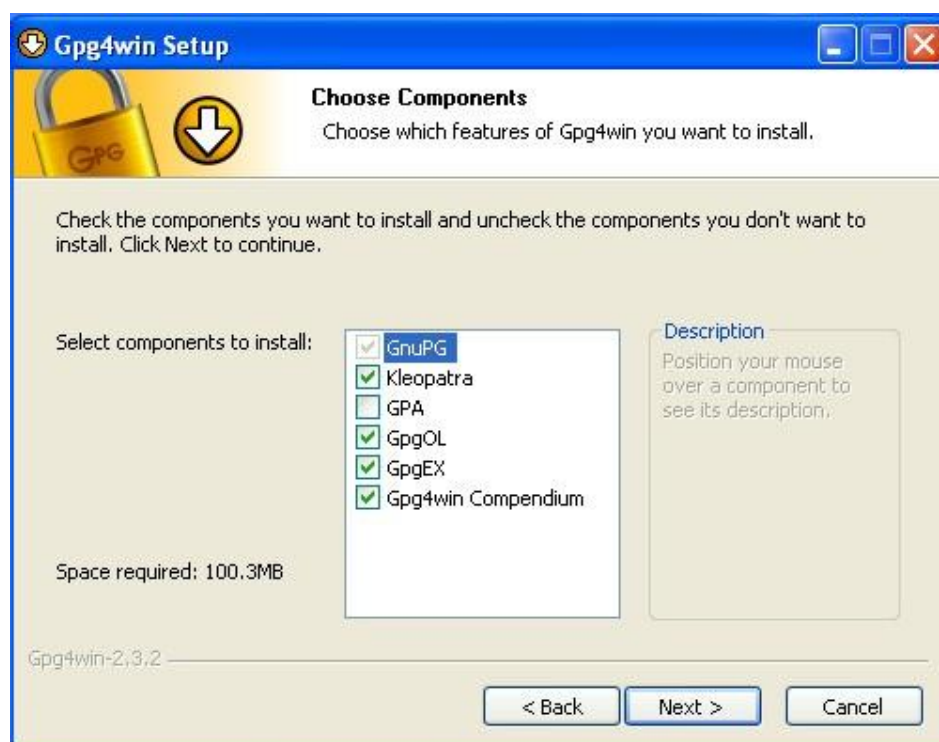
3. When the “Welcome” screen is displayed, click the “Next” button



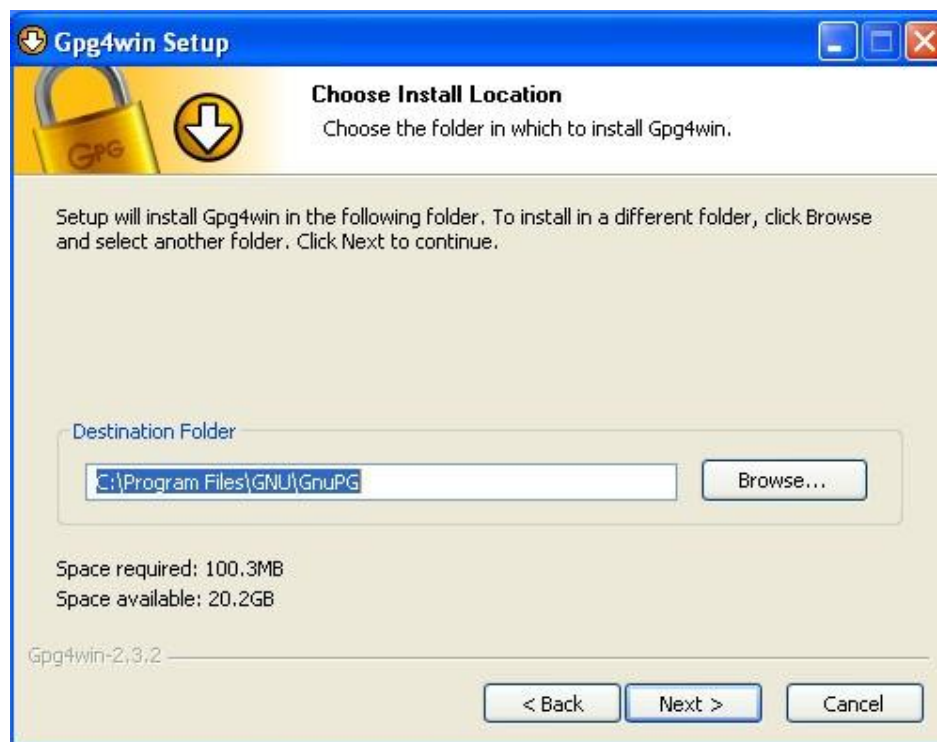
4. When the “License Agreement” page is displayed, click the “Next” button



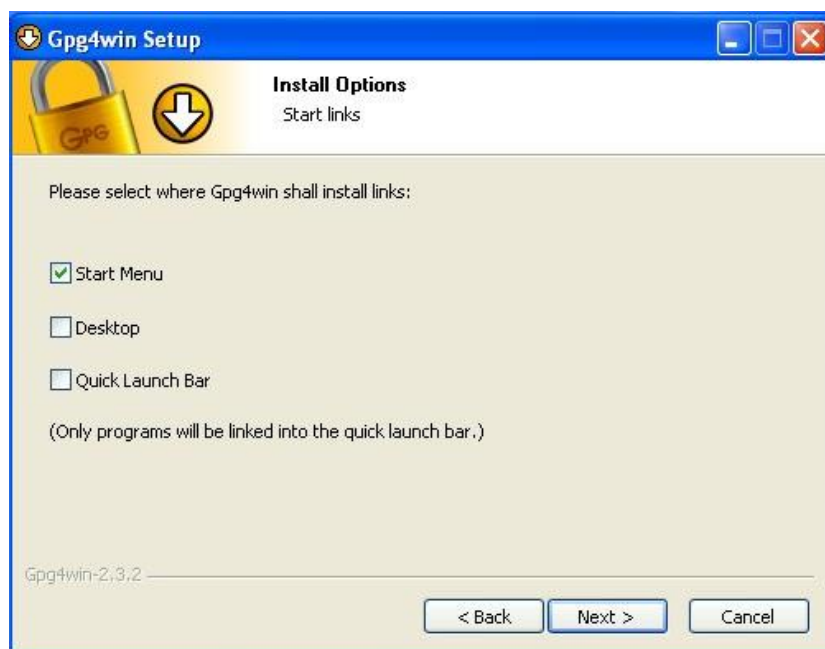
5. Set the check box values as specified below, then click the “Next” button



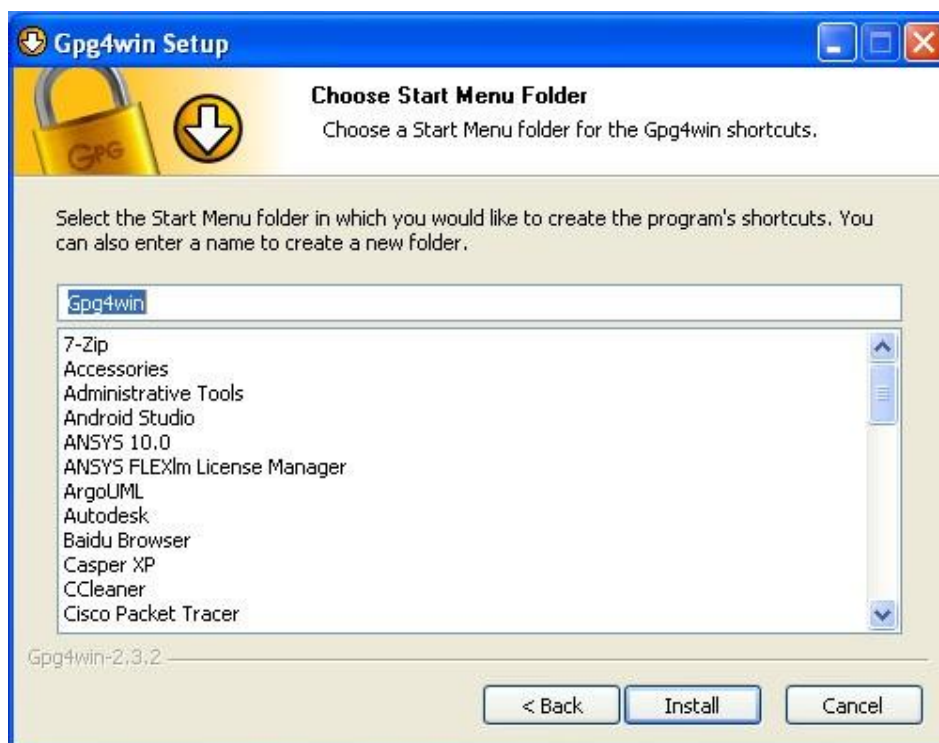
- Set the location where you want the software to be installed. The default location is fine. Then, click the “Next” button.



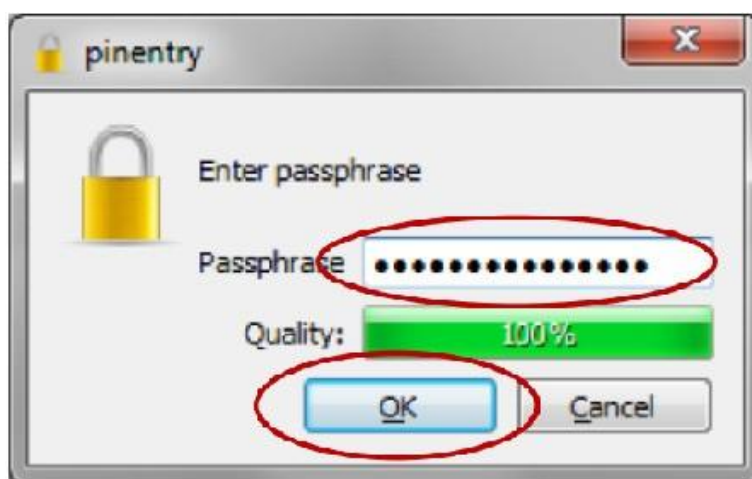
- Specify where you want shortcuts to the software placed, then click the “Next” button.



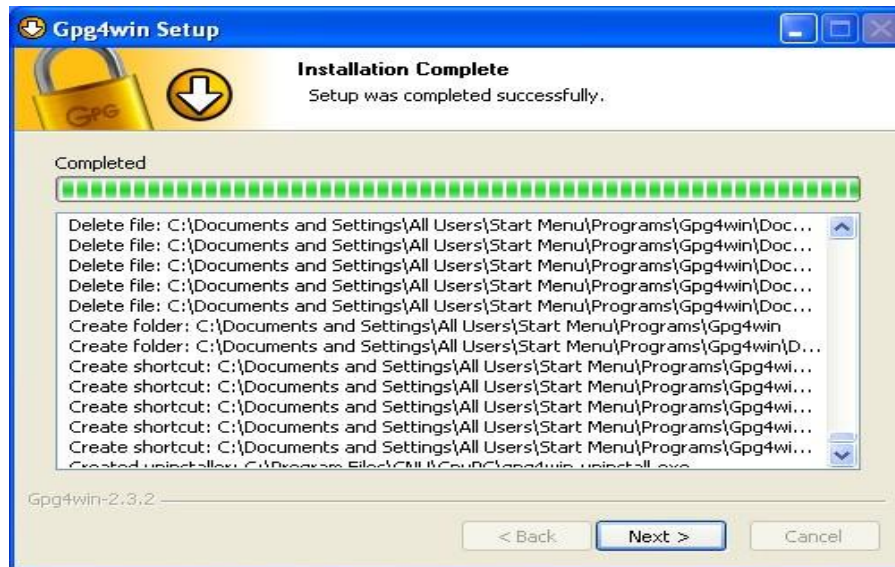
8. If you selected to have a GPG shortcut in your Start Menu, specify the folder in which it will be placed. The default “Gpg4win” is OK. Click the “Install” button to continue



9. A warning will be displayed if you have Outlook or Explorer opened. If this occurs, click the “OK” button.



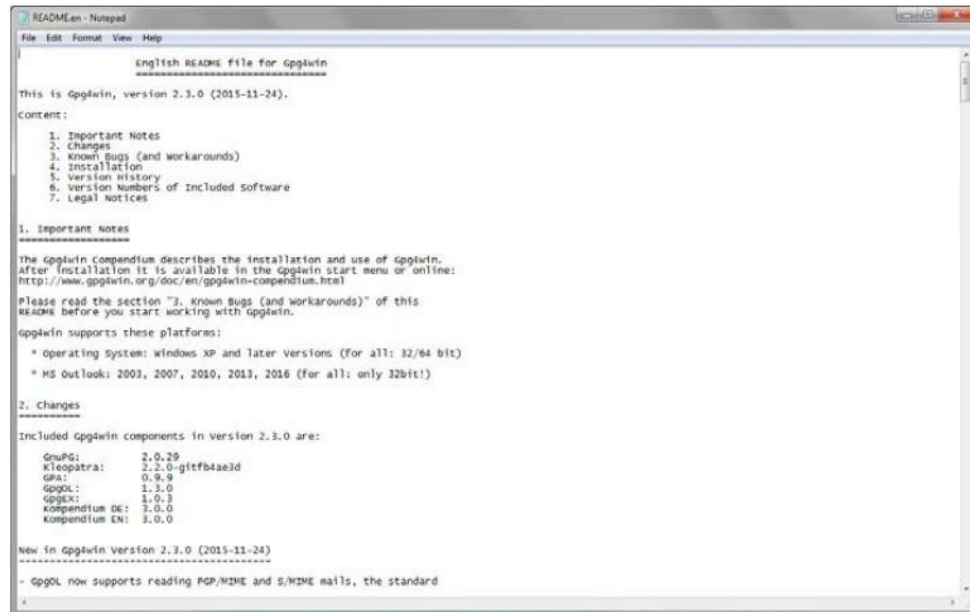
10. The installation process will tell you when it is complete. Click the “Next” button



11. Once the Gpg4win setup wizard is complete, the following screen will be displayed. Click the “Finish” button



12. If you do not uncheck the “Show the README file” check box, the README file will be displayed. The window can be closed after you’ve reviewed it.



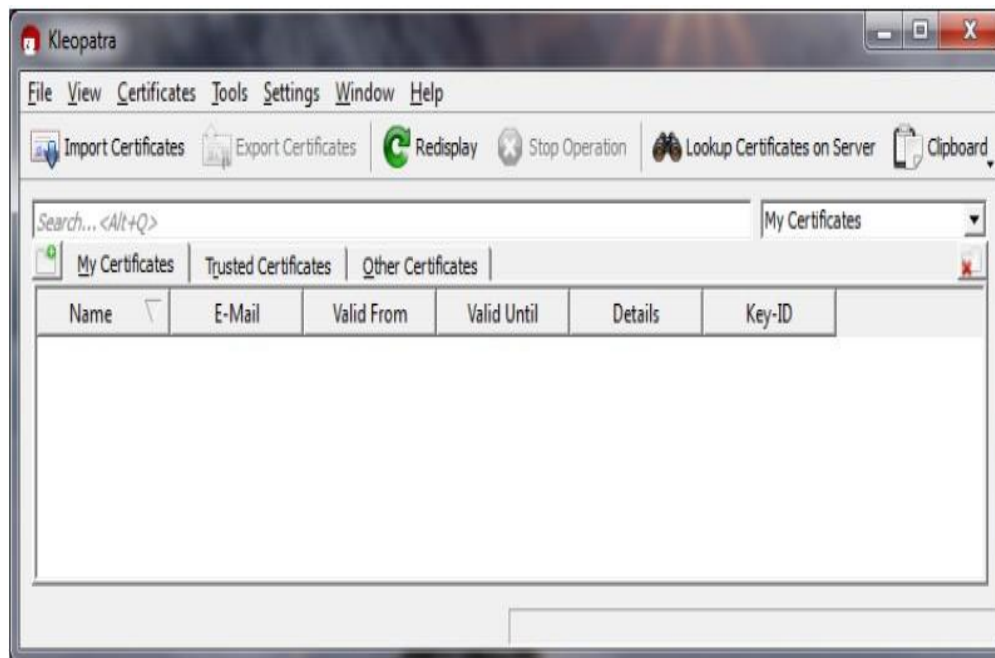
CREATING YOUR PUBLIC AND PRIVATE KEYS

GPG encryption and decryption is based upon the keys of the person who will be receiving the encrypted file or message. Any individual who wants to send the person an encrypted file or message must possess the recipient’s public key certificate to encrypt the message. The recipient must have the associated private key, which is different than the public key, to be able to decrypt the file. The public and private key pair for an individual is usually generated by the individual on his or her computer using the installed GPG program, called “Kleopatra” and the following procedure:

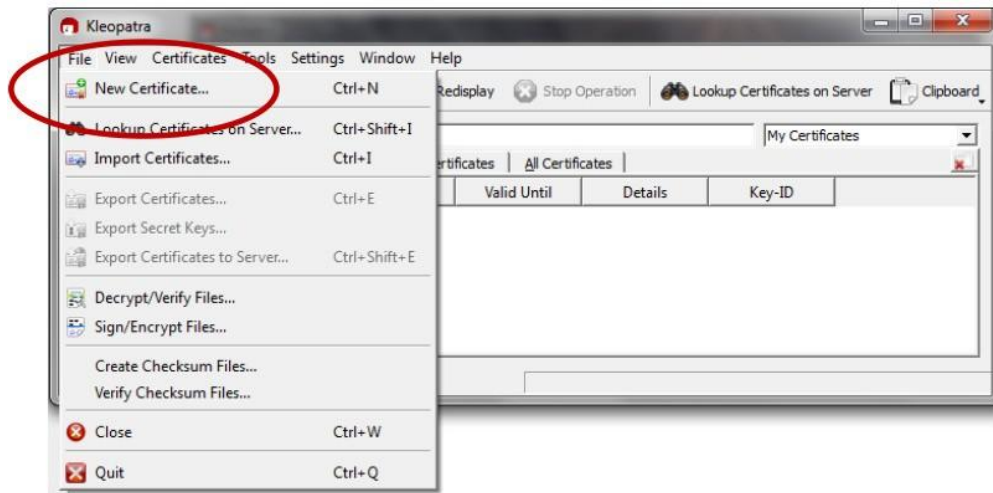
1. From your start bar, select the “Kleopatra” icon to start the Kleopatra certificate management software



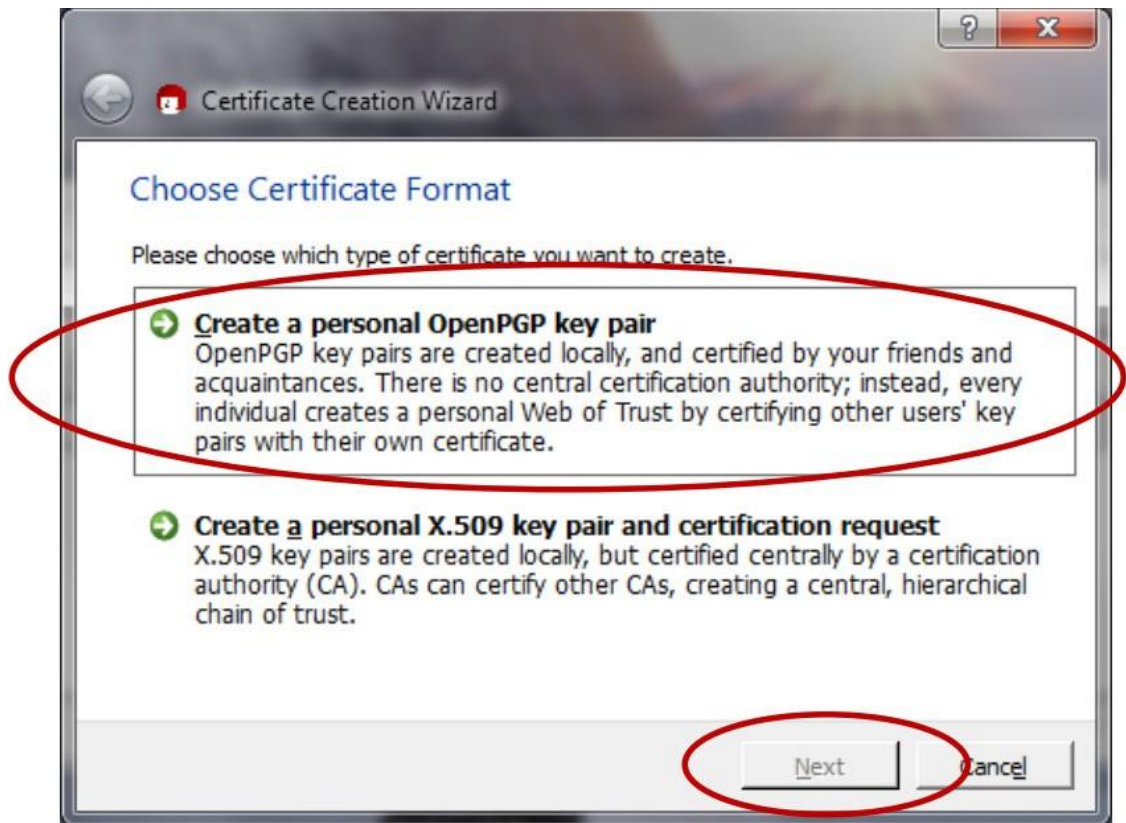
2. The following screen will be displayed



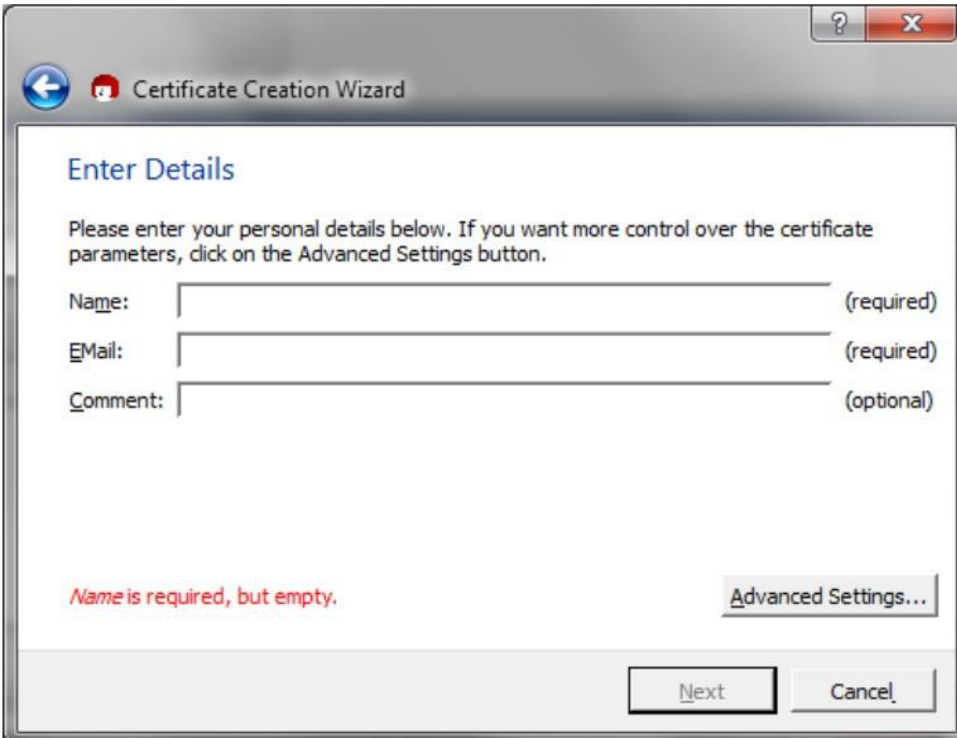
3. From the “File” dropdown, click on the “New Certificate” option



4. The following screen will be displayed. Click on “Create a personal OpenPGP key pair” and the “Next” button

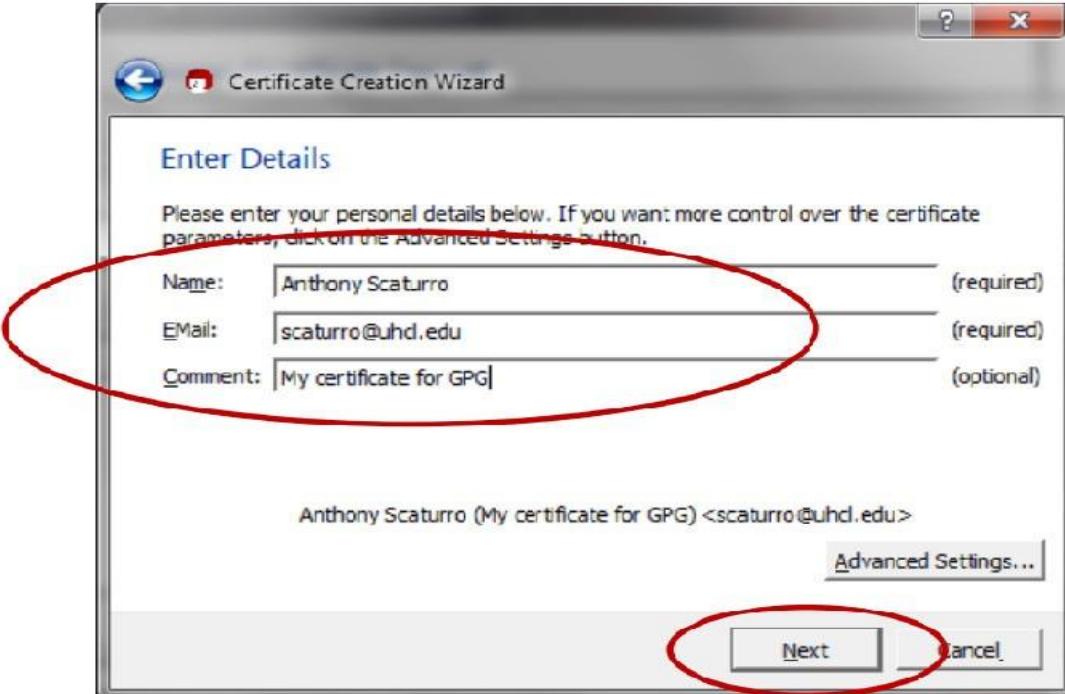


5. The Certificate Creation Wizard will start and display the following:



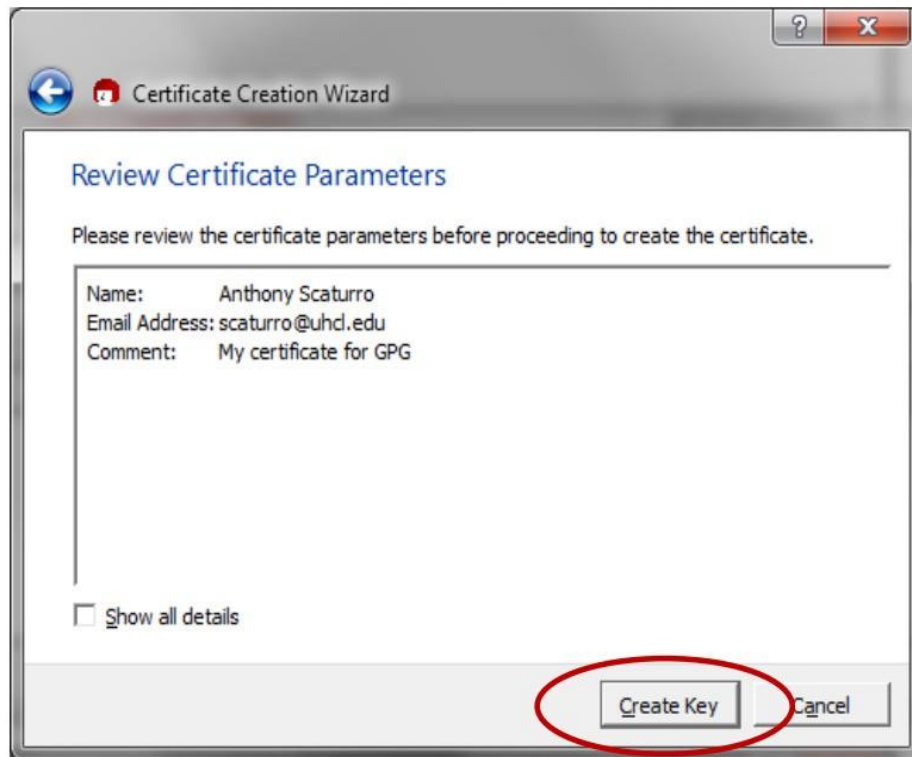
The screenshot shows the 'Certificate Creation Wizard' window with the 'Enter Details' tab selected. The window has a title bar with a question mark and a close button. Below the title bar is a navigation bar with a back arrow and the text 'Certificate Creation Wizard'. The main content area is titled 'Enter Details' and contains the instruction: 'Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.' There are three input fields: 'Name:' (required), 'EMail:' (required), and 'Comment:' (optional). The 'Name' field is empty, and a red error message 'Name is required, but empty.' is displayed below it. The 'EMail' field is also empty. The 'Comment' field is empty. At the bottom right, there is an 'Advanced Settings...' button. At the bottom center, there are 'Next' and 'Cancel' buttons.

6. Enter your name and e-mail address. You may also enter an optional comment. Then, click the “Next” button

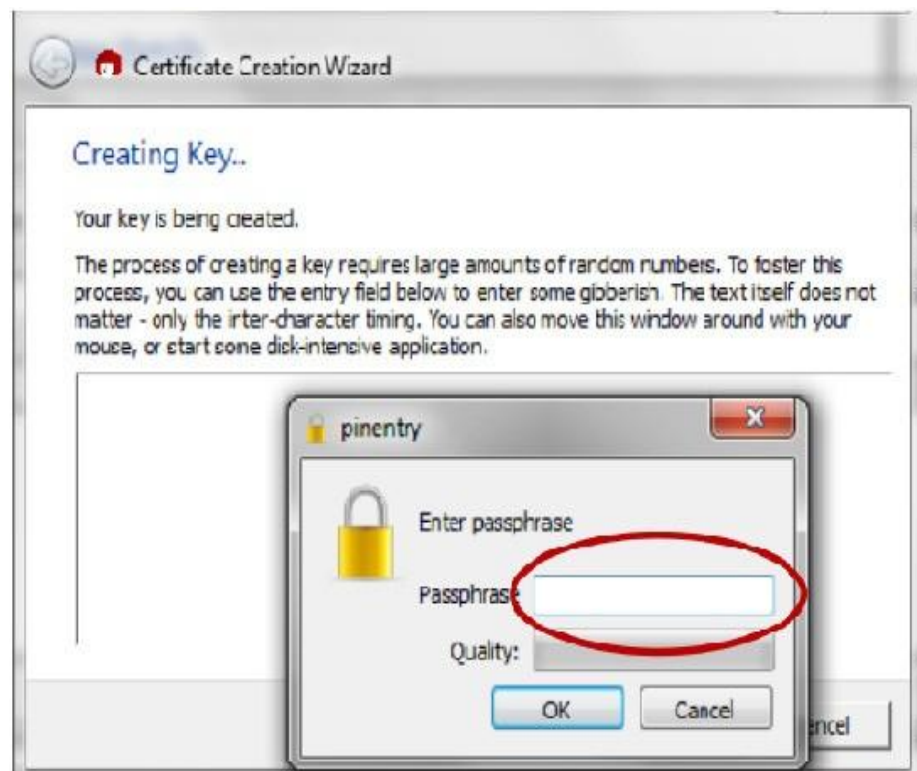


The screenshot shows the 'Certificate Creation Wizard' window with the 'Enter Details' tab selected. The window has a title bar with a question mark and a close button. Below the title bar is a navigation bar with a back arrow and the text 'Certificate Creation Wizard'. The main content area is titled 'Enter Details' and contains the instruction: 'Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.' There are three input fields: 'Name:' (required), 'EMail:' (required), and 'Comment:' (optional). The 'Name' field contains 'Anthony Scaturro', the 'EMail' field contains 'scaturro@uhd.edu', and the 'Comment' field contains 'My certificate for GPG'. A red oval highlights the 'Name' and 'EMail' fields. Below the input fields, the text 'Anthony Scaturro (My certificate for GPG) <scaturro@uhd.edu>' is displayed. At the bottom right, there is an 'Advanced Settings...' button. At the bottom center, there are 'Next' and 'Cancel' buttons. A red oval highlights the 'Next' button.

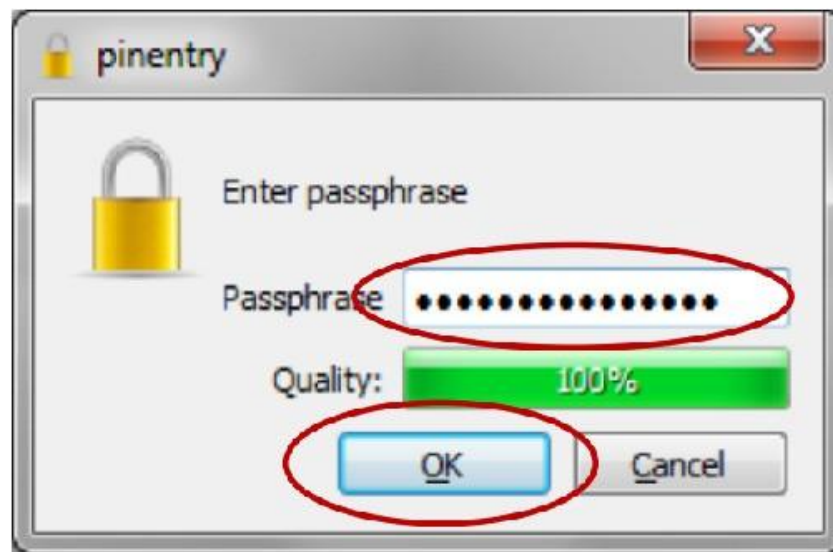
7. Review your entered values. If OK, click the “Create Key” button



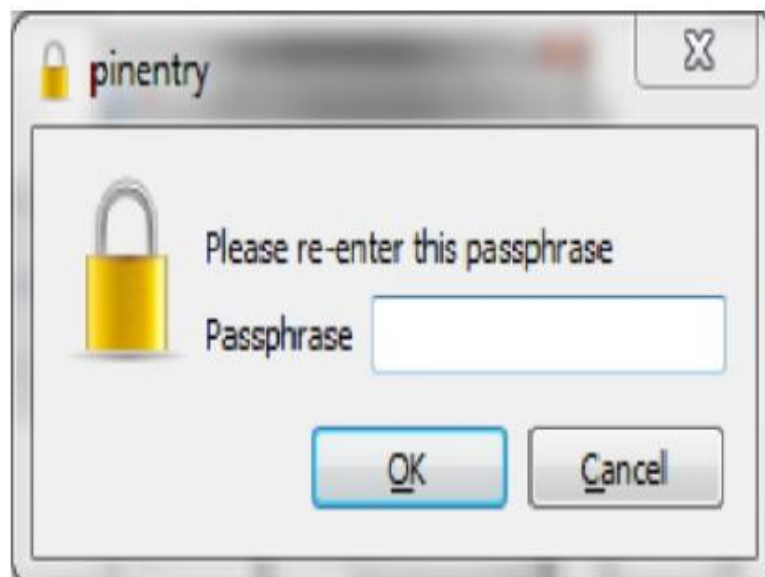
8. You will be asked to enter a passphrase



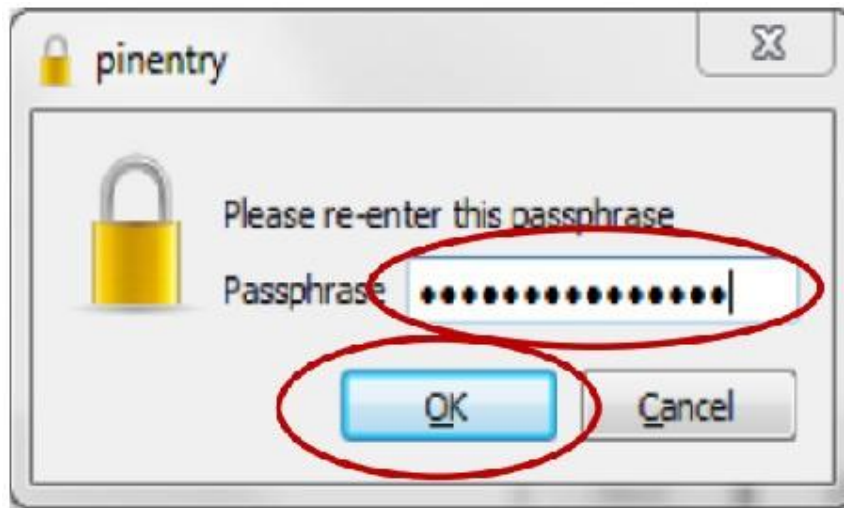
9. The passphrase should follow strong password standards. After you've entered your passphrase, click the "OK" button.



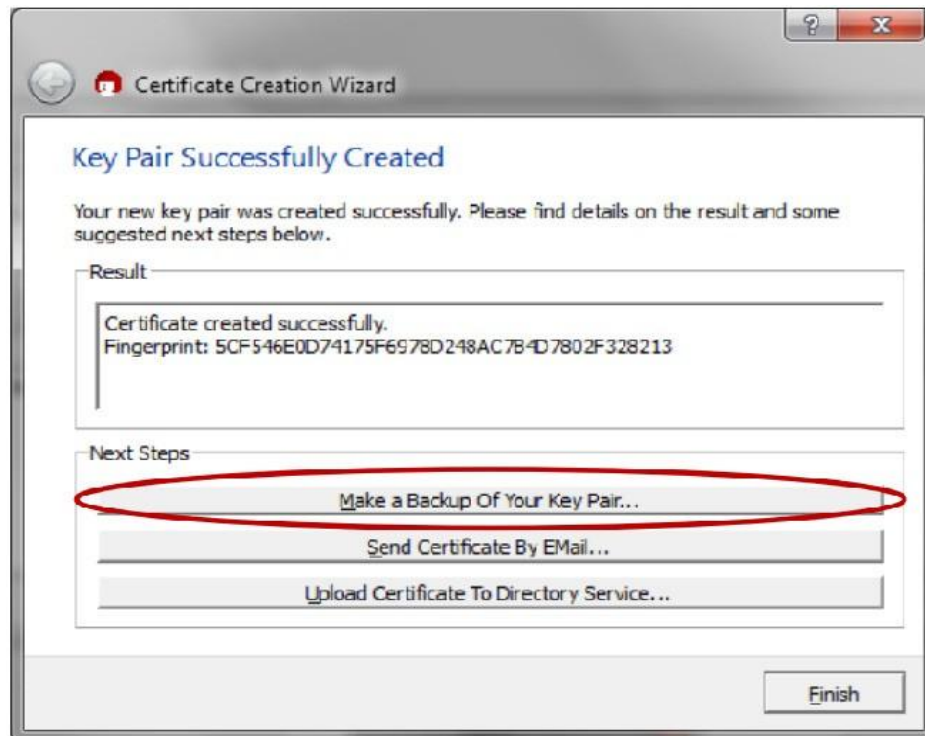
10. You will be asked to re-enter the passphrase



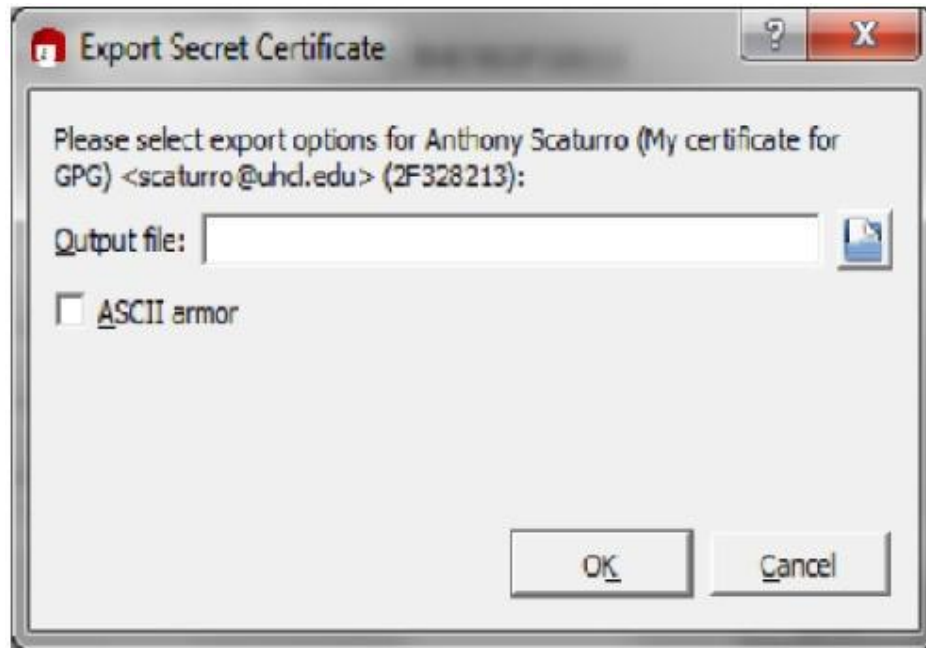
11. Re-enter the passphrase value. Then click the “OK” button. If the passphrases match, the certificate will be created.



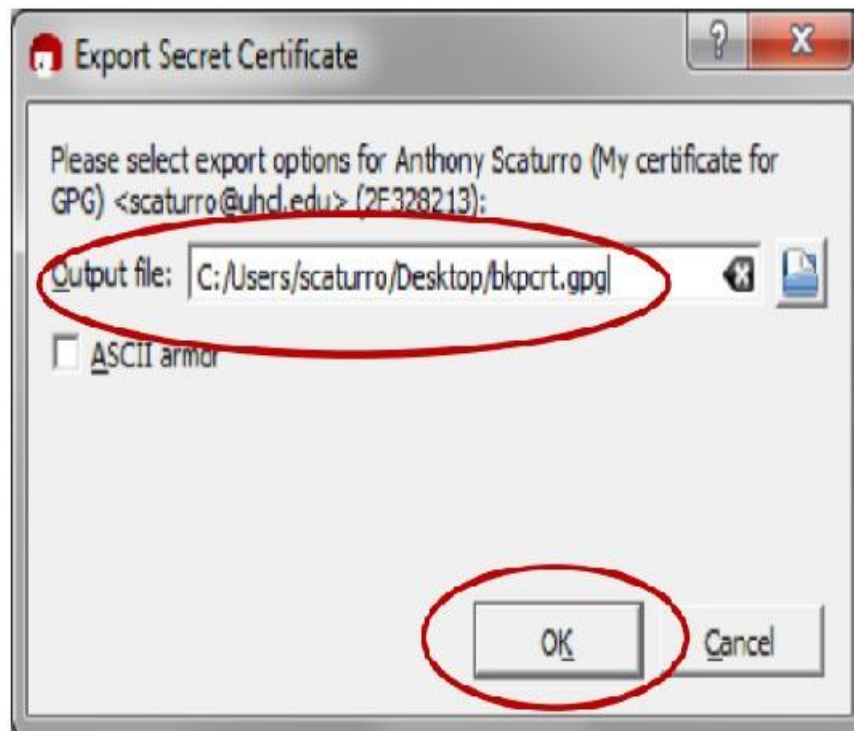
12. Once the certificate is created, the following screen will be displayed. You can save a backup of your public and private keys by clicking the “Make a backup Of Your Key Pair” button. This backup can be used to copy certificates onto other authorized computers.



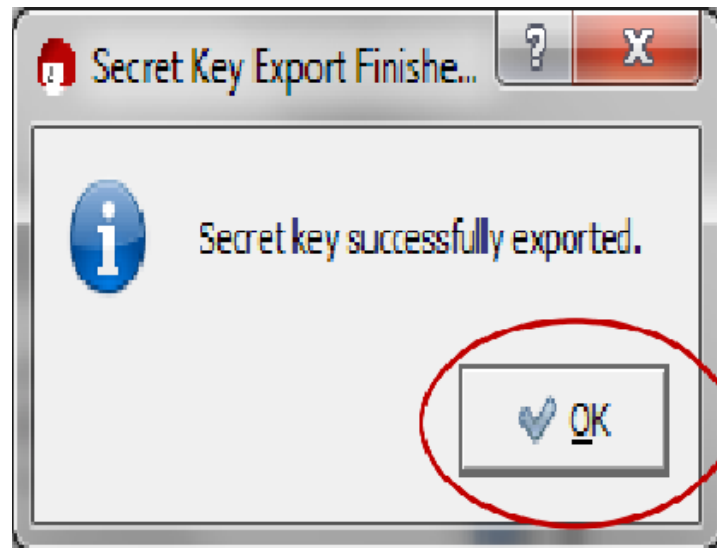
13. If you choose to backup your key pair, you will be presented with the following screen:



14. Specify the folder and name the file. Then click the "OK" button.



15. After the key is exported, the following will be displayed. Click the “OK” button.



16. You will be returned to the “Key Pair Successfully Created” screen. Click the “Finish” button.

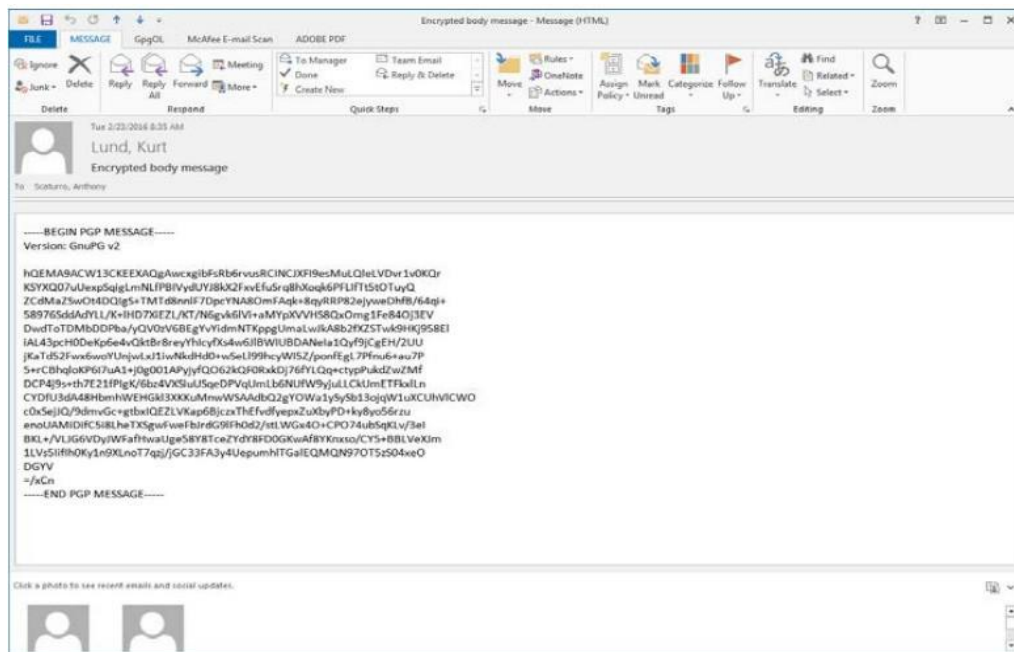


17. Before the program closes, you will need to confirm that you want to close the program by clicking on the “Quit Kleopatra” button

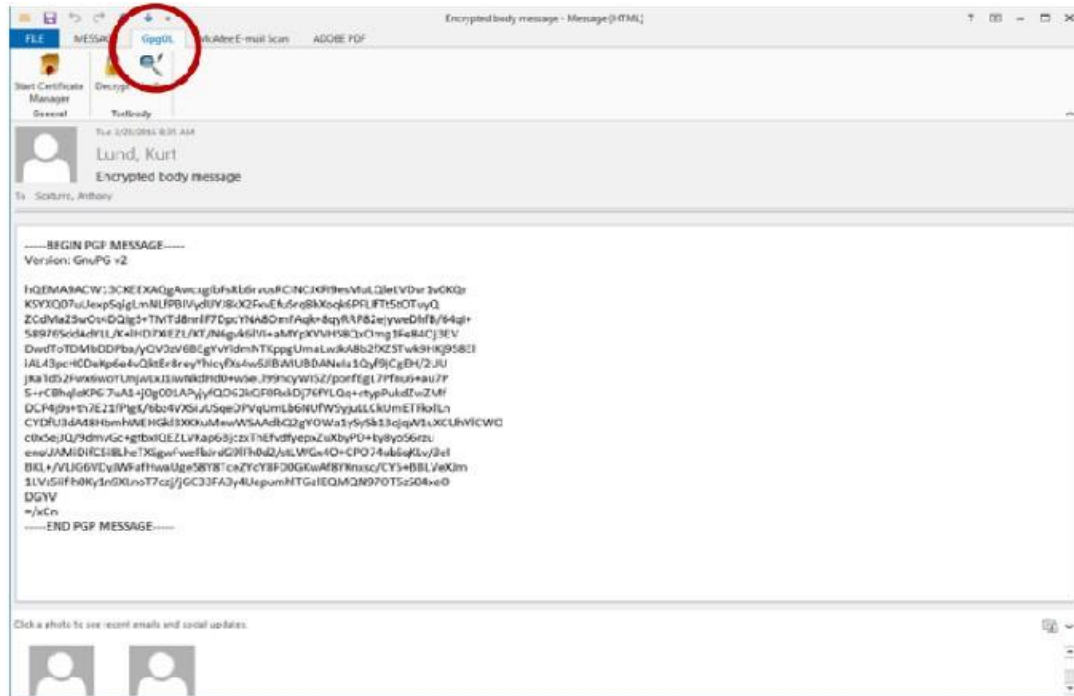


DECRYPTING AN ENCRYPTED E-MAIL THAT HAS BEEN SENT TO YOU:

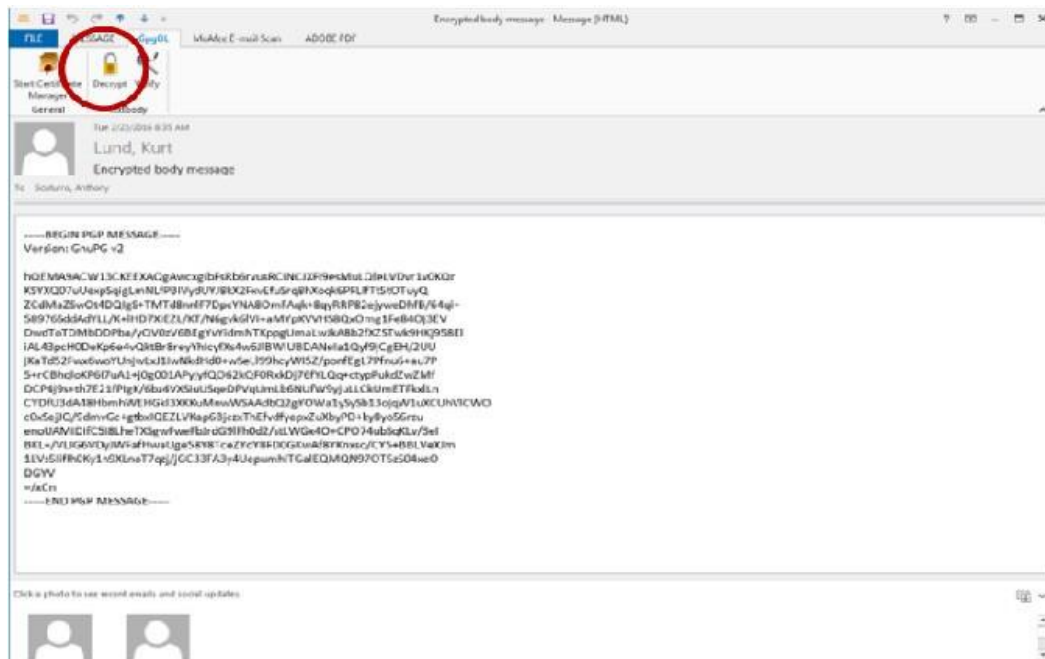
1. Open the e-mail message



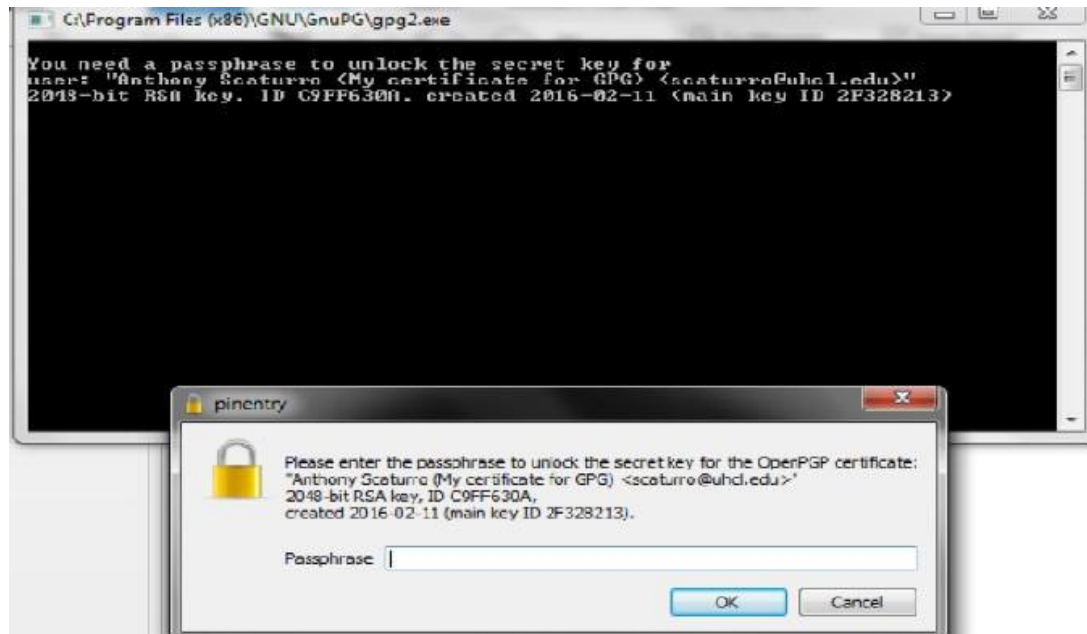
2. Select the GpgOL tab



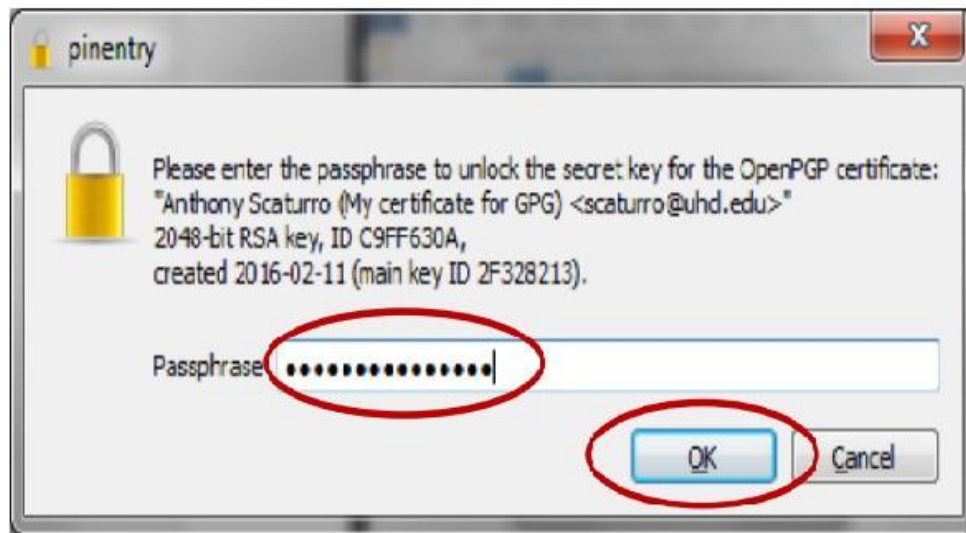
3. Click the "Decrypt" button



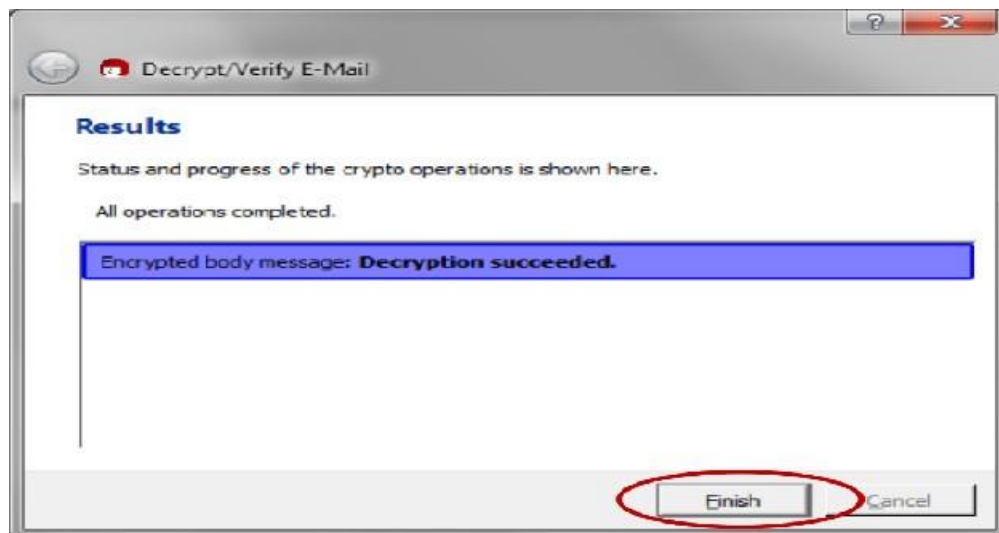
4. A command window will open along with a window that asks for the Passphrase to your private key that will be used to decrypt the incoming message.



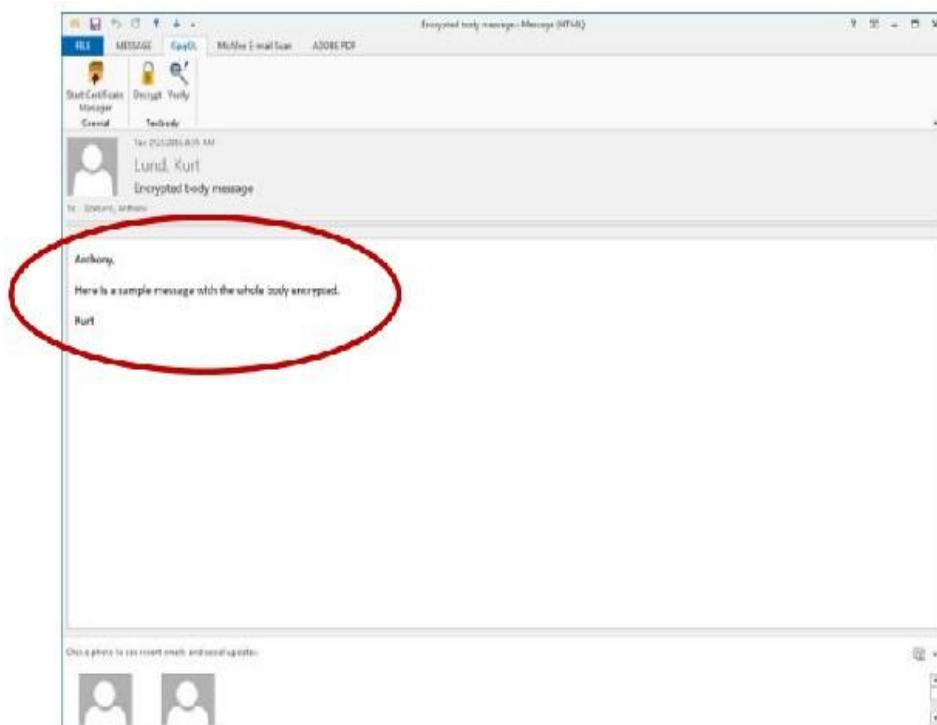
5. Enter your passphrase and click the “OK” button



6. The results window will tell you if the decryption succeeded. Click the “Finish” button to close the window



7. Your unencrypted e-mail message body will be displayed.



8. When you close the e-mail you will be asked if you want to save the e-mail message in its unencrypted form. For maximum security, click the “No” button. This will keep the message encrypted within the e-mail system and will require you to enter your passphrase each time you reopen the e-mail message



WORKING WITH KF SENSOR TOOL FOR CREATING AND MONITORING HONEYPOT

AIM:

Honey Pot is a device placed on Computer Network specifically designed to capture malicious network traffic. KF Sensor is the tool to setup as honeypot when KF Sensor is running it places a siren icon in the windows system tray in the bottom right of the screen. If there are no alerts then green icon is displayed.

INTRODUCTION:

HONEY POT:

A honeypot is a computer system that is set up to act as a decoy to lure cyber attackers, and to detect, deflect or study attempts to gain unauthorized access to information systems. Generally, it consists of a computer, applications, and data that simulate the behavior of a real system that appears to be part of a network but is actually isolated and closely monitored. All communications with a honeypot are considered hostile, as there's no reason for legitimate users to access a honeypot. Viewing and logging this activity can provide an insight into the level and types of threat a network infrastructure faces while distracting attackers away from assets of real value. Honeypots can be classified based on their deployment (use/action) and based on their level of involvement.

Based on deployment, honey pots may be classified as:

1. Production honey pots
2. Research honey pots

Production honey pots are easy to use, capture only limited information, and are used primarily by companies or corporations. Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honey pots.

Research honey pots are run to gather information about the motives and tactics of the Black hat community targeting different networks. These honey pots do not add direct value to a specific organization; instead, they are used to research the threats that organizations face and to learn how to better protect against those threats.

KF SENSOR:

KFSensor is a Windows based honey pot Intrusion Detection System (IDS). It acts as a honey pot to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By acting as a decoy server it can divert attacks from critical systems and provide a higher level of information than can be achieved by using firewalls and NIDS alone. KFSensor is a system installed in a network in order to divert and study an attacker's behavior. This is a new technique that is very effective in detecting attacks.

The main feature of KFSensor is that every connection it receives is a suspect hence it results in very few false alerts. At the heart of KFSensor sits a powerful internet daemon service that is built to handle multiple ports and IP addresses. It is written to resist denial of service and buffer overflow attacks. Building on this flexibility KFSensor can respond to connections in a variety of ways, from simple port listening and basic services (such as echo), to complex simulations of standard system services. For the HTTP protocol KFSensor accurately simulates the way Microsoft's web server (IIS) responds to both valid and invalid requests. As well as being able to host a website it also handles complexities such as range requests and client side cache negotiations. This makes it extremely difficult for an attacker to fingerprint, or identify KFSensor as a honey pot.

PROCEDURE:

STEP-1: Download KF Sensor Evaluation Setup File from KF Sensor Website.

STEP-2: Install with License Agreement and appropriate directory path.

STEP-3: Reboot the Computer now. The KF Sensor automatically starts during windows boot.

STEP-4: Click Next to setup wizard.

STEP-5: Select all port classes to include and Click Next.

STEP-6: "Send the email and Send from email", enter the ID and Click Next.

STEP-7: Select the options such as Denial of Service[DOS], Port Activity, Proxy Emulsion, Network Port Analyzer, Click Next.

STEP-8: Select Install as System service and Click Next.

STEP-9: Click finish.

SCREENSHOTS:

KFSensor Professional - Evaluation Trial

File View Scenario Signatures Settings Help

Localhost

0 Closed TCP Ports
24 **HTTP - Error**
25 SMTP
53 DNS
63 DHCP
80 **HTTP - Recent**
110 POP3
119 NNTP
145 **MSRPC - Error**
139 NETSession5...
339 LDAP
443 HTTPS
445 **NETSMB - Error**
593 GSS
1328 MSCS
1300 SOCKS
1388 SQL Server
2234 DirectPlay
3128 GlobalProxy
3156 Global Dial...
3889 Terminal Ser...
5100 MSN Messenger
5157 Web Service...
8180 IIS Proxy

0 Closed UDP Ports
42 XING UDP
67 **DHCP - Recent**
68 **DHCP Client**
83 Keberos
137 NETName Ser...
130 **NET Datagram**
151 SNMP

ID	Start	Duration	Pr...	Ser...	Name	Ysior	Sig. Message	Received
26	3/1/2012 9:54:40 AM 656	0.010	UDP	128	NET Datagram ...	BTPS-PC		NET DGRAM Packet: id:...
25	3/1/2012 9:54:25 AM 015	0.010	TCP	80	IIS	COMP2	IIS view script s...	PROFFIND / Canon.BP...
24	3/1/2012 9:54:25 AM 015	0.010	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1...
23	3/1/2012 9:54:11 AM 343	0.010	UDP	128	NET Datagram ...	COM15		NET DGRAM Packet: id:...
22	3/1/2012 9:53:28 AM 968	0.010	TCP	80	IIS	COMP2	IIS view script s...	PROFFIND / Canon.BP...
21	3/1/2012 9:53:28 AM 968	0.010	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1...
20	3/1/2012 9:53:22 AM 328	0.010	UDP	128	NET Datagram ...	COMPUTER14		NET DGRAM Packet: id:...
19	3/1/2012 9:53:09 AM 093	0.010	UDP	128	NET Datagram ...	FRONTOFFICEPC		NET DGRAM Packet: id:...
18	3/1/2012 9:52:56 AM 453	0.010	UDP	128	NET Datagram ...	COM1		NET DGRAM Packet: id:...
17	3/1/2012 9:52:54 AM 656	0.010	UDP	128	NET Datagram ...	COM15		NET DGRAM Packet: id:...
16	3/1/2012 9:52:54 AM 659	0.010	UDP	128	NET Datagram ...	COM15		NET DGRAM Packet: id:...
15	3/1/2012 9:52:42 AM 046	0.010	UDP	68	DHCP Client	192.168.1.1		[02 01 05 00 00 00 00 00]
14	3/1/2012 9:52:46 AM 234	0.010	UDP	67	DHCP	com15		DHCP: Boot Request: [00 01 05 00 00 00 00 00]
13	3/1/2012 9:52:41 AM 734	0.010	UDP	128	NET Datagram ...	CIVILDEPT		NET DGRAM Packet: id:...
12	3/1/2012 9:52:36 AM 750	0.010	UDP	128	NET Datagram ...	BTPS-PC		NET DGRAM Packet: id:...
11	3/1/2012 9:52:31 AM 078	0.010	UDP	67	DHCP	BTPS-PC		DHCP: Boot Request: [00 01 05 00 00 00 00 00]
10	3/1/2012 9:52:26 AM 953	0.010	TCP	80	IIS	COMP2	IIS view script s...	PROFFIND / Canon.BP...
9	3/1/2012 9:52:25 AM 000	0.015	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1...
8	3/1/2012 9:52:25 AM 015	0.010	TCP	80	IIS	COMP2	IIS view script s...	PROFFIND / Canon.BP...
7	3/1/2012 9:52:11 AM 582	0.010	UDP	128	NET Datagram ...	CIVILDEPT		NET DGRAM Packet: id:...
6	3/1/2012 9:52:06 AM 781	0.010	UDP	128	NET Datagram ...	com15		NET DGRAM Packet: id:...
5	3/1/2012 9:51:55 AM 031	0.010	UDP	128	NET Datagram ...	COM1		NET DGRAM Packet: id:...
4	3/1/2012 9:51:45 AM 937	0.010	UDP	128	NET Datagram ...	COM15		NET DGRAM Packet: id:...
3	3/1/2012 9:51:30 AM 508	0.010	UDP	128	NET Datagram ...	COM15		NET DGRAM Packet: id:...
2	3/1/2012 9:51:20 AM 974	0.010	UDP	68	DHCP Client	192.168.1.1		[02 01 05 00 00 00 00 00]
1	3/1/2012 9:51:20 AM 968	0.010	UDP	67	DHCP	com15		DHCP: Boot Request: [00 01 05 00 00 00 00 00]

KFSensor Professional - Evaluation Trial

File View Scenario Signatures Settings Help

Hosts

176.76.252.26 - Recent...
122.45.101.67 - Recent...
176.73.49.60 - Recent...
192.168.1.1 - Recent A...
192.168.1.1 - BTPS-PC...
192.168.1.52 - CIVILDE...
192.168.1.53 - FRONTO...
192.168.1.58 - COMPUT...
192.168.1.62 - COMP11...
192.168.1.5 - ELECTRI...
192.168.1.78 - COMP2...
192.168.1.73 - COMP1...
192.168.1.14 - com15...
192.168.1.1 - COM15...
222.107.67.174 - Rec...

ID	Start	Duration	Pr...	Ser...	Name	Ysior	Sig. Message	Received
44	3/1/2012 9:56:17 AM 395	0.000	UDP	1222	UDP Packet:	222.107.67.174		[0E 01 15 00 02] [0A...
43	3/1/2012 9:56:17 AM 177	0.000	UDP	1224	UDP Packet:	176.76.252.26		[CA 01 00 00 00 00 00 00]
42	3/1/2012 9:56:16 AM 895	0.000	UDP	1223	UDP Packet:	176.76.252.26		[CA 01 00 00 00 00 00 00]
41	3/1/2012 9:57:08 AM 968	0.000	UDP	67	DHCP	BTPS-PC		DHCP: Boot Request: [00 01 05 00 00 00 00 00]
40	3/1/2012 9:56:16 AM 213	0.000	UDP	1217	UDP Packet:	222.107.67.174		[07 00 00 00 00 00 00 00]
39	3/1/2012 9:56:25 AM 375	0.000	UDP	128	NET Datagram ...	com15		NET DGRAM Packet: id:...
38	3/1/2012 9:56:16 AM 147	0.000	UDP	1220	UDP Packet:	176.73.49.60		[E1 06 15 00 00 00 00 00]
37	3/1/2012 9:56:15 AM 821	0.000	UDP	1219	UDP Packet:	176.73.49.60		[0A 0F 12 00 0A 00 00 00]
36	3/1/2012 9:56:09 AM 128	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROFFIND / Canon.BP...
35	3/1/2012 9:56:09 AM 125	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1...
34	3/1/2012 9:56:15 AM 262	0.000	UDP	1218	UDP Packet:	122.45.101.67		[00 01 15 00 00 00 00 00]
33	3/1/2012 9:56:15 AM 049	0.000	UDP	1216	UDP Packet:	122.45.101.67		[61 00 00 00 00 00 00 00]
32	3/1/2012 9:56:14 AM 652	0.000	UDP	1215	UDP Packet:	122.45.101.67		[00 00 00 00 00 00 00 00]
31	3/1/2012 9:55:54 AM 406	0.000	UDP	128	NET Datagram ...	ELECTRICALDEPT		NET DGRAM Packet: id:...
30	3/1/2012 9:55:29 AM 093	0.016	TCP	80	IIS	COMP2	IIS view script s...	PROFFIND / Canon.BP...
29	3/1/2012 9:55:29 AM 045	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1...
28	3/1/2012 9:55:28 AM 068	0.000	UDP	68	DHCP Client	192.168.1.1		[02 01 05 00 00 00 00 00]
27	3/1/2012 9:55:28 AM 078	0.000	UDP	67	DHCP	com15		DHCP: Boot Request: [00 01 05 00 00 00 00 00]
26	3/1/2012 9:54:40 AM 656	0.000	UDP	128	NET Datagram ...	BTPS-PC		NET DGRAM Packet: id:...
25	3/1/2012 9:54:29 AM 015	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROFFIND / Canon.BP...
24	3/1/2012 9:54:29 AM 015	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1...
23	3/1/2012 9:54:11 AM 343	0.000	UDP	128	NET Datagram ...	COM15		NET DGRAM Packet: id:...
22	3/1/2012 9:53:28 AM 968	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROFFIND / Canon.BP...
21	3/1/2012 9:53:28 AM 968	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1...
20	3/1/2012 9:53:22 AM 328	0.000	UDP	128	NET Datagram ...	COMPUTER14		NET DGRAM Packet: id:...
19	3/1/2012 9:53:09 AM 093	0.000	UDP	128	NET Datagram ...	FRONTOFFICEPC		NET DGRAM Packet: id:...
18	3/1/2012 9:52:56 AM 453	0.000	UDP	128	NET Datagram ...	COM1		NET DGRAM Packet: id:...
17	3/1/2012 9:52:54 AM 656	0.000	UDP	128	NET Datagram ...	COM15		NET DGRAM Packet: id:...
16	3/1/2012 9:52:54 AM 659	0.000	UDP	128	NET Datagram ...	COM15		NET DGRAM Packet: id:...
15	3/1/2012 9:52:42 AM 046	0.000	UDP	68	DHCP Client	192.168.1.1		[02 01 05 00 00 00 00 00]
14	3/1/2012 9:52:46 AM 234	0.000	UDP	67	DHCP	com15		DHCP: Boot Request: [00 01 05 00 00 00 00 00]
13	3/1/2012 9:52:41 AM 734	0.000	UDP	128	NET Datagram ...	CIVILDEPT		NET DGRAM Packet: id:...
12	3/1/2012 9:52:36 AM 750	0.000	UDP	128	NET Datagram ...	BTPS-PC		NET DGRAM Packet: id:...
11	3/1/2012 9:52:31 AM 078	0.000	UDP	67	DHCP	BTPS-PC		DHCP: Boot Request: [00 01 05 00 00 00 00 00]
10	3/1/2012 9:52:26 AM 953	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROFFIND / Canon.BP...
9	3/1/2012 9:52:25 AM 000	0.015	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1...

Server: Canon.BP... Path: /...
Server: Canon.BP... Path: /...

Wireshark Professional - Evaluation Trial									
View Statistics Packets Settings Help									
Filters	Time	Duration	Protocol	Series	Name	Vendor	Sig. Message	Received	
0.0.0.0 - 255.255.255.255	2012.9.18.10.21.27	0.000	UDP	1523	UDP Packet	MIKROSOFT-6556EA		0107700E 0C05B0 A6E5A68...	
24.54.76.192 - Recv...	2012.9.18.10.21.27	0.000	UDP	1522	UDP Packet	MIKROSOFT-6556EA		1E051A00 C596E7 AC0F1606...	
31.131.181.158 - Recv...	2012.10.10.10.29 AM...	0.016	TCP	80	IS	COMP2	CS View Sock. S...	PROPFIND /CanonUP-HTTP	
46.49.293.12 - Recv...	2012.10.10.10.29 AM...	0.000	TCP	80	IS	COMP2	CS View Sock. S...	OPTIONS /HTTP	
46.626.244 - M0000...	2012.9.18.10.21.27	0.000	UDP	1520	UDP Packet	78.97.105.133		041F1310 0E45C03E 14E0...	
46.102.17.223 - Recv...	2012.9.18.10.21.27	0.000	UDP	1518	UDP Packet	78.97.105.133		041F0000 054040A4 07C7B7...	
46.100.169.132 - Recv...	2012.9.18.10.21.27	0.000	UDP	1516	UDP Packet	112.206.103.74.pkt...		0C050000 054040A4 07C7B7...	
46.241.110.25 - Recv...	2012.9.18.10.21.27	0.000	UDP	1515	UDP Packet	112.206.103.74.pkt...		1E051A00 0C05B0 A6E5A68...	
49.248.13.190 - S000...	2012.9.18.10.21.27	0.000	UDP	1514	UDP Packet	78.111.104.187		041F1310 0E45C03E 14E0...	
50.177.151.26 - Recv...	2012.9.18.10.21.27	0.000	UDP	1513	UDP Packet	78.111.104.187		041F0000 054040A4 07C7B7...	
59.23.151.204 - Recv...	2012.9.18.10.21.27	0.000	UDP	1510	UDP Packet	109-179-82-171.net...		0C050000 054040A4 07C7B7...	
59.126.122.92 - Recv...	2012.9.18.10.21.27	0.000	UDP	1507	UDP Packet	CANEXAS		0B0B11 0000 0C05B0 A6E5A68...	
59.144.55.226 - Recv...	2012.9.18.10.21.27	0.000	UDP	1509	UDP Packet	smtp.tlvs.co.in		A2770000 190E190E190E190E...	
59.148.20.211 - 009...	2012.9.18.10.21.27	0.000	UDP	1508	UDP Packet	smtp.tlvs.co.in		0B0B11 0000 0C05B0 A6E5A68...	
61.34.107.100 - Recv...	2012.9.18.10.21.27	0.000	UDP	1509	UDP Packet	customer.444131.meg...		1E051A00 0C05B0 A6E5A68...	
71.43.42.154 - 110F...	2012.9.18.10.21.27	0.000	UDP	1503	UDP Packet	base02d5.vetusa.com.jp		R...0077 330E 0E45C03E 14E0...	
72.258.93.227 - Recv...	2012.9.18.10.21.27	0.000	UDP	1502	UDP Packet	base02d5.vetusa.com.jp		1E051A00 0C05B0 A6E5A68...	
70.00.251.50 - Recv...	2012.9.18.10.21.27	0.000	UDP	1501	UDP Packet	customer.444131.meg...		1E051A00 0C05B0 A6E5A68...	
70.97.165.139 - Recv...	2012.9.18.10.21.27	0.000	UDP	1499	UDP Packet	CC_0004		F1700000 054040A4 07C7B7...	
70.97.160.74 - Recv...	2012.9.18.10.21.27	0.000	UDP	1494	UDP Packet	CC_0004		A6151500 0C05B0 A6E5A68...	
70.111.104.187 - Recv...	2012.10.09.12.09 AM...	0.000	TCP	80	IS	COMP2	CS View Sock. S...	PROPFIND /CanonUP-HTTP	
79.114.172.206 - 7...	2012.10.09.12.09 AM...	0.000	TCP	80	IS	COMP2	CS View Sock. S...	OPTIONS /HTTP	
79.125.49.51 - 1B-0...	2012.9.18.10.21.27	0.000	UDP	1492	UDP Packet	112.206.103.74.pkt...		0C050000 054040A4 07C7B7...	
70.170.188.185 - Recv...	2012.9.18.10.21.27	0.000	UDP	1491	UDP Packet	112.206.103.74.pkt...		0C051A00 0C05B0 A6E5A68...	
82.00.130.160 - Recv...	2012.9.18.11.07.29...	0.000	UDP	1490	UDP Packet	178-168-14-215.stat...		0C120000 054040A4 07C7B7...	
84.240.34.146 - AC...	2012.9.18.11.07.29...	0.000	UDP	1489	UDP Packet	178-168-14-215.stat...		1F400000 054040A4 07C7B7...	
85.122.41.1194 - Recv...	2012.9.18.10.21.27	0.000	UDP	1489	UDP Packet	109-74-127-249.meg...		041F0000 054040A4 07C7B7...	
85.204.143.139 - Recv...	2012.9.18.10.21.27	0.000	UDP	1484	UDP Packet	109-74-127-249.meg...		0C051600 0630F3 E064154F5F...	
87.67.22.1227 - 02...	2012.9.18.10.21.27	0.000	UDP	1480	UDP Packet	ACER		1F400000 0630F3 E064154F5F...	
88.80.167.140 - HO...	2012.9.18.10.21.27	0.000	UDP	1479	UDP Packet	ACER		AN000000 301E190E190E190E...	
88.208.268.162 - co...	2012.9.18.10.21.27	0.000	UDP	1472	UDP Packet	CHANGHEE		1E051A00 0C05B0 A6E5A68...	
89.423.159.230 - Recv...	2012.9.18.10.21.27	0.000	UDP	1470	UDP Packet	CHANGHEE		041F0000 054040A4 07C7B7...	
92.141.41.13.51 - Recv...	2012.9.18.10.21.27	0.000	UDP	1470	UDP Packet	78.97.160.74		0C051600 0630F3 E064154F5F...	
92.141.41.13.51 - Recv...	2012.9.18.10.21.27	0.000	UDP	1469	UDP Packet	78.97.160.74		041F0000 054040A4 07C7B7...	
93.182.250.195 - Recv...	2012.9.18.10.21.27	0.000	UDP	1468	UDP Packet	112.206.103.74.pkt...		0C051600 0630F3 E064154F5F...	

INSTALLATION OF ROOTKITS

AIM:

Root kit is a stealth type of malicious software designed to hide the existence of certain process from normal methods of detection and enables continued privileged access to a computer.

INTRODUCTION:

Breaking the term rootkit into the two component words, root and kit, is a useful way to define it. Root is a UNIX/Linux term that's the equivalent of Administrator in Windows. The word kit denotes programs that allow someone to obtain root/admin-level access to the computer by executing the programs in the kit — all of which is done without end-user consent or knowledge.

A root kit is a type of malicious software that is activated each time your system boots up. Root kits are difficult to detect because they are activated before your system's Operating System has completely booted up. A root kit often allows the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Root kits are able to intercept data from terminals, network connections, and the keyboard.

Root kits have two primary functions: remote command/control (back door) and software eavesdropping. Root kits allow someone, legitimate or otherwise, to administratively control a computer. This means executing files, accessing logs, monitoring user activity, and even changing the computer's configuration. Therefore, in the strictest sense, even versions of VNC are root kits. This surprises most people, as they consider root kits to be solely malware, but in of themselves they aren't malicious at all.

The presence of a root kit on a network was first documented in the early 1990s. At that time, Sun and Linux operating systems were the primary targets for a hacker looking to install a root kit. Today, root kits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

PROCEDURE:

STEP-1: Download Root kit Tool from GMER website www.gmer.net.

STEP-2: This displays the Processes, Modules, Services, Files, Registry, RootKit / Malwares, Autostart, CMD of local host.

STEP-3: Select Processes menu and kill any unwanted process if any.

STEP-4: Modules menu displays the various system files like .sys, .dll

STEP-5: Services menu displays the complete services running with Auto start, Enable, Disable, System, Boot.

STEP-6: Files menu displays full files on Hard-Disk volumes.

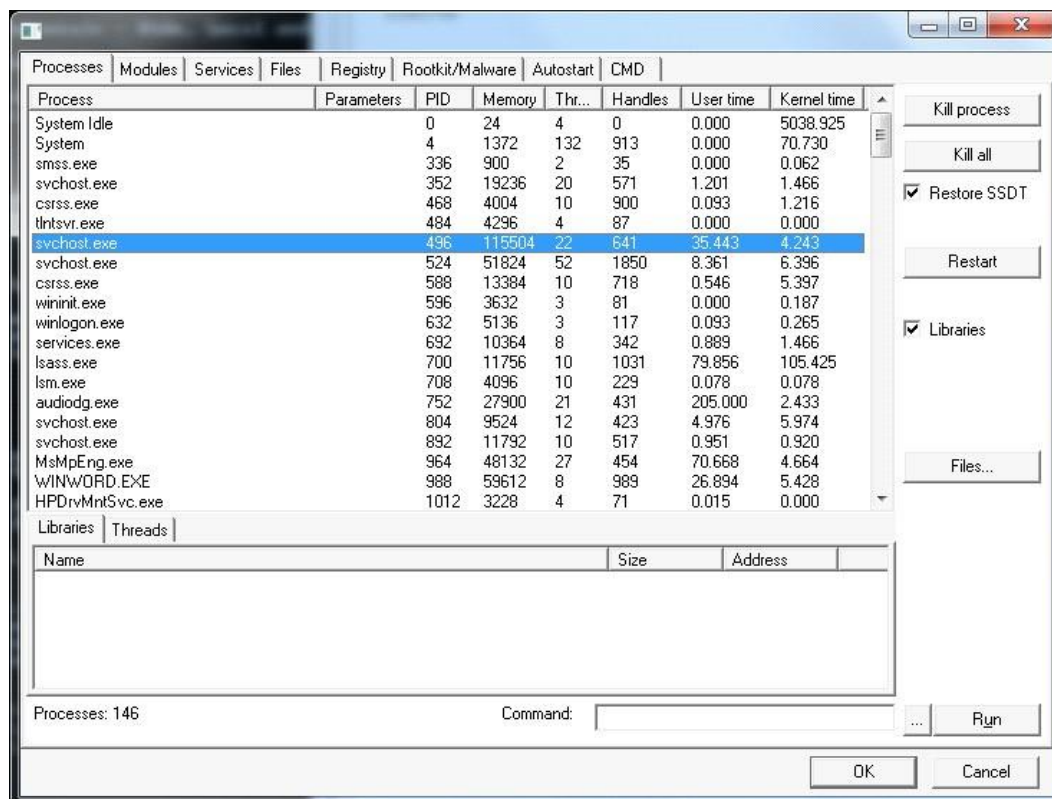
STEP-7: Registry displays Hkey_Current_user and Hkey_Local_Machine.

STEP-8: Root kits / Malwares scans the local drives selected.

STEP-9: Auto start displays the registry base Auto start applications.

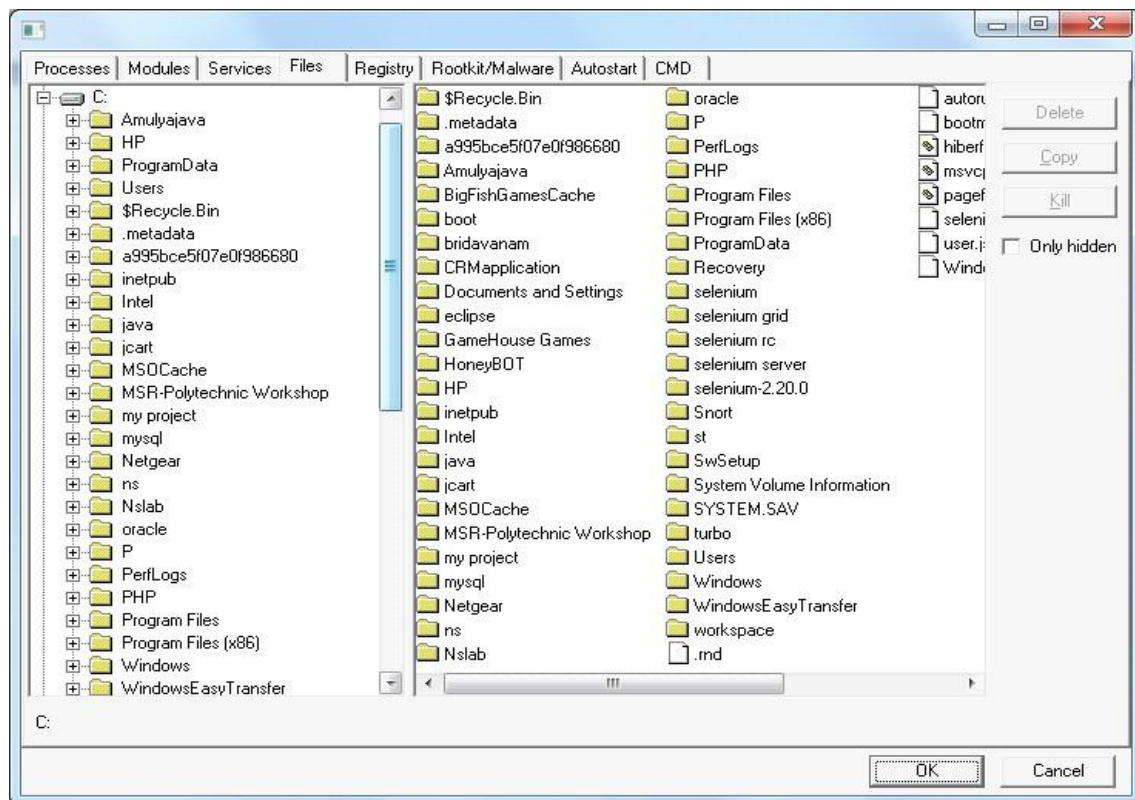
STEP-10: CMD allows the user to interact with command line utilities or Registry

SCREENSHOTS:



Processes Modules Services Files Registry Rootkit/Malware Autostart CMD					
Name	File	Address	Size		
ntoskrnl.exe	\SystemRoot\system32\ntoskrnl.exe	0305C000	6193152		
hal.dll	\SystemRoot\system32\hal.dll	03013000	299008		
kdcom.dll	\SystemRoot\system32\kdcom.dll	00B0C000	40960		
mcupdate_Genui...	\SystemRoot\system32\mcupdate_GenuineIntel.dll	00C00000	323584		
PSHED.dll	\SystemRoot\system32\PSHED.dll	00C4F000	81920		
CLFS.SYS	\SystemRoot\system32\CLFS.SYS	00C63000	385024		
Cl.dll	\SystemRoot\system32\Cl.dll	00CC1000	786432		
Wd01000.sys	\SystemRoot\system32\drivers\Wd01000.sys	00EA3000	671744		
WDFLDR.SYS	\SystemRoot\system32\drivers\WDFLDR.SYS	00F47000	61440		
ACPI.sys	\SystemRoot\system32\drivers\ACPI.sys	00F56000	356352		
WMILIB.SYS	\SystemRoot\system32\drivers\WMILIB.SYS	00FAD000	36864		
msisadrv.sys	\SystemRoot\system32\drivers\msisadrv.sys	00FB6000	40960		
pci.sys	\SystemRoot\system32\drivers\pci.sys	00FC0000	208896		
vdroot.sys	\SystemRoot\system32\drivers\vdroot.sys	00FF3000	53248		
partmgr.sys	\SystemRoot\system32\drivers\partmgr.sys	00E00000	86016		
compbatt.sys	\SystemRoot\system32\DRIVERS\compbatt.sys	00E15000	36864		
BATT.C.SYS	\SystemRoot\system32\DRIVERS\BATT.C.SYS	00E1E000	49152		
volmgr.sys	\SystemRoot\system32\drivers\volmgr.sys	00E2A000	86016		
volmgrx.sys	\SystemRoot\system32\drivers\volmgrx.sys	00E3F000	376832		
mountmgr.sys	\SystemRoot\system32\drivers\mountmgr.sys	00D61000	106496		
iaStor.sys	\SystemRoot\system32\DRIVERS\iaStor.sys	0103A000	2138112		
atap.sys	\SystemRoot\system32\drivers\atap.sys	01244000	36864		
ataport.SYS	\SystemRoot\system32\drivers\ataport.SYS	0124D000	172032		
msahci.sys	\SystemRoot\system32\drivers\msahci.sys	01277000	45056		
PCIIDE.SYS	\SystemRoot\system32\drivers\PCIIDE.SYS	01282000	65536		
amdxdm.sys	\SystemRoot\system32\drivers\amdxdm.sys	01292000	45056		
fltmgr.sys	\SystemRoot\system32\drivers\fltmgr.sys	0129D000	311296		
fileinfo.sys	\SystemRoot\system32\drivers\fileinfo.sys	012E9000	81920		
Ntfs.sys	\SystemRoot\system32\drivers\Ntfs.sys	0142D000	1716224		
msrpc.sys	\SystemRoot\system32\drivers\msrpc.sys	012FD000	385024		
ksecdd.sys	\SystemRoot\system32\drivers\ksecdd.sys	015D0000	110532		
...		

Processes Modules Services Files Registry Rootkit/Malware Autostart CMD				
Name	Start	File name	Description	
.NET CLR Data				
.NET CLR Netwo...				
.NET CLR Netwo...				
.NET Data Provid...				
.NET Data Provid...				
.NET Framework				
1394ohci	MANUAL	\SystemRoot\system32\drivers\1394ohci.sys	1394 OHCI Compliant Host Controller	
ACPI	BOOT	system32\drivers\ACPI.sys	Microsoft ACPI Driver	
AcpiPmi	MANUAL	\SystemRoot\system32\drivers\acpipmi.sys	ACPI Power Meter Driver	
adp94xx	MANUAL	\SystemRoot\system32\DRIVERS\adp94xx.sys		
adpahci	MANUAL	\SystemRoot\system32\DRIVERS\adpahci.sys		
adpu320	MANUAL	\SystemRoot\system32\DRIVERS\adpu320.sys		
adsi				
AeLookupSvc	MANUAL	%systemroot%\system32\svchost.exe -k netsvcs	@%SystemRoot%\system32\aelupsvc.dll,-2	
AERTFilters	AUTO	C:\Program Files\Realtek\Audio\HDA\AERTSr...	Andrea RT Filters Service	
AFD	SYSTEM	\SystemRoot\system32\drivers\afd.sys	@%systemroot%\system32\drivers\afd.sys,-1000	
AgereSoftModem	MANUAL	system32\DRIVERS\agrsm64.sys	Agere Systems Soft Modem	
agp440	MANUAL	\SystemRoot\system32\drivers\agp440.sys	Intel AGP Bus Filter	
ALG	MANUAL	%SystemRoot%\system32\alg.exe	@%SystemRoot%\system32\Alg.exe,-113	
aliide	MANUAL	\SystemRoot\system32\drivers\aliide.sys		
amdide	MANUAL	\SystemRoot\system32\drivers\amdide.sys		
AmdK8	MANUAL	\SystemRoot\system32\DRIVERS\amdK8.sys	AMD K8 Processor Driver	
AmdPPM	MANUAL	\SystemRoot\system32\DRIVERS\amdpdm.sys	AMD Processor Driver	
amdsata	MANUAL	\SystemRoot\system32\drivers\amdsata.sys		
amdsbs	MANUAL	\SystemRoot\system32\DRIVERS\amdsbs.sys		
amdxdm	BOOT	system32\drivers\amdxdm.sys		
AppHostSvc	AUTO	%windir%\system32\svchost.exe -k apphost	@%windir%\system32\inetsrv\iisres.dll,-30012	
AppID	MANUAL	\SystemRoot\system32\drivers\appid.sys	@%systemroot%\system32\appidsvc.dll,-103	
AppIDSvc	MANUAL	%SystemRoot%\system32\svchost.exe -k Local...	@%systemroot%\system32\appidsvc.dll,-101	
Appinfo	MANUAL	%SystemRoot%\system32\svchost.exe -k netsvcs	@%systemroot%\system32\appidinfo.dll,-101	
AppMgmt	MANUAL	%SystemRoot%\system32\svchost.exe -k netsvcs	@appmgmts.dll,-3251	
...



WORKING WITH NET STUMBLER TO PERFORM WIRELESS

AUDIT ON A ROUTER

AIM:

To perform wireless audit on an access point or a router and decrypt WEP and WPA (Net Stumbler).

INTRODUCTION:

NET STUMBLER:

Nets tumbler (Network Stumbler) is one of the Wi-Fi hacking tool which only compatible with windows, this tool also a freeware. With this program, we can search for wireless network which open and infiltrate the network. Its having some compatibility and network adapter issues. Nets tumbler is a tool for Windows that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP. A trimmed-down version called Minis tumbler is available for the handheld Windows CE operating system.

It has many uses:

- ✓ Verify that your network is set up the way you intended
- ✓ Find locations with poor coverage in your WLAN.
- ✓ Detect other networks that may be causing interference on your network
- ✓ Detect unauthorized "rogue" access points in your workplace
- ✓ Help aim directional antennas for long-haul WLAN links.
- ✓ Use it recreationally for WarDriving.

PROCEDURE:

STEP-1: Download and install Netstumbler.

STEP-2: It is highly recommended that the PC should have wireless network card in order to access wireless router.

STEP-3: Now Run Nets tumbler in record mode and configure wireless card.

STEP-4: There are several indicators regarding the strength of the signal, such as GREEN indicates Strong, YELLOW and other color indicates a weaker signal, RED indicates a very weak and GREY indicates a signal loss.

STEP-5: Lock symbol with GREEN bubble indicates the Access point has encryption enabled.

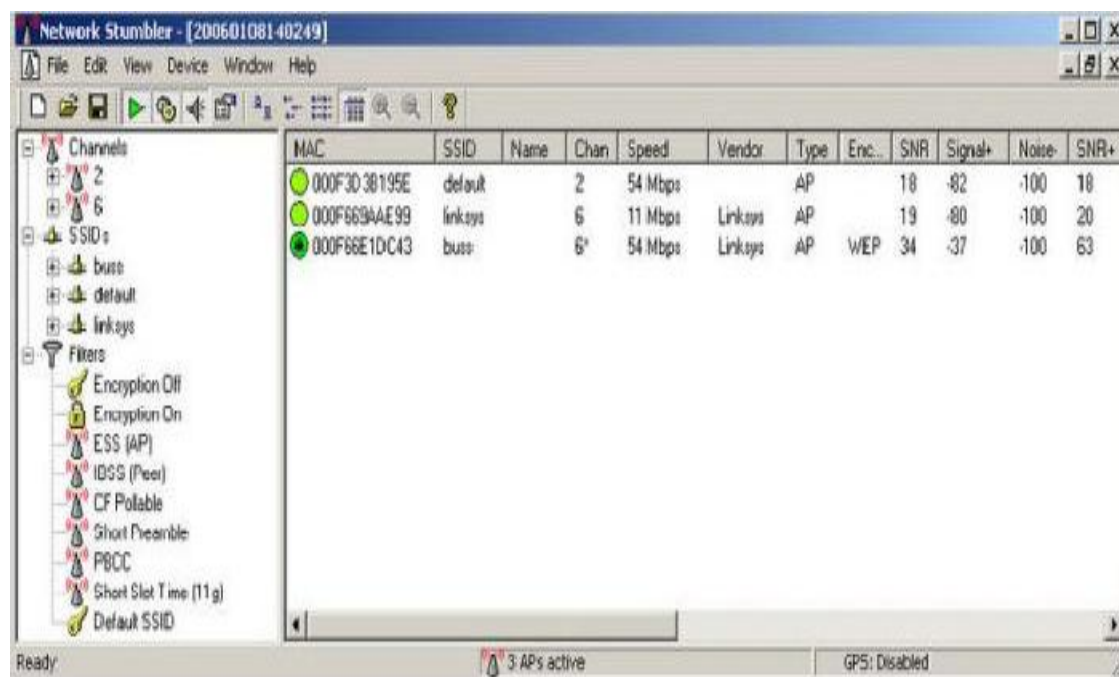
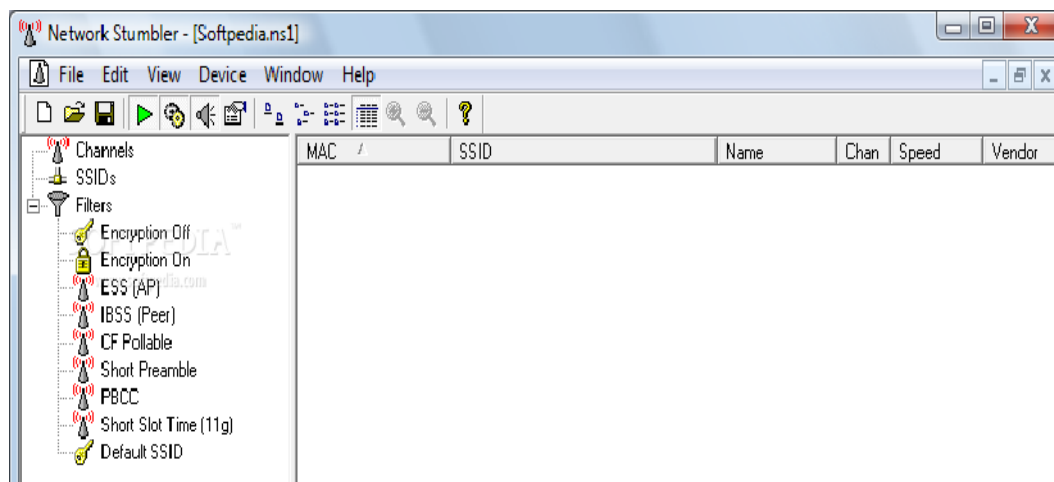
STEP-6: MAC assigned to Wireless Access Point is displayed on right hand pane.

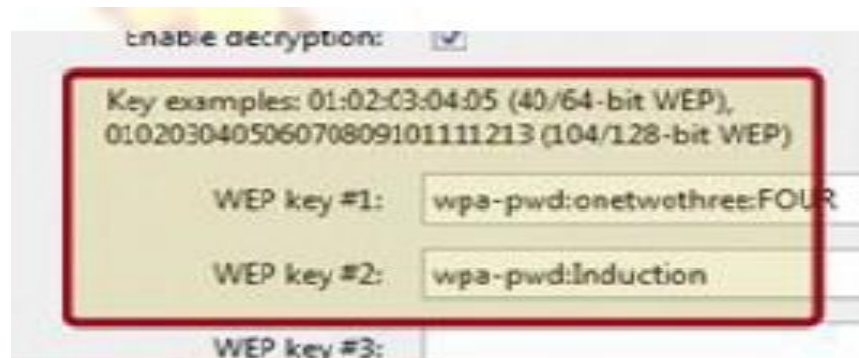
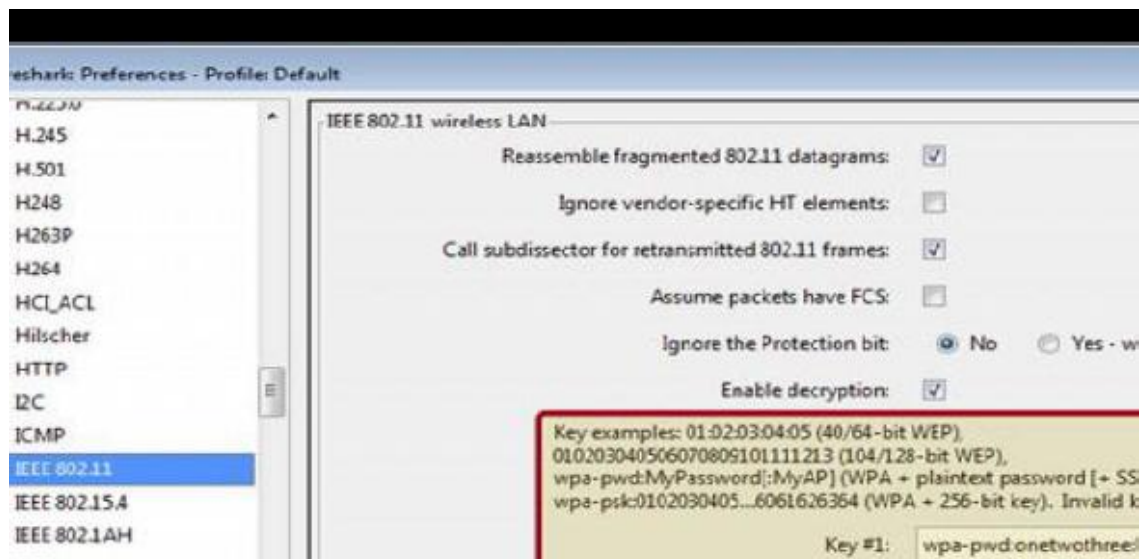
STEP-7: The next column displays the Access points Service Set Identifier[SSID] which is useful to crack the password.

STEP-8: To decrypt use Wire Shark tool by selecting Edit preferences IEEE 802.11.

STEP-9: Enter the WEP keys as a string of hexadecimal numbers as A1B2C3D4E5.

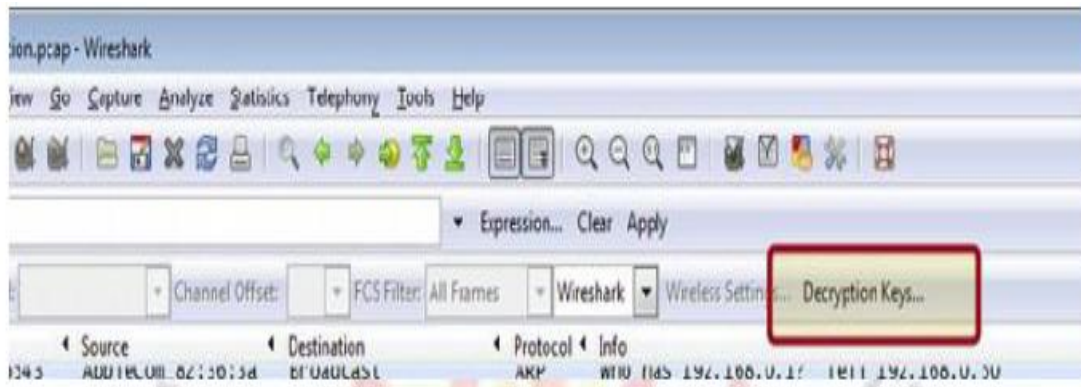
SCREENSHOTS:





Adding Keys: Wireless Toolbar

- If the system is having the Windows version of Wireshark and have an AirPcap adapter, then we can add decryption keys using the wireless toolbar.
- If the toolbar isn't visible, you can show it by selecting View Wireless Toolbar.
- Click on the Decryption Keys button on the toolbar:



- This will open the decryption key management window. As shown in the window you can select between three decryption modes: None, Wireshark and Driver:



AUTOMATED ATTACK AND PENETRATION TOOLS EXPLORING GN-STALKER, A VULNERABILITY ASSESSMENT TOOL

AIM:

To explore automated and penetration tools on network (KF Sensor)

PRELAB DISCUSSION:

HONEYPOTS

When it comes to computer security, honeypots are all the rage. Honeypots can detect unauthorized activities that might never be picked up by a traditional intrusion detection system. Furthermore, since almost all access to a honeypot is unauthorized, nearly everything in a honeypot's logs is worth paying attention to. Honeypots can act as a decoy to keep hackers away from your production servers. At the same time though, a honeypot can be a little tricky to deploy. In this article, I will walk you through the process of deploying a honeypot.

INTRODUCTION

There are many different types of honeypot systems. Honeypots can be hardware appliances or they can be software based. Software based honeypots can reside on top of a variety of operating systems. For the most part though, honeypots fall into two basic categories; real and virtual.

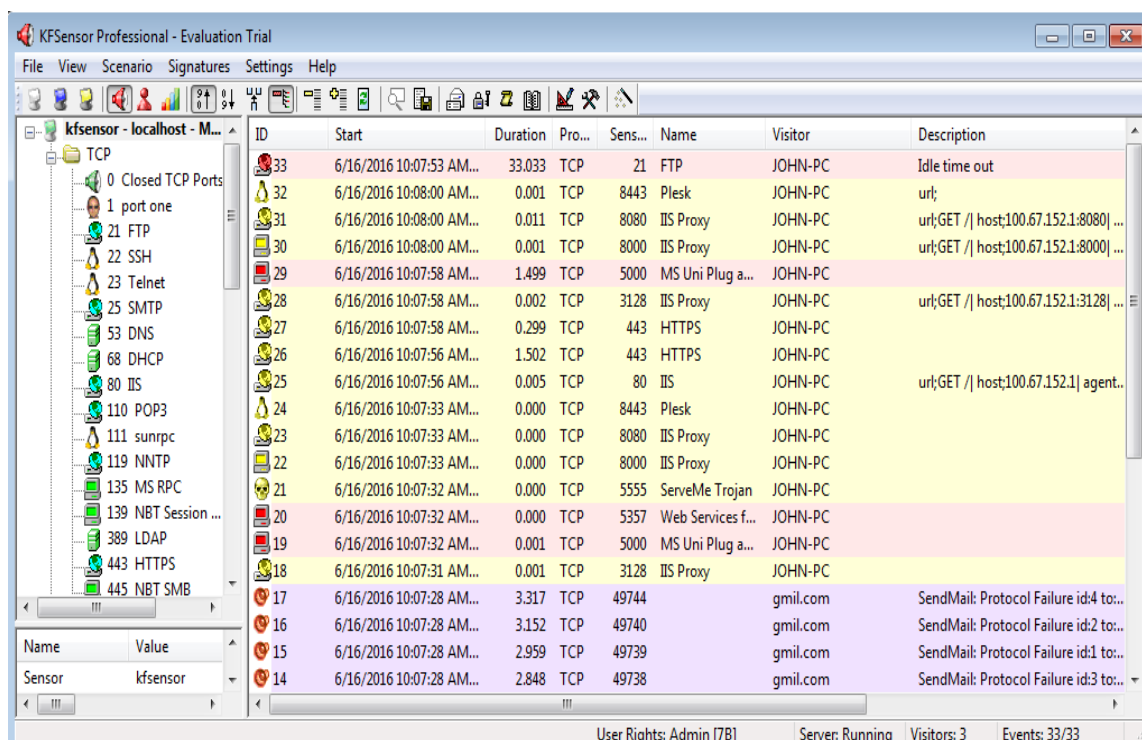
A virtual honeypot is essentially an emulated server. There are both hardware and software implementations of virtual honeypots. For example, if a network administrator was concerned that someone might try to exploit an FTP server, the administrator might deploy a honeypot appliance that emulates an FTP server.

Downloading and installing KF Sensor

- The KF Sensor download consists of a 1.7 MB self-extracting executable file.
- Download the file and copy it into an empty folder on your computer.
- When you double click on the file, it will launch a very basic Setup program.
- The only thing special that you need to know about the Setup process is that it will require a reboot

Using KFSensor

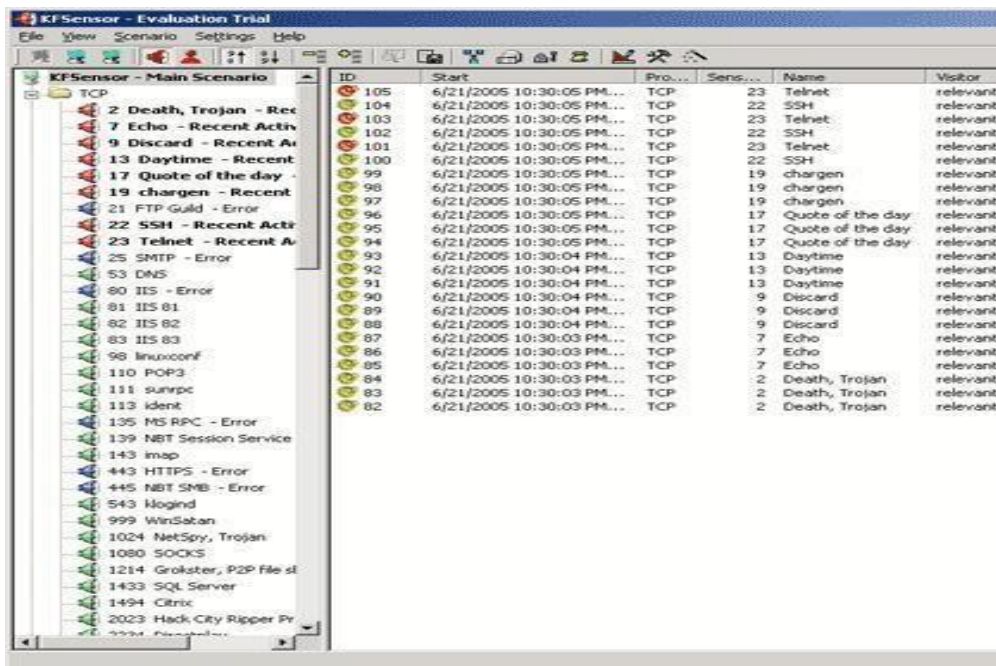
Step1: You will see the main KFSensor screen shown



- As you can see, the column on the left contains a list of port numbers and what the port is typically used for.
- If the icon to the left of a port listing is green, it means that KFSensor is actively monitoring that port for attacks.
- If the icon is blue, it means that there has been an error and KFSensor is not watching for exploits aimed at that particular port.

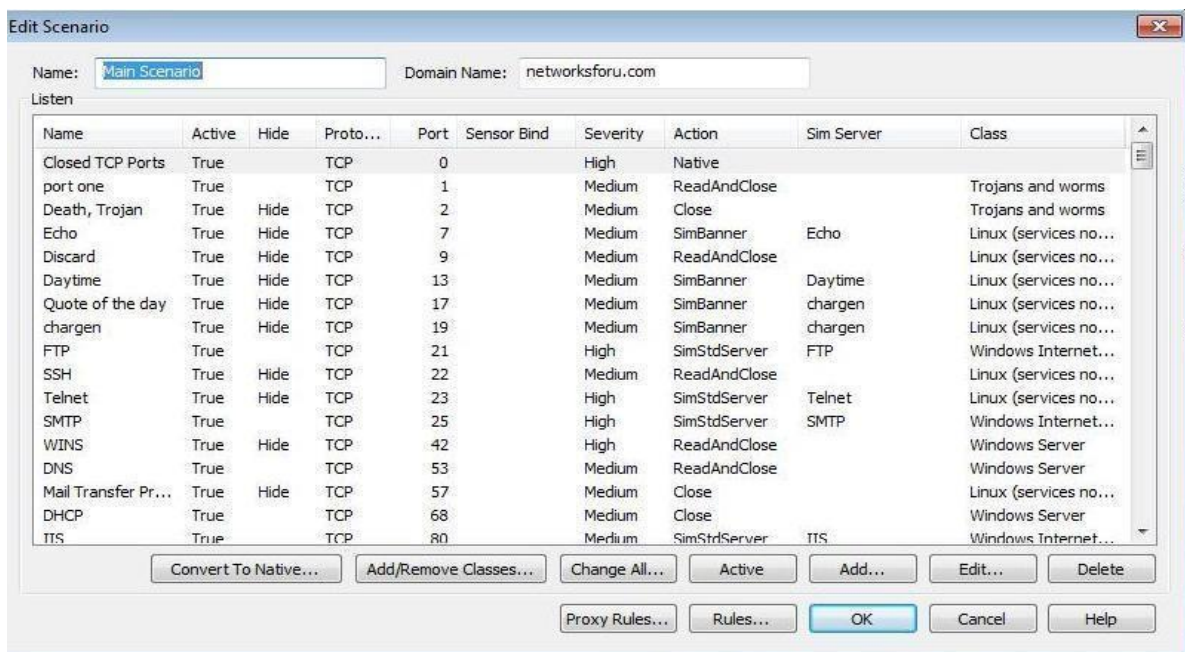
Testing the software

- Once you've got the software up and running, one of the best things that you can do is to test the software by launching a port scan against the machine that's running KFSensor.
 - For the port scan, we using the HostScan.
- It simply scans a block of IP addresses, looking for open ports. Figure B shows how the KFSensor reacts to a partial port scan.
- If you look at Figure B, you will notice that the icons next to ports that were scanned turn red to indicate recent activity.



Modifying the Honeypot's behavior

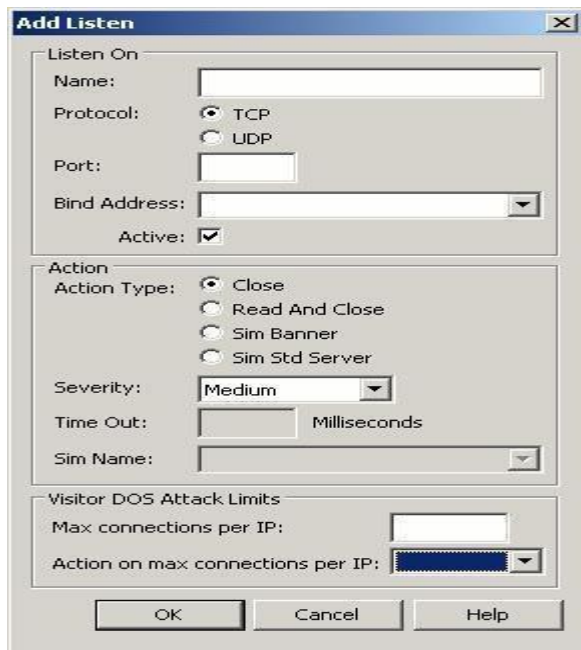
- To create or modify rules, select the Edit Active Scenario command from the scenario menu.
- When you do, you will see a dialog box which contains a summary of all of the existing rules.
- You can either select a rule and click the Edit button to edit a rule, or you can click the Add button to create a new rule.
- Both procedures work similarly.



Click the Add button and you will see the Add Listen dialog box, shown in Figure D.

- The first thing that this dialog box asks for is a name. This is just a name for the rule.
- Pick something descriptive though, because the name that you enter is what will show up in the logs whenever the rule is triggered.

Click on Add Button

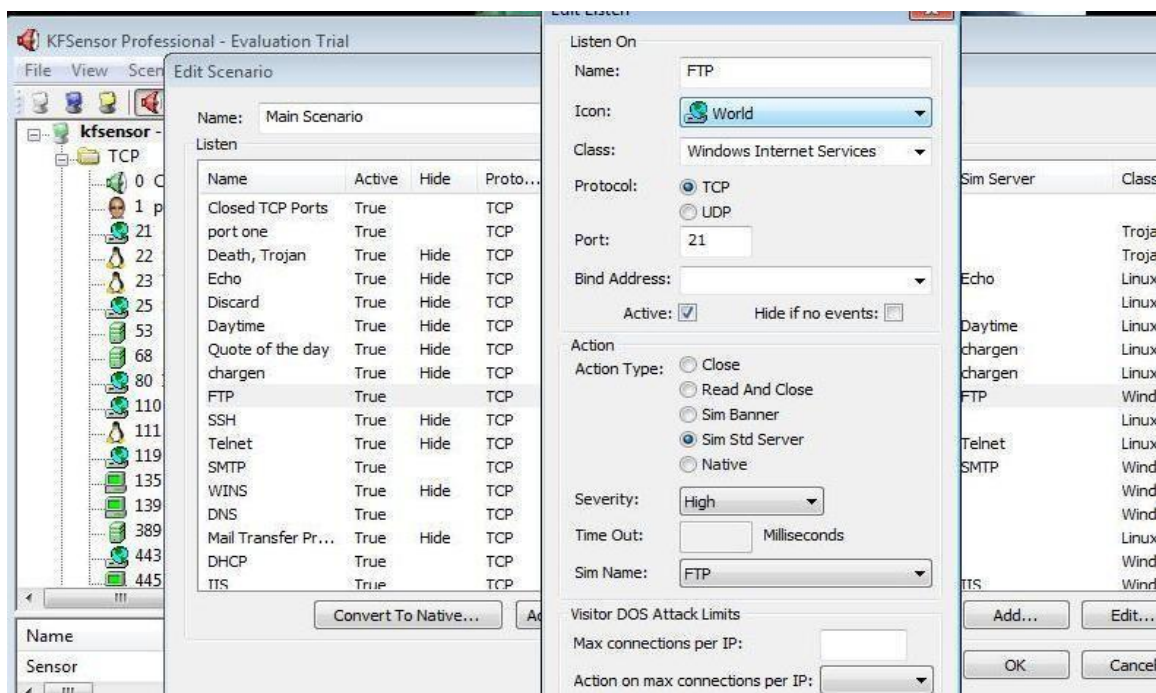


The 'Add Listen' dialog box is used to configure a new listener rule. It contains the following fields and options:

- Listen On:**
 - Name: (text input)
 - Protocol: ☒ TCP, ☐ UDP
 - Port: (text input)
 - Bind Address: (dropdown menu)
 - Active: ☒
- Action:**
 - Action Type: ☒ Close, ☐ Read And Close, ☐ Sim Banner, ☐ Sim Std Server
 - Severity: (dropdown menu, currently 'Medium')
 - Time Out: (text input) Milliseconds
 - Sim Name: (dropdown menu)
- Visitor DOS Attack Limits:**
 - Max connections per IP: (text input)
 - Action on max connections per IP: (dropdown menu)

Buttons: OK, Cancel, Help

Click on Edit Button



The KFSensor Professional - Evaluation Trial interface shows the 'Edit Scenario' window. The 'Listen' tab is active, displaying a list of configured listeners. The 'FTP' listener is selected, and its configuration is shown in the 'Edit Listen' dialog box on the right.

Name	Active	Hide	Proto...
Closed TCP Ports	True		TCP
port one	True		TCP
Death, Trojan	True	Hide	TCP
Echo	True	Hide	TCP
Discard	True	Hide	TCP
Daytime	True	Hide	TCP
Quote of the day	True	Hide	TCP
chargen	True	Hide	TCP
FTP	True		TCP
SSH	True	Hide	TCP
Telnet	True	Hide	TCP
SMTP	True		TCP
WINS	True	Hide	TCP
DNS	True		TCP
Mail Transfer Pr...	True	Hide	TCP
DHCP	True		TCP
ITS	True		TCP

Edit Listen dialog box (FTP):

- Listen On:**
 - Name: FTP
 - Icon: World
 - Class: Windows Internet Services
 - Protocol: ☒ TCP, ☐ UDP
 - Port: 21
 - Bind Address: (dropdown menu)
 - Active: ☒ Hide if no events: ☐
- Action:**
 - Action Type: ☐ Close, ☐ Read And Close, ☐ Sim Banner, ☒ Sim Std Server, ☐ Native
 - Severity: High
 - Time Out: (text input) Milliseconds
 - Sim Name: FTP
- Visitor DOS Attack Limits:**
 - Max connections per IP: (text input)
 - Action on max connections per IP: (dropdown menu)

Buttons: Add..., Edit..., OK, Cancel

- The next few fields are protocol, port, and Bind Address. These fields allow you to choose what the rule is listening for. For example, you could configure the rule to listen to TCP port 1023 on IP address 192.168.1.100. The bind address portion of the rule is optional though. If you leave the bind address blank, the rule will listen across all of the machine's NICs.
- Now that you have defined the listener, it's time to configure the action that the rule takes when traffic is detected on the specified port. Your options are close, read and close, Sim Banner, and SimStd Server.
- The close option tells the rule to just terminate the connection. Read and close logs the information and then terminates the connection. The SimStd Server and Sim Banner options

pertain to server emulation. The Sim Banner option allows you to perform a very simple server emulation, such as what you might use to emulate an FTP server.

- The Sim STD Server option allows you to emulate a more complex server, such as an IIS server.
- If you choose to use one of the sim options, you will have to fill in the simulator's name just below the Time Out field.
- The other part of the Action section that's worth mentioning is the severity section. KFSensor treated some events as severe and other events as a more moderate threat. The dialog box's Severity drop down list allows you to determine what level of severity should be associated with the event that you are logging.
- The final portion of the Add Listen dialog box is the Visitor DOS Attack Limits section. This section allows you to prevent denial of service attacks against KFSensor. You can determine the maximum number of connections to the machine per IP address (remember that this applies on a per rule basis).
- If your threshold is exceeded, you can choose to either ignore the excessive connections or you can lock out the offending IP address.
- Now that you have configured the new rule, select the Active Button to Enable/Disable. The new rule should now be in effect.

DEFEATING MALWARE – ROOTKIT HUNTER

AIM

Root kit is a stealth type of malicious software designed to hide the existence of certain process from normal methods of detection and enables continued privileged access to a computer.

PRELAB DISCUSSION and PROCEDURE :

- Download Rootkit Tool from GMER website. www.gmer.net
- This displays the Processes, Modules, Services, Files, Registry, RootKit/Malwares, Autostart, CMD of local host.
- Select Processes menu and kill any unwanted process if any. Modules menu displays the various system files like .sys, .dll
- Services menu displays the complete services running with Autostart, Enable, Disable, System, Boot.
- Files menu displays full files on Hard-Disk volumes.
- Registry displays **Hkey_Current_user** and **Hkey_Local_Machine**. Rootkits/Malwares scans the local drives selected.
- **Autostart** displays the registry base Autostart applications.
- CMD allows the user to interact with command line utilities or Registry.

