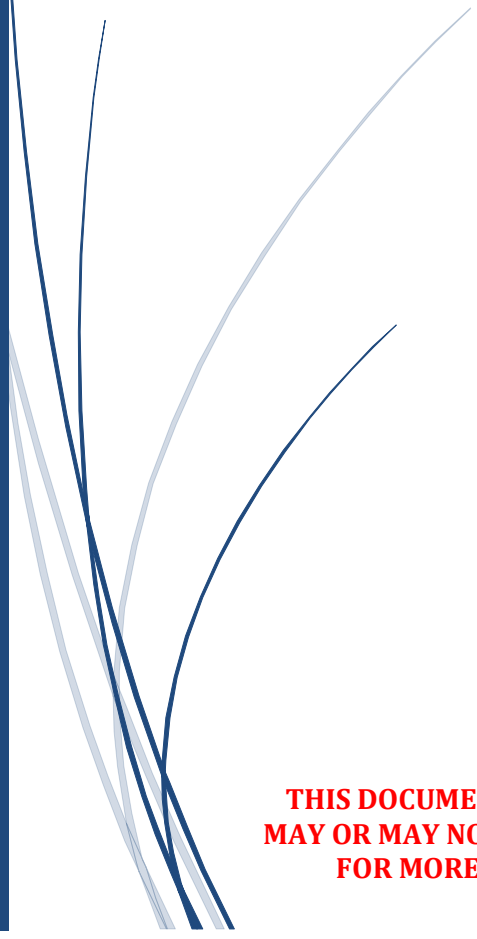
Chapter 12

Evading IDS Firewall and Honeypots

Lab Manual



THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

INDEX

Practical 1: Detecting Malicious Traffic in a network using SNORT-NIDS

Step 1: Installing Snort IDS in Kali Linux.

Execute the following command to update kali linux repository.

apt-get update

```
root@kali:~# apt-get update
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling InRelease [20.3 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [13.4 MB]
16% [2 Packages 104 kB/13.4 MB 1%]
```

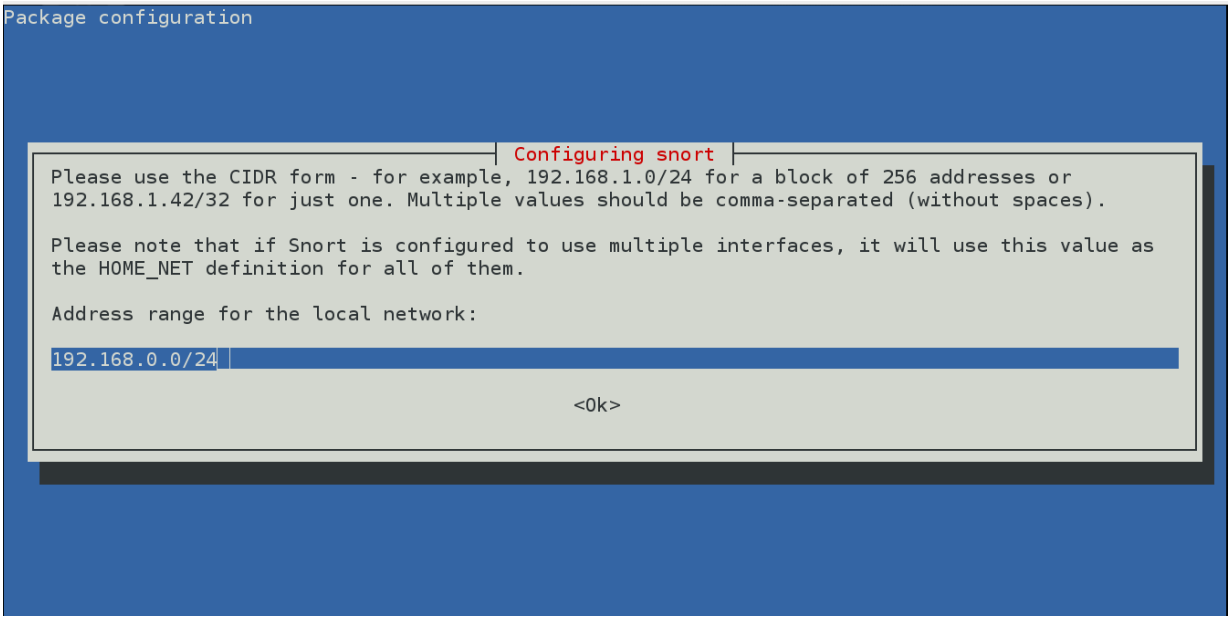
To install snort application, execute the following command

apt-get install snort -y

```
root@kali:~# apt-get install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdaq2 oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 upgraded, 6 newly installed, 0 to remove and 1119 not upgraded.
Need to get 2,230 kB of archives.
After this operation, 7,325 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

While installing snort, we need to provide network range (if you don't know your network range, please click ***Ok*** without any changes.)

In this case, we modified it to ***192.168.0.0/24*** network range as shown below



Step 2: Configuring Snort

To know the IP address and network interface name, execute ***ifconfig.*** To make snort act as IDS, we need to modify our IP in snort configuration file according to our requirement.

Open the configuration file ***/etc/snort/snort.conf*** in your favourite text editor (in this case we are opening it in ***VIM*** editor) and find a line which contains ***ipvar HOME_NET any*** *(*Probably that would be line 51*)*

```
root@kali:~# vim /etc/snort/snort.conf
```

```
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET any
```

change '***any***' into ***your IP*** (192.168.0.146) press ***Esc*** on keyboard and type ***:wq*** and press ***enter*** to save the changes.

```
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.0.146

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
```

Step 3: Running Snort in Kali Linux to detect intrusions

Execute the following commands, to start snort

/etc/init.d/snort start

snort –q –A console –i eth0 –c /etc/snort/snort.conf

```
root@kali:~# /etc/init.d/snort start
[ ok ] Starting snort (via systemctl): snort.service.
root@kali:~#
```

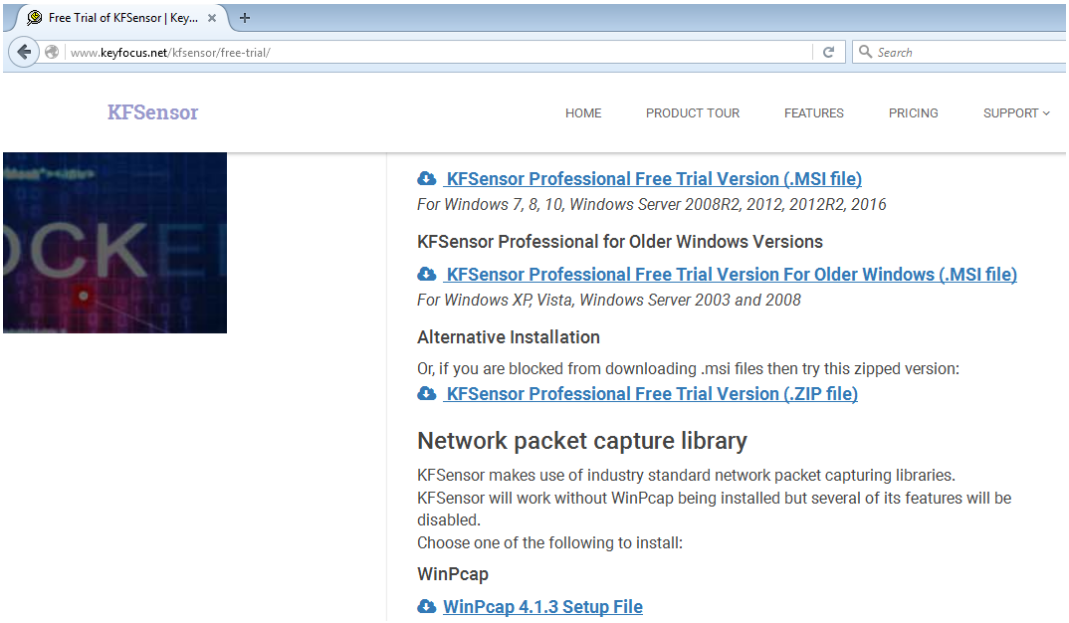
```
root@kali:~# snort -q -A console -i eth0 -c /etc/snort/snort.conf
```

Now, snort is capable of detecting malicious traffic based on pre-configured rules and displays attack information on the terminal as shown in the below image.

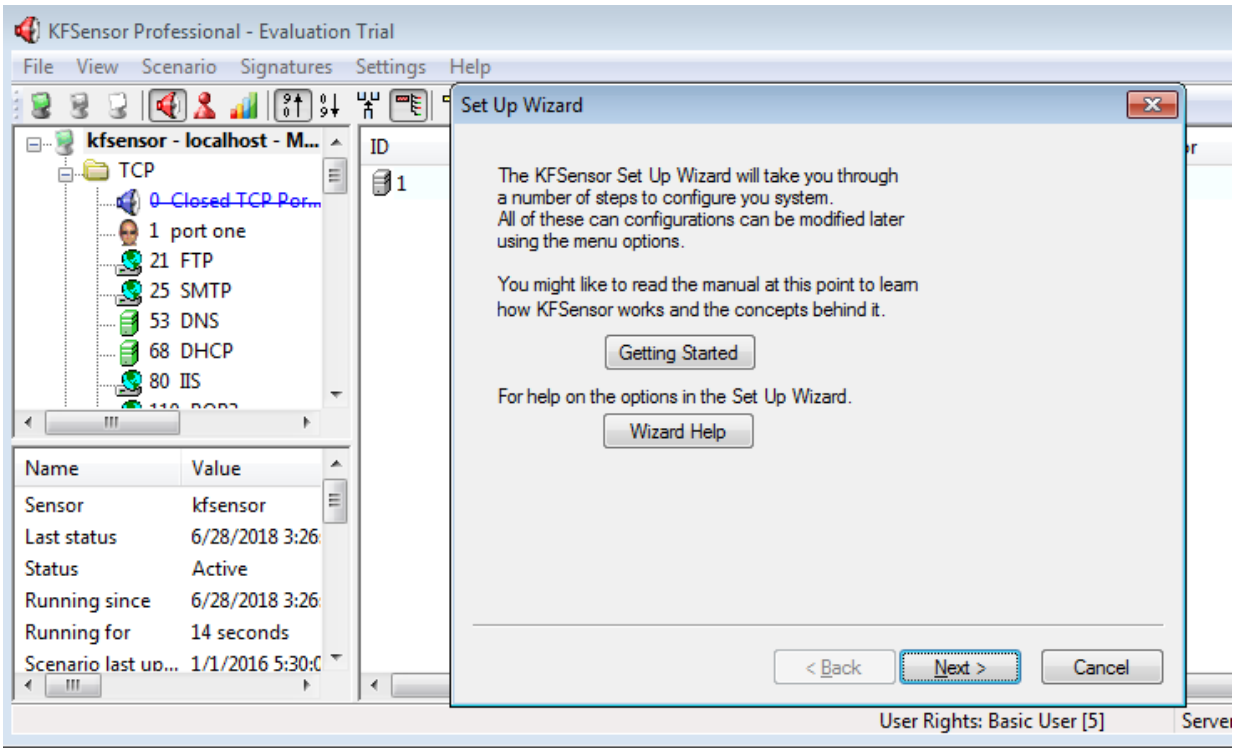
```
root@kali:~# snort -q -A console -i eth0 -c /etc/snort/snort.conf
07/02-17:30:28.191527  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
5.255.255:67
07/02-17:30:28.357863  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
ff30:c0ea
07/02-17:30:28.359803  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
ff30:c0ea
07/02-17:30:45.668868  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
07/02-17:30:45.807714  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
07/02-17:30:45.998653  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
5.255.255:67
07/02-17:30:46.013441  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
5.255.255:67
07/02-17:30:46.652928  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic]
ff84:3e70
```

Practical 2: Using KFSensor to build a Honeypot.

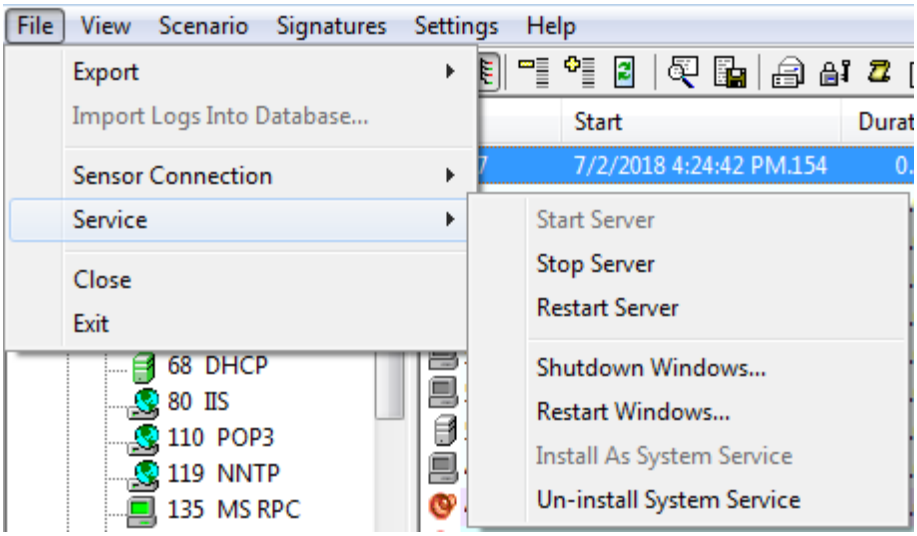
Visit KFSensor official website http://www.keyfocus.net/kfsensor/free-trial/ and register with your details. Download ***KFSensor*** package and ***WinPcap*** software package as a dependency to KFSensor.



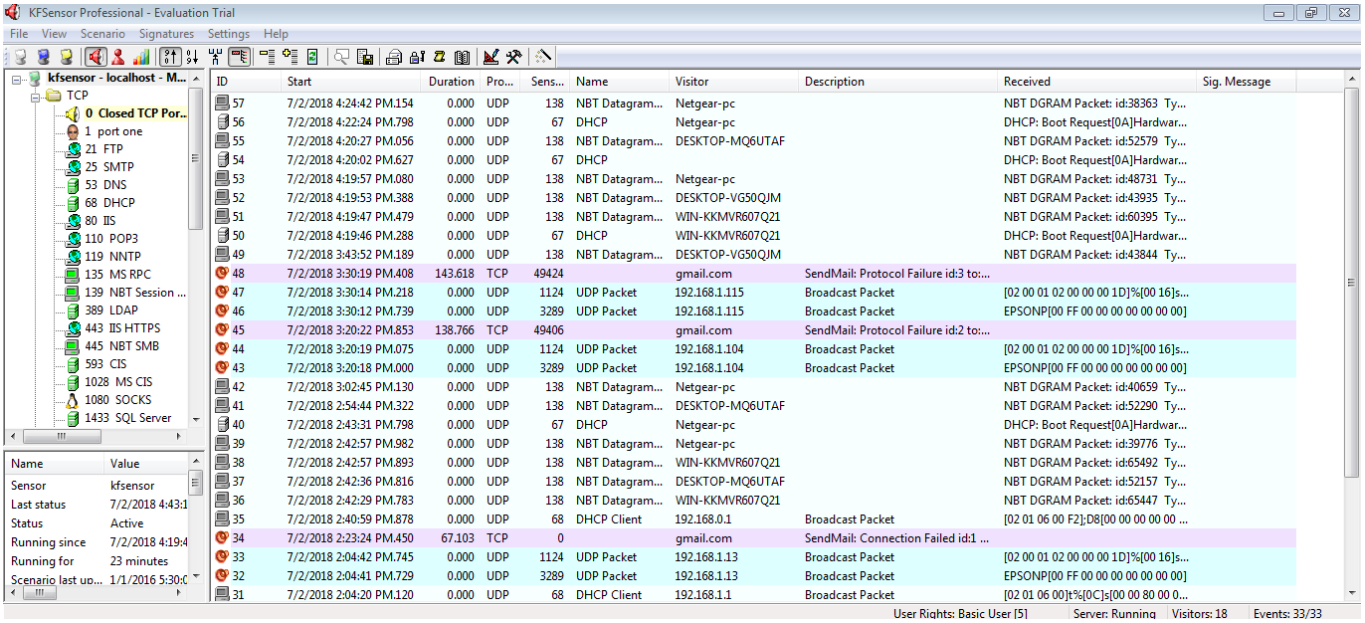
Install ***winpcap*** first and install ***KFSensor*** and restart your computer once. After rebooting your computer please go to start menu, find KFSensor and launch the application.



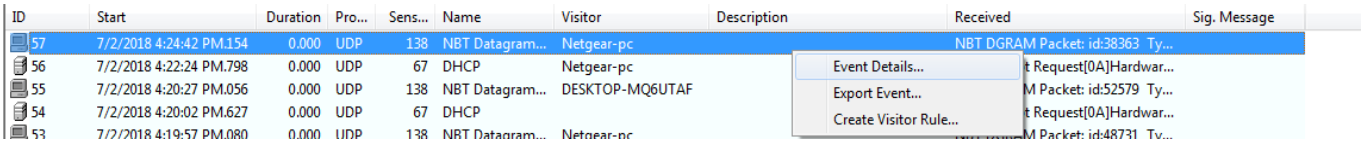
Under ***File*** tab, select ***Service*** and then click on ***Start Service*** and proceed with the application wizard to turn your PC into a honeypot machine to attract the attackers.

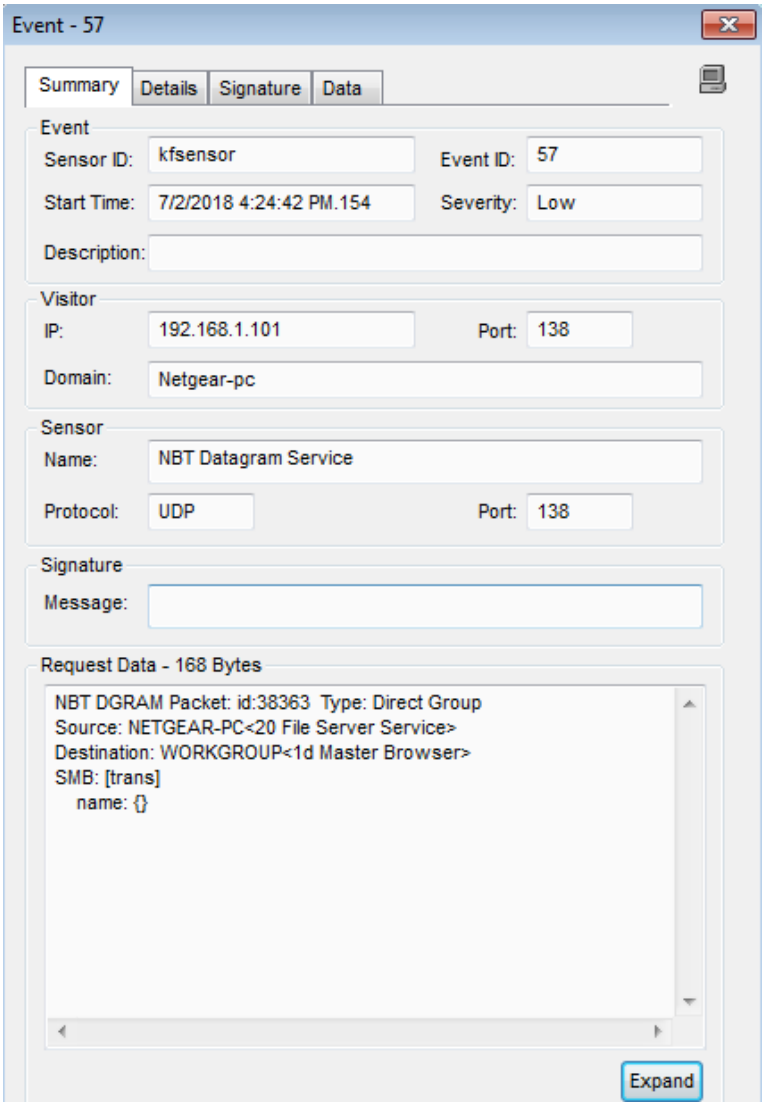


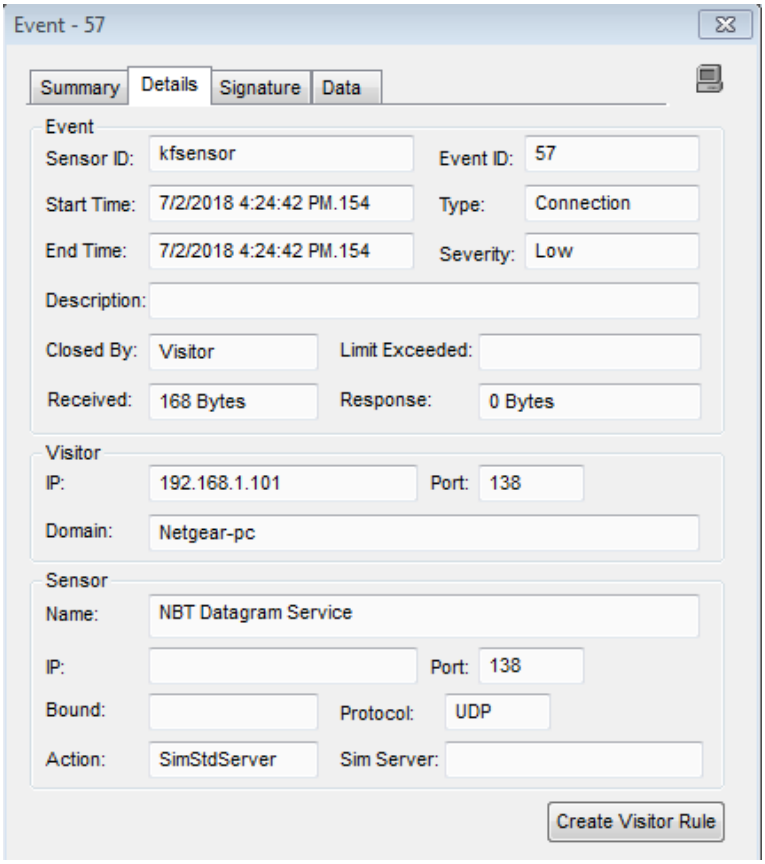
If anyone performs an attack on the computer, KFSensor will display alerts.



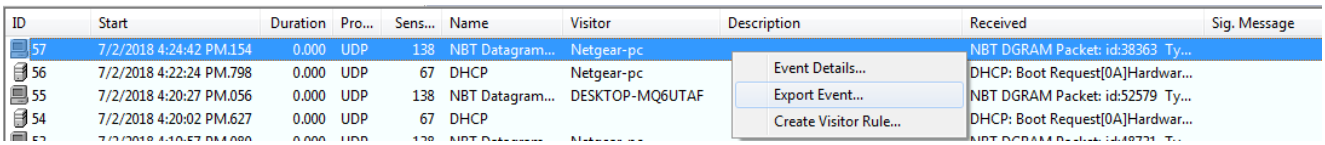
Right-click on any alert, select ***Event Details*** to view the information about the alert.

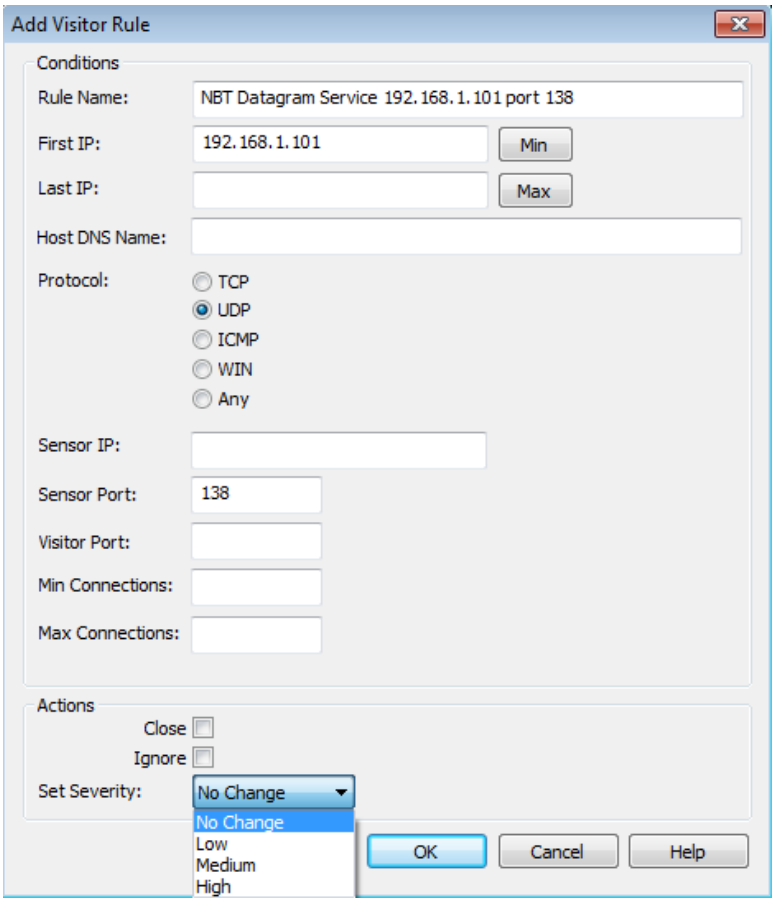



Event - 57
Summary
Details
Signature
Data
Event
Sensor ID: kfsensor
Event ID: 57
Start Time: 7/2/2018 4:24:42 PM.154
Severity: Low
Description:
Visitor
IP: 192.168.1.101
Port: 138
Domain: Netgear-pc
Sensor
Name: NBT Datagram Service
Protocol: UDP
Port: 138
Signature
Message:
Request Data - 168 Bytes
NBT DGRAM Packet: id:38363 Type: Direct Group
Source: NETGEAR-PC<20 File Server Service>
Destination: WORKGROUP<1d Master Browser>
SMB: [trans]
name: {}
Expand



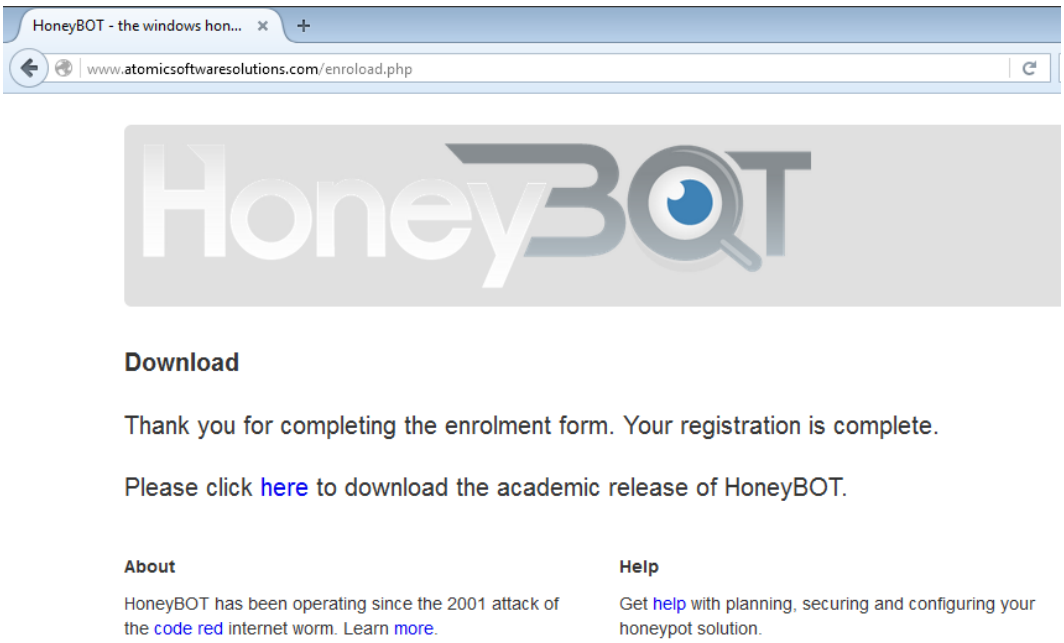
Right-click on any alert, select ***Create Visitor Rule*** to create a customized rule to get alerts



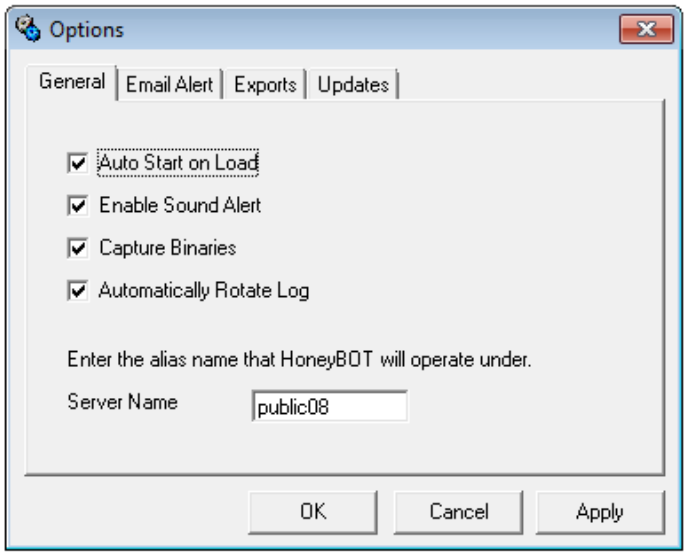


Practical 3: HoneyBot on windows

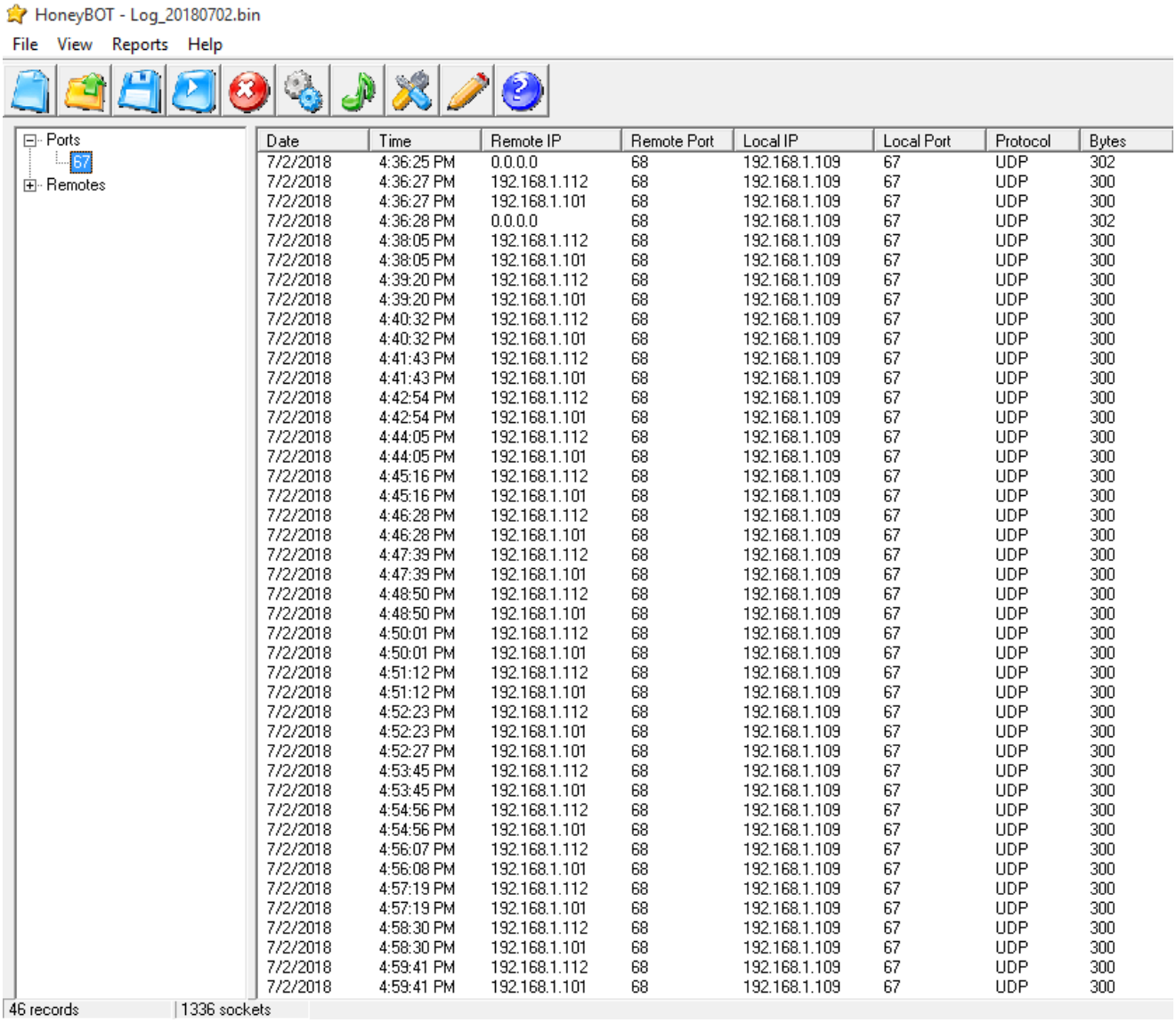
Visit https://www.atomicsoftwaresolutions.com/ and register for ***academic release*** with your details.



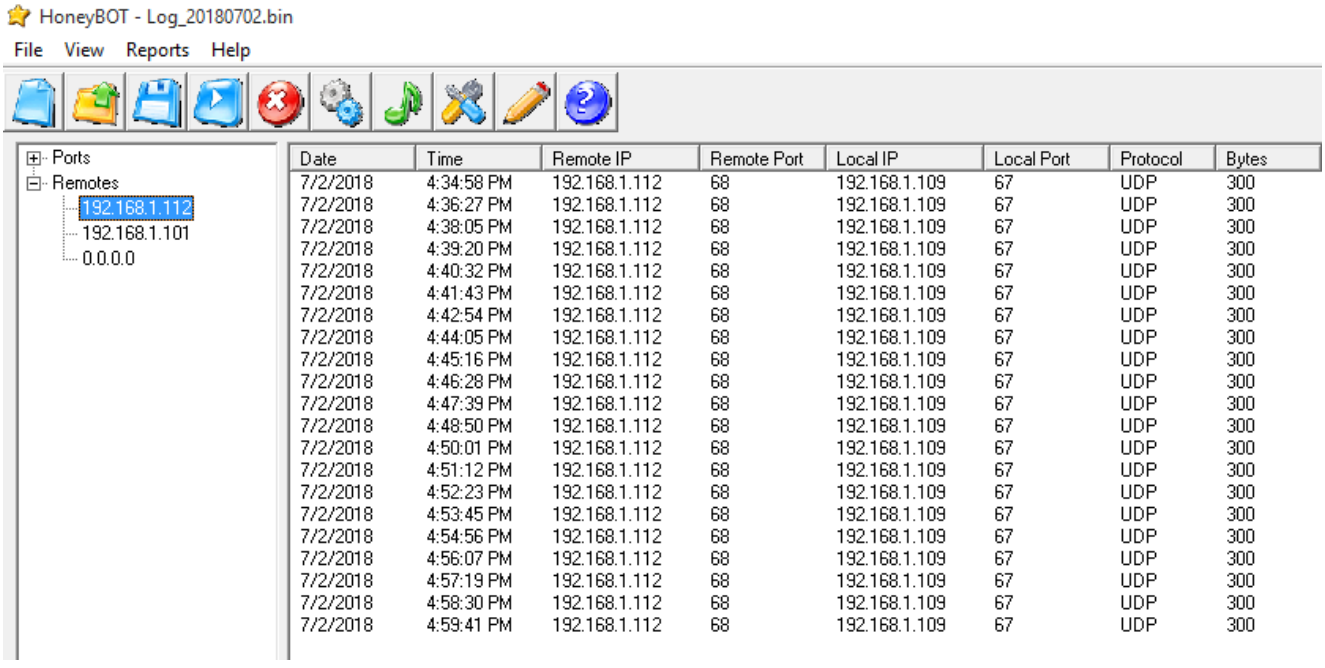
Download and install **HoneyBot** software. After installation of HoneyBot, when it prompts ***Options*** window, you can select necessary options and click ***OK.***



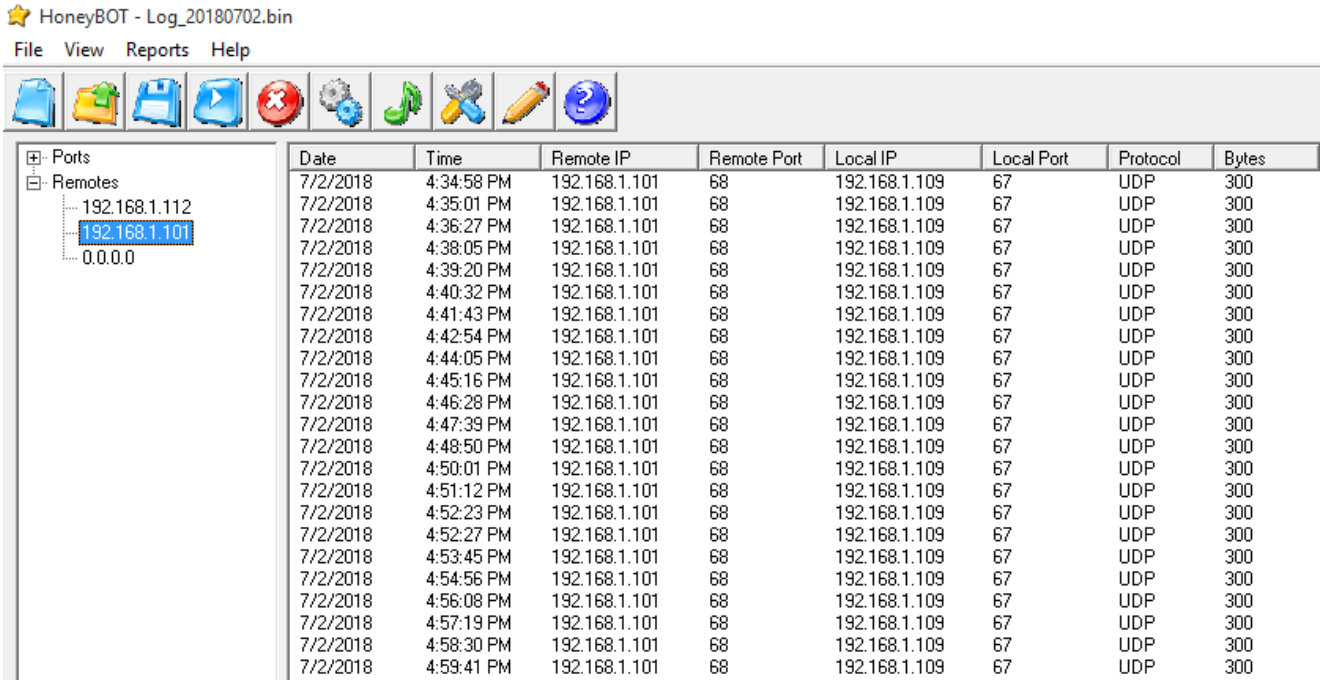
The honeybot application will display alerts when anyone performs an attack on the computer.

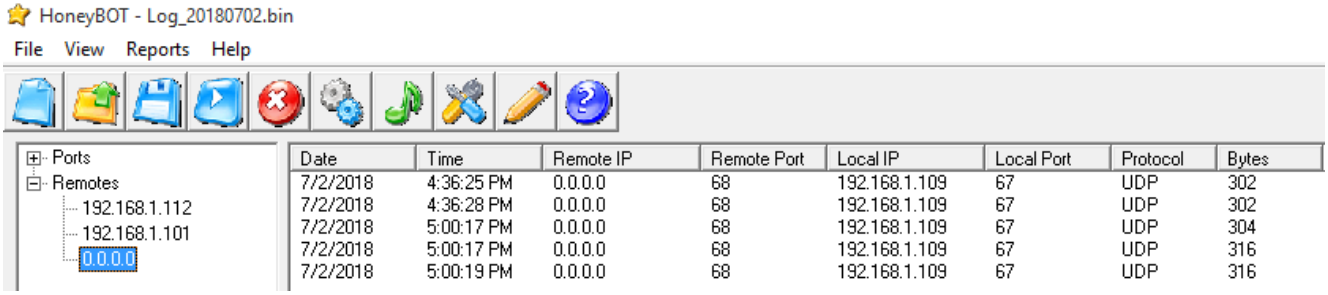


Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
7/2/2018	4:36:25 PM	0.0.0.0	68	192.168.1.109	67	UDP	302
7/2/2018	4:36:27 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:36:27 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:36:28 PM	0.0.0.0	68	192.168.1.109	67	UDP	302
7/2/2018	4:38:05 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:38:05 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:39:20 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:39:20 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:40:32 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:40:32 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:41:43 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:41:43 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:42:54 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:42:54 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:44:05 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:44:05 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:45:16 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:45:16 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:46:28 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:46:28 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:47:39 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:47:39 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:48:50 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:48:50 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:50:01 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:50:01 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:51:12 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:51:12 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:52:23 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:52:23 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:52:27 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:53:45 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:53:45 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:54:56 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:54:56 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:56:07 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:56:08 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:57:19 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:57:19 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:58:30 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:58:30 PM	192.168.1.101	68	192.168.1.109	67	UDP	300
7/2/2018	4:59:41 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:59:41 PM	192.168.1.101	68	192.168.1.109	67	UDP	300

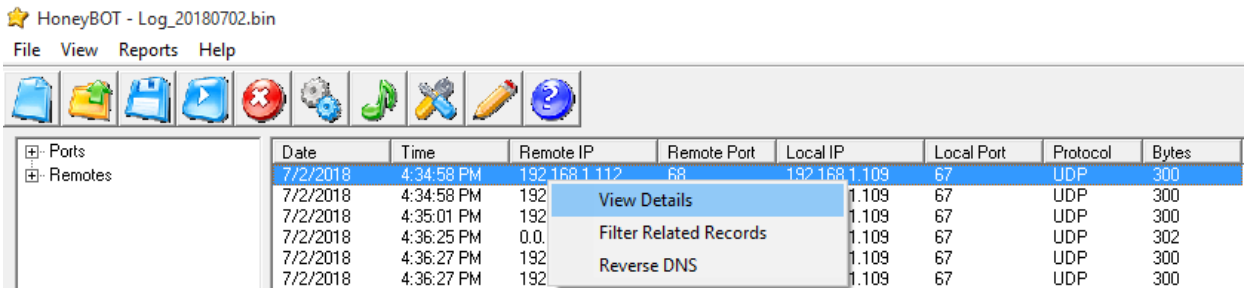


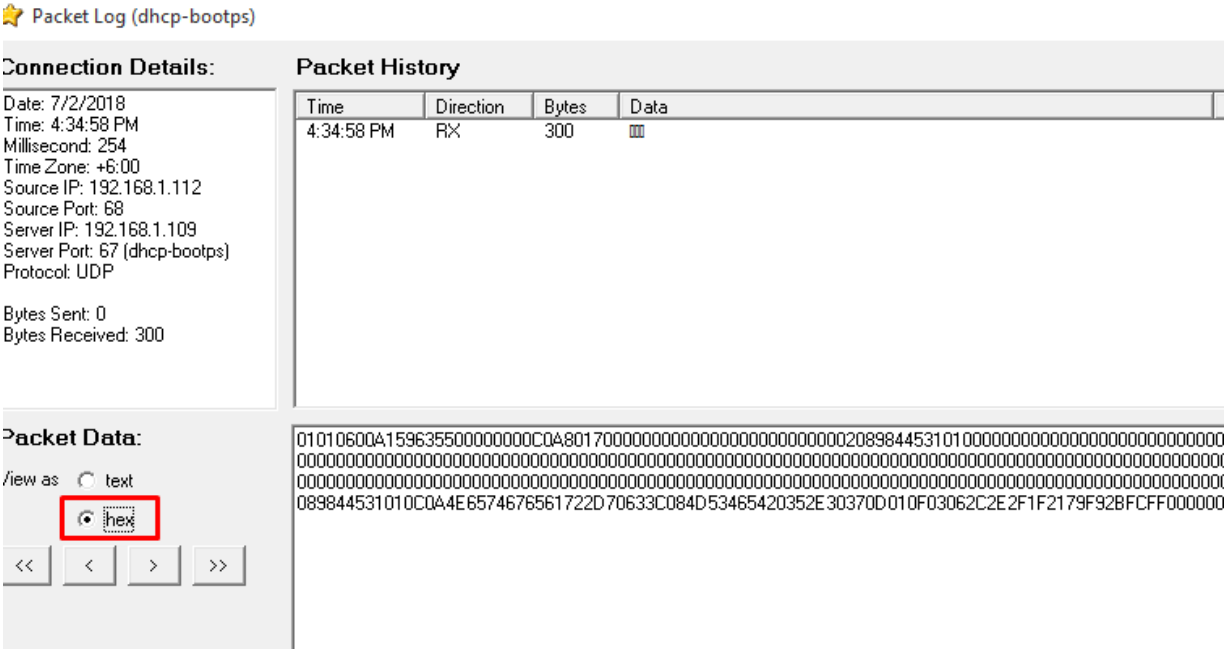
Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
7/2/2018	4:34:58 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:36:27 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:38:05 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:39:20 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:40:32 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:41:43 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:42:54 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:44:05 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:45:16 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:46:28 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:47:39 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:48:50 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:50:01 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:51:12 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:52:23 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:53:45 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:54:56 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:56:07 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:57:19 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:58:30 PM	192.168.1.112	68	192.168.1.109	67	UDP	300
7/2/2018	4:59:41 PM	192.168.1.112	68	192.168.1.109	67	UDP	300



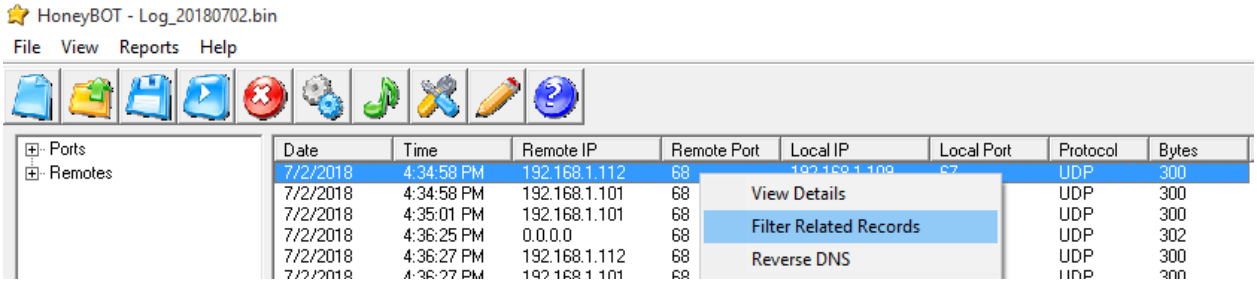


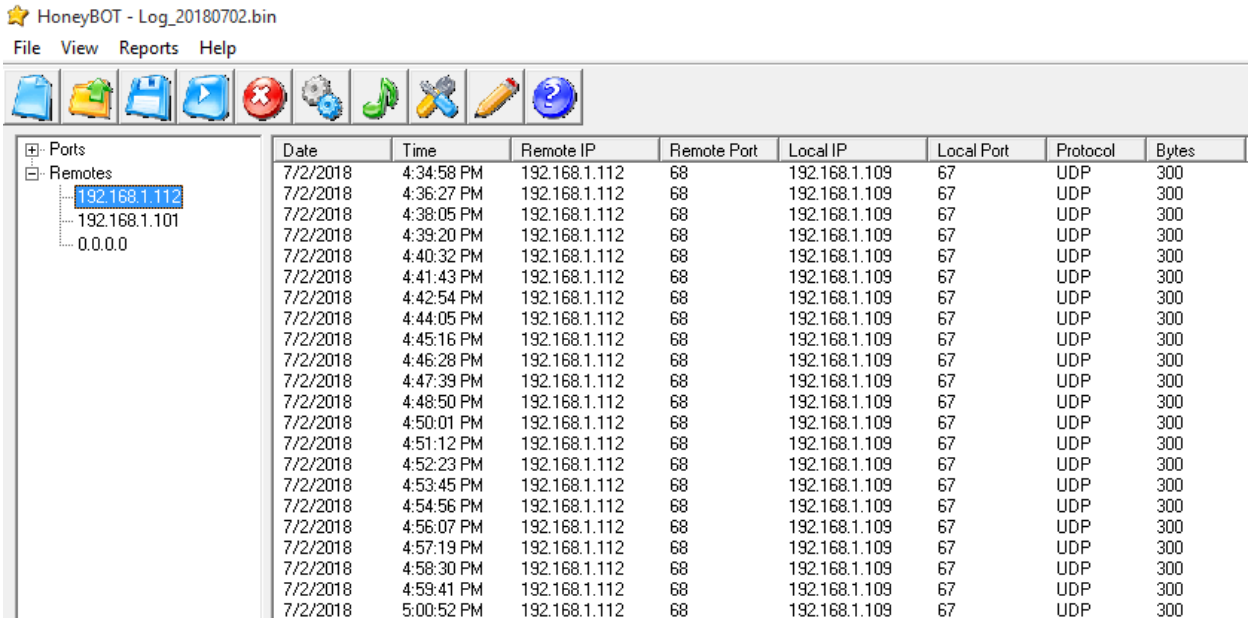
To view more information about alerts, right-click on any alert, choose ***View Details***.





Right-click on any alert, choose ***Filter Related Records*** to filter results.

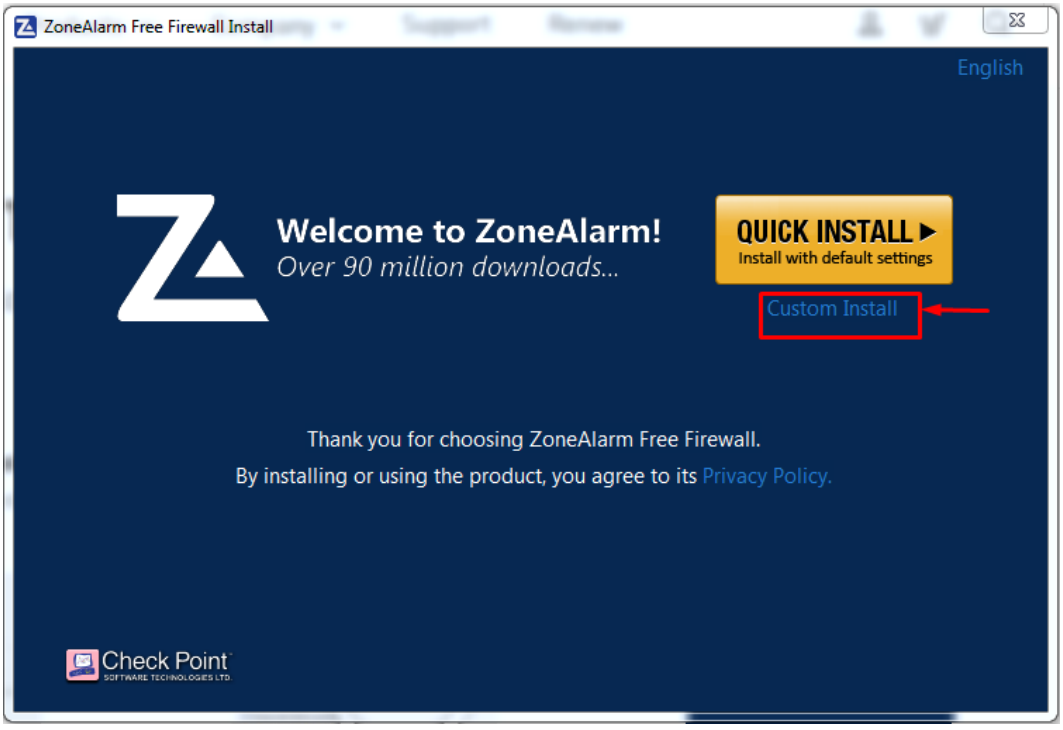


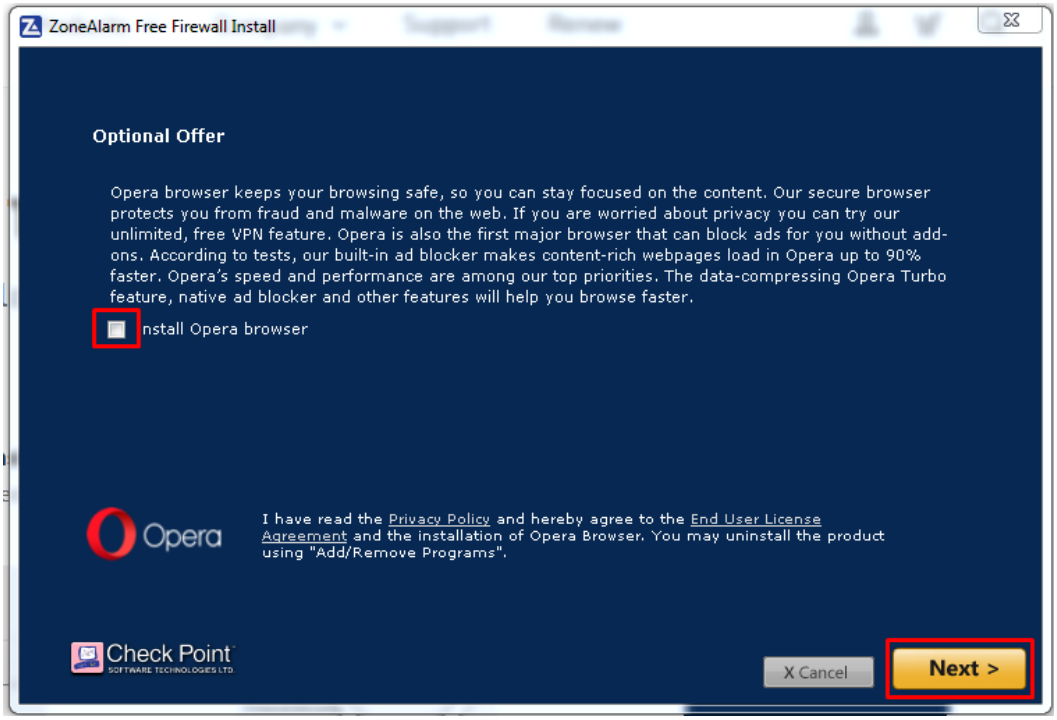


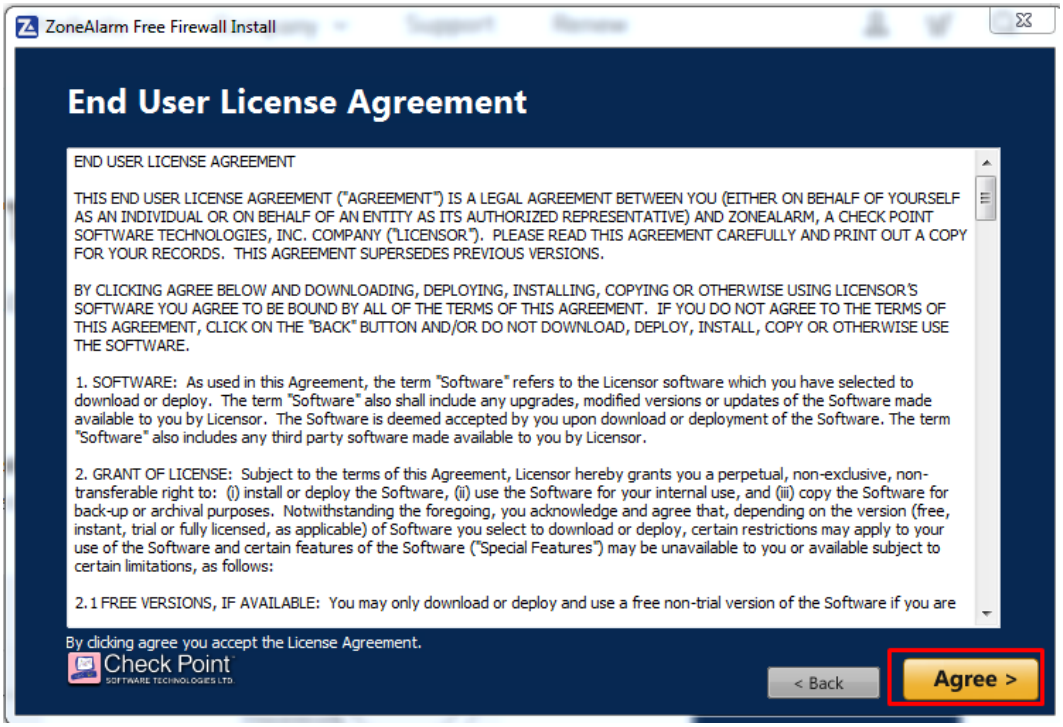
Practical 4: Custom installation of Zonealarm Firewall on Windows

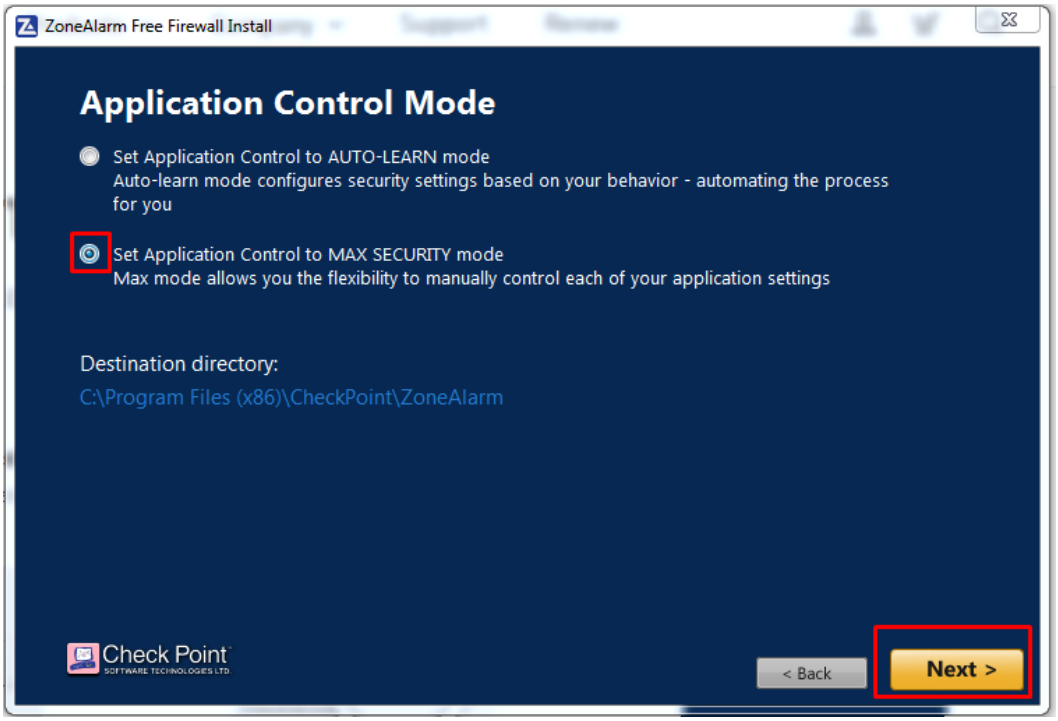
Visit https://www.zonealarm.com/software/free-firewall/ and download a free version of ZoneAlarm firewall.

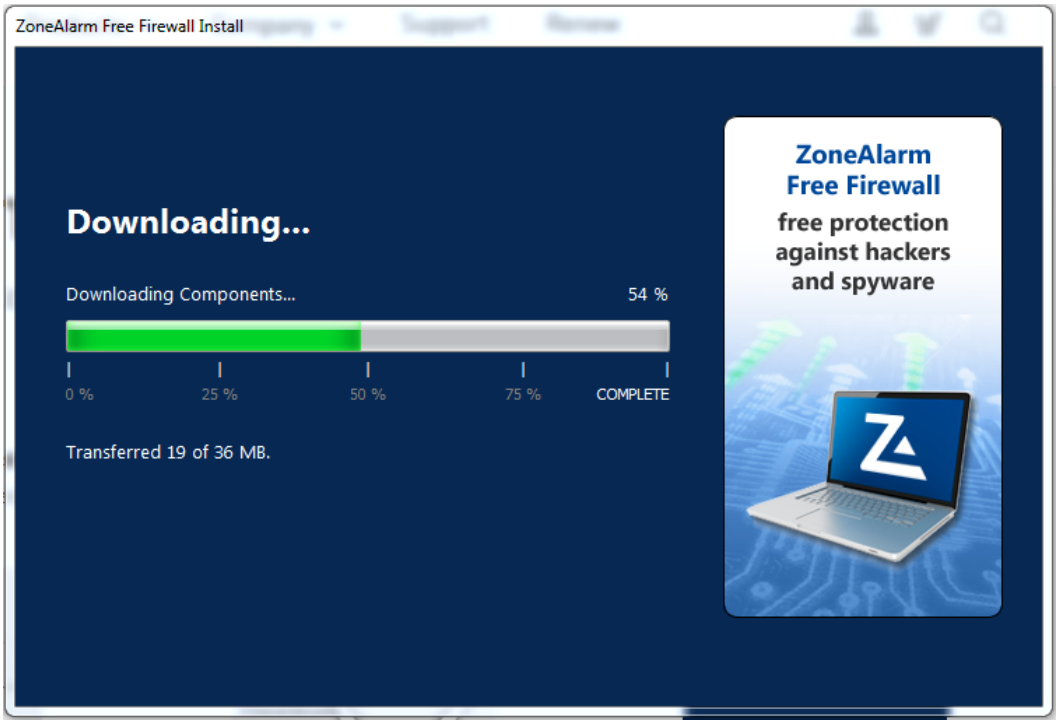
To customize the installation, click on ***Custom Install*** and follow the procedure as shown in below images.

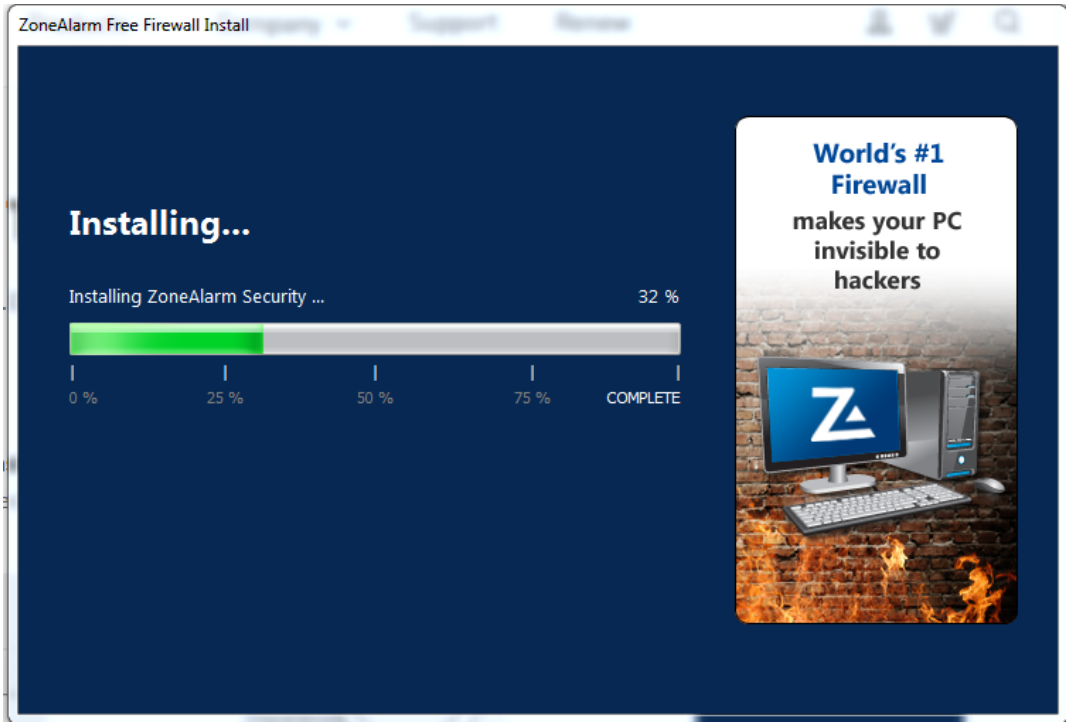


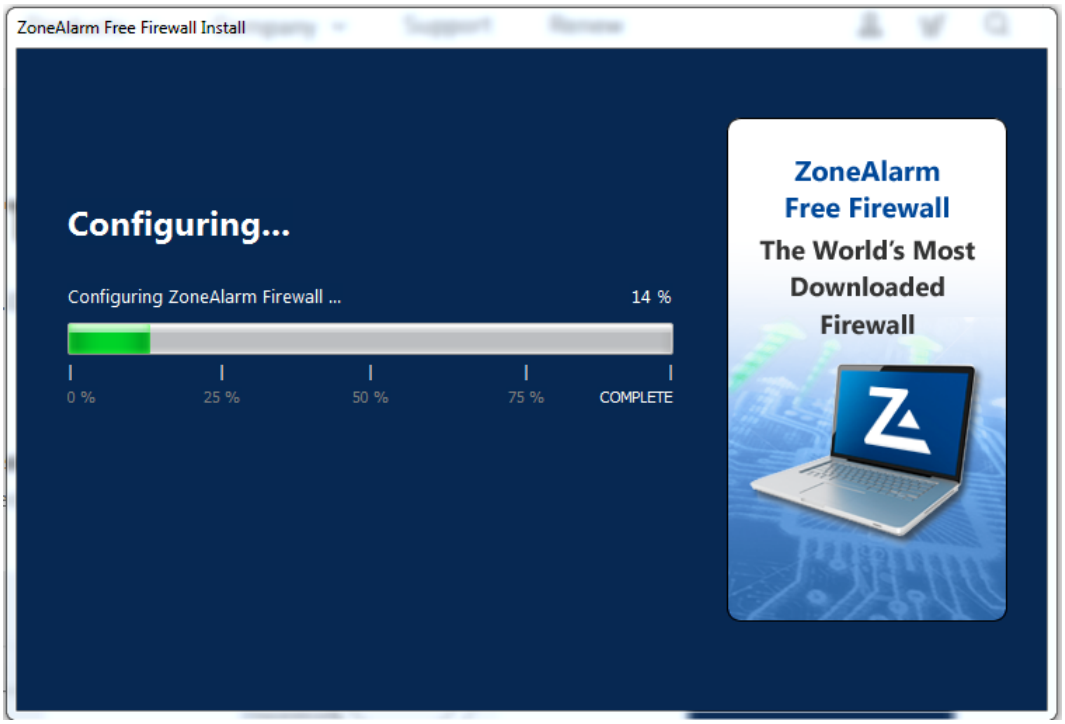

ZoneAlarm Free Firewall Install
Optional Offer
Opera browser keeps your browsing safe, so you can stay focused on the content. Our secure browser protects you from fraud and malware on the web. If you are worried about privacy you can try our unlimited, free VPN feature. Opera is also the first major browser that can block ads for you without add-ons. According to tests, our built-in ad blocker makes content-rich webpages load in Opera up to 90% faster. Opera's speed and performance are among our top priorities. The data-compressing Opera Turbo feature, native ad blocker and other features will help you browse faster.
nstall Opera browser
Opera
I have read the Privacy Policy and hereby agree to the End User License Agreement and the installation of Opera Browser. You may uninstall the product using "Add/Remove Programs".
Check Point
X Cancel
Next >

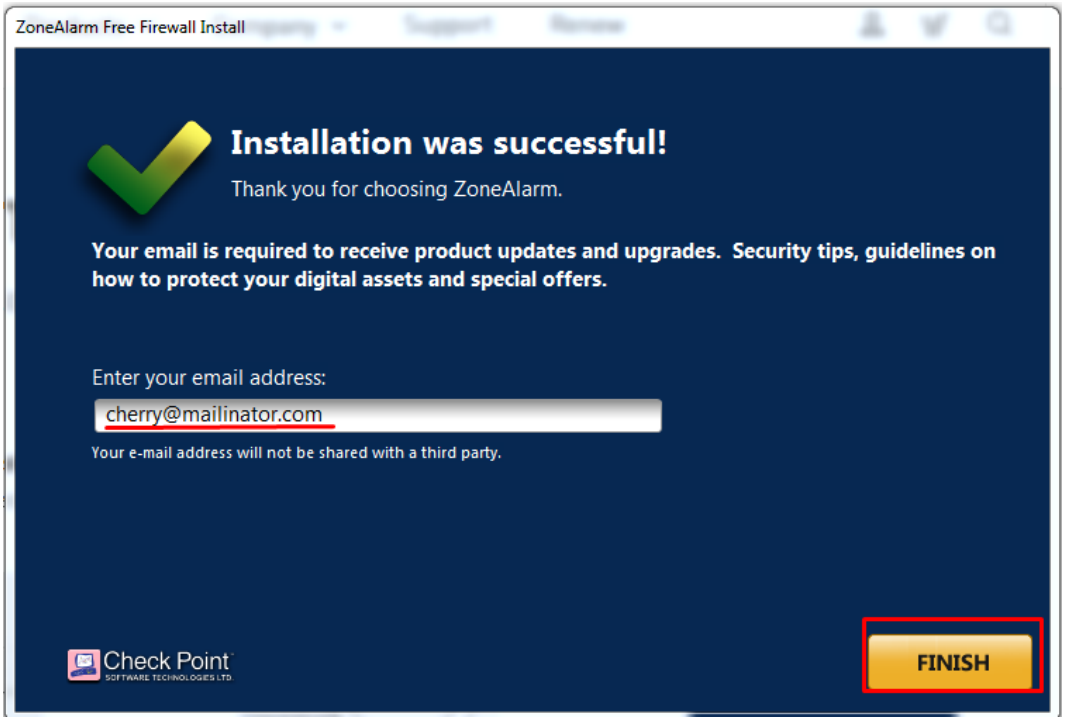

ZoneAlarm Free Firewall Install
End User License Agreement
END USER LICENSE AGREEMENT
THIS END USER LICENSE AGREEMENT ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU (EITHER ON BEHALF OF YOURSELF AS AN INDIVIDUAL OR ON BEHALF OF AN ENTITY AS ITS AUTHORIZED REPRESENTATIVE) AND ZONEALARM, A CHECK POINT SOFTWARE TECHNOLOGIES, INC. COMPANY ("LICENSOR"). PLEASE READ THIS AGREEMENT CAREFULLY AND PRINT OUT A COPY FOR YOUR RECORDS. THIS AGREEMENT SUPERSEDES PREVIOUS VERSIONS.
BY CLICKING AGREE BELOW AND DOWNLOADING, DEPLOYING, INSTALLING, COPYING OR OTHERWISE USING LICENSOR'S SOFTWARE YOU AGREE TO BE BOUND BY ALL OF THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, CLICK ON THE "BACK" BUTTON AND/OR DO NOT DOWNLOAD, DEPLOY, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.
1. SOFTWARE: As used in this Agreement, the term "Software" refers to the Licensor software which you have selected to download or deploy. The term "Software" also shall include any upgrades, modified versions or updates of the Software made available to you by Licensor. The Software is deemed accepted by you upon download or deployment of the Software. The term "Software" also includes any third party software made available to you by Licensor.
2. GRANT OF LICENSE: Subject to the terms of this Agreement, Licensor hereby grants you a perpetual, non-exclusive, non-transferable right to: (i) install or deploy the Software, (ii) use the Software for your internal use, and (iii) copy the Software for back-up or archival purposes. Notwithstanding the foregoing, you acknowledge and agree that, depending on the version (free, instant, trial or fully licensed, as applicable) of Software you select to download or deploy, certain restrictions may apply to your use of the Software and certain features of the Software ("Special Features") may be unavailable to you or available subject to certain limitations, as follows:
2.1 FREE VERSIONS, IF AVAILABLE: You may only download or deploy and use a free non-trial version of the Software if you are
By clicking agree you accept the License Agreement.
Check Point
< Back
Agree >


ZoneAlarm Free Firewall Install
Application Control Mode
Set Application Control to AUTO-LEARN mode
Auto-learn mode configures security settings based on your behavior - automating the process for you
Set Application Control to MAX SECURITY mode
Max mode allows you the flexibility to manually control each of your application settings
Destination directory:
C:\Program Files (x86)\CheckPoint\ZoneAlarm
Check Point
SOFTWARE TECHNOLOGIES LTD.
< Back
Next >

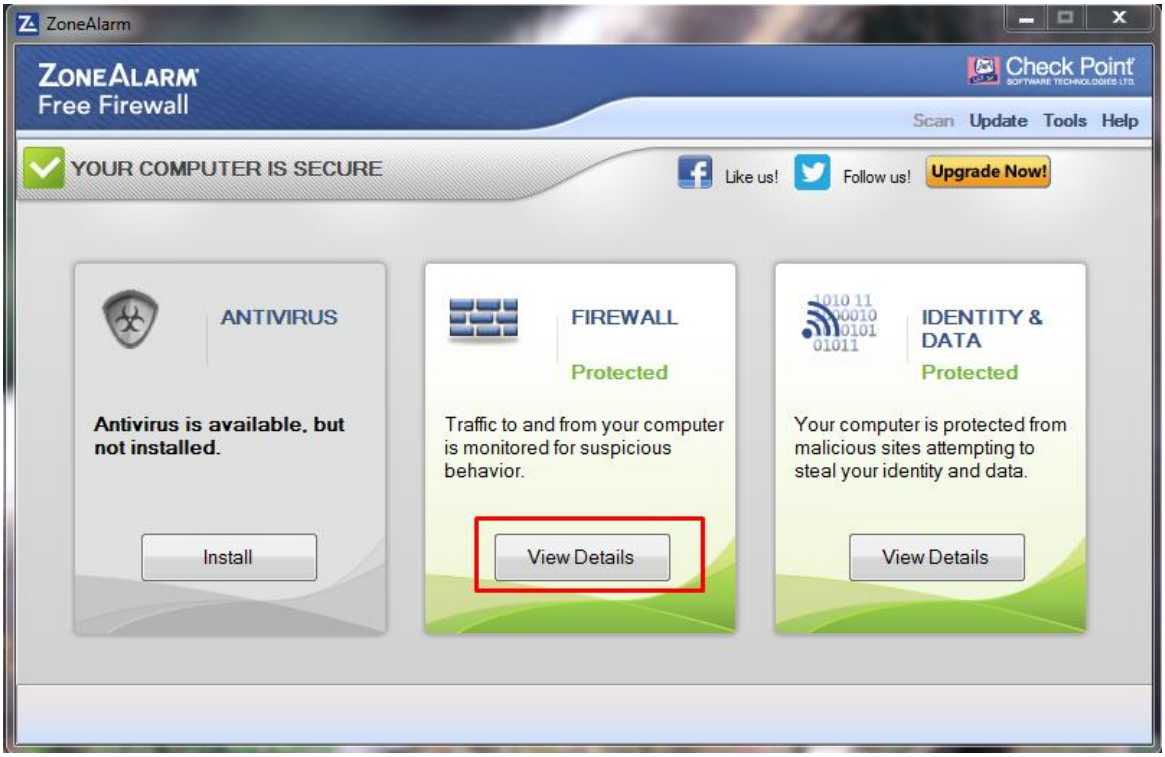

ZoneAlarm Free Firewall Install
Downloading...
Downloading Components...
54 %
0 %
25 %
50 %
75 %
COMPLETE
Transferred 19 of 36 MB.
ZoneAlarm
Free Firewall
free protection
against hackers
and spyware

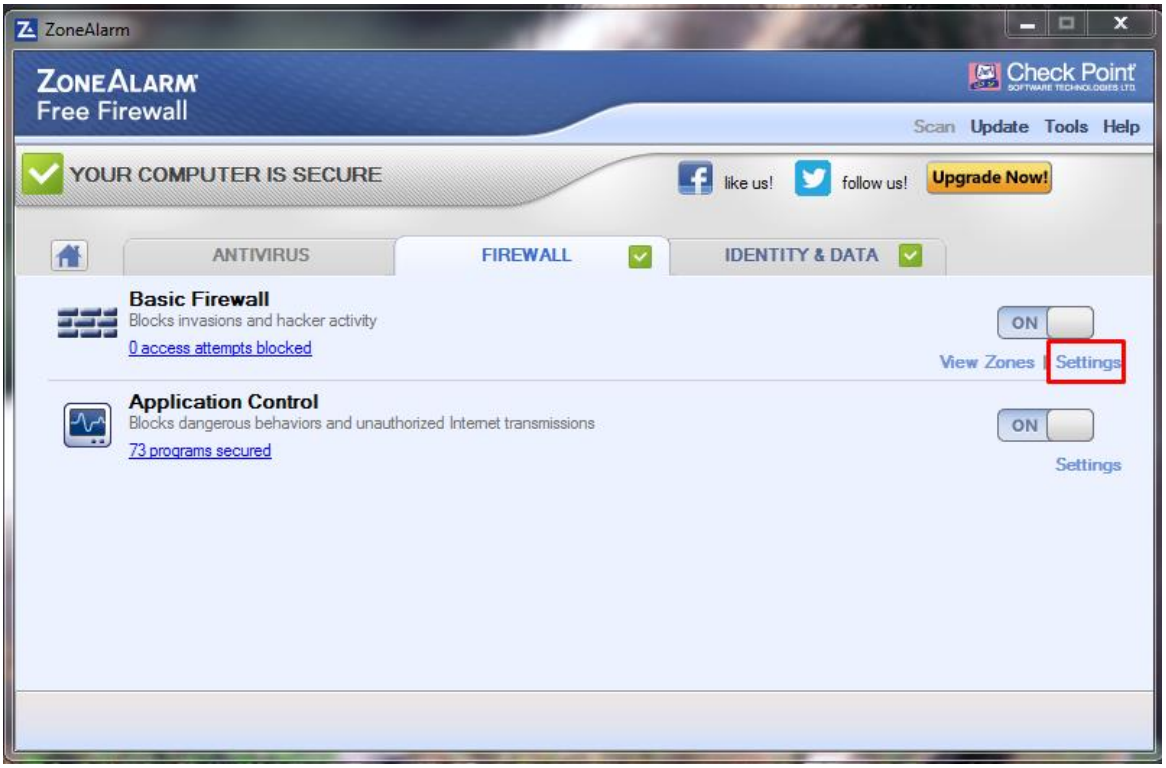

ZoneAlarm Free Firewall Install
Installing...
Installing ZoneAlarm Security ...
32 %
0 %
25 %
50 %
75 %
COMPLETE
World's #1 Firewall
makes your PC invisible to hackers

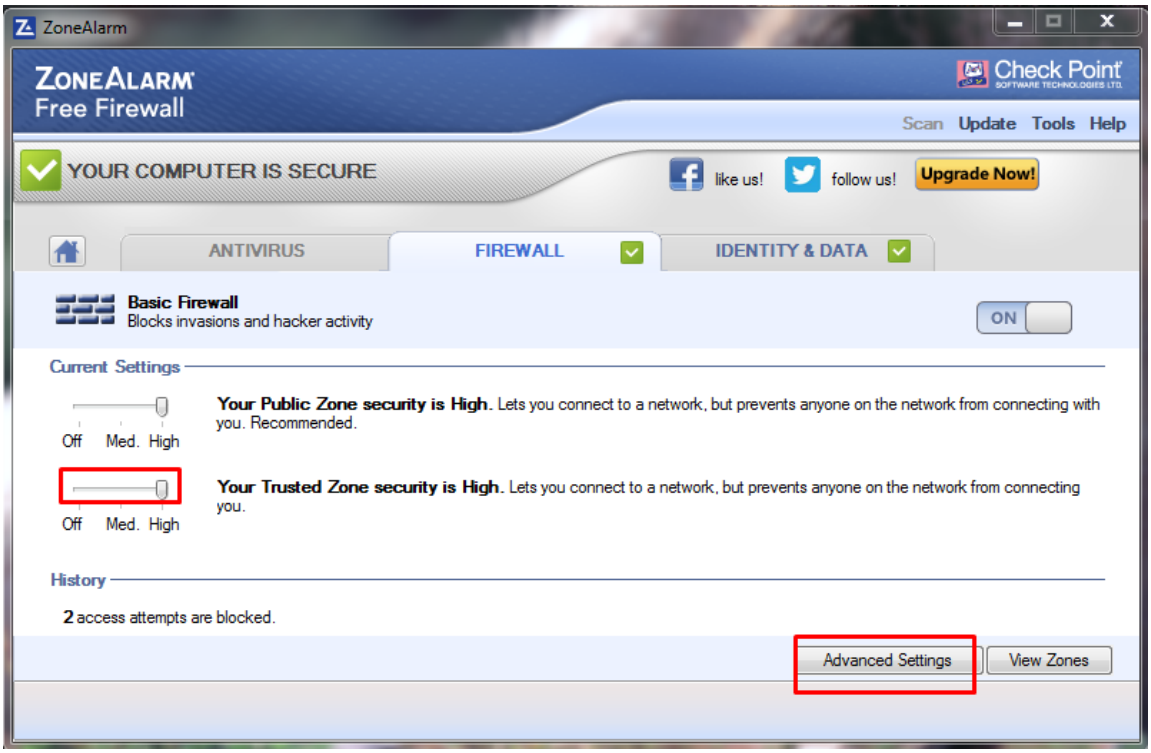

ZoneAlarm Free Firewall Install
Configuring...
Configuring ZoneAlarm Firewall ...
14 %
0 %
25 %
50 %
75 %
COMPLETE
ZoneAlarm Free Firewall
The World's Most Downloaded Firewall

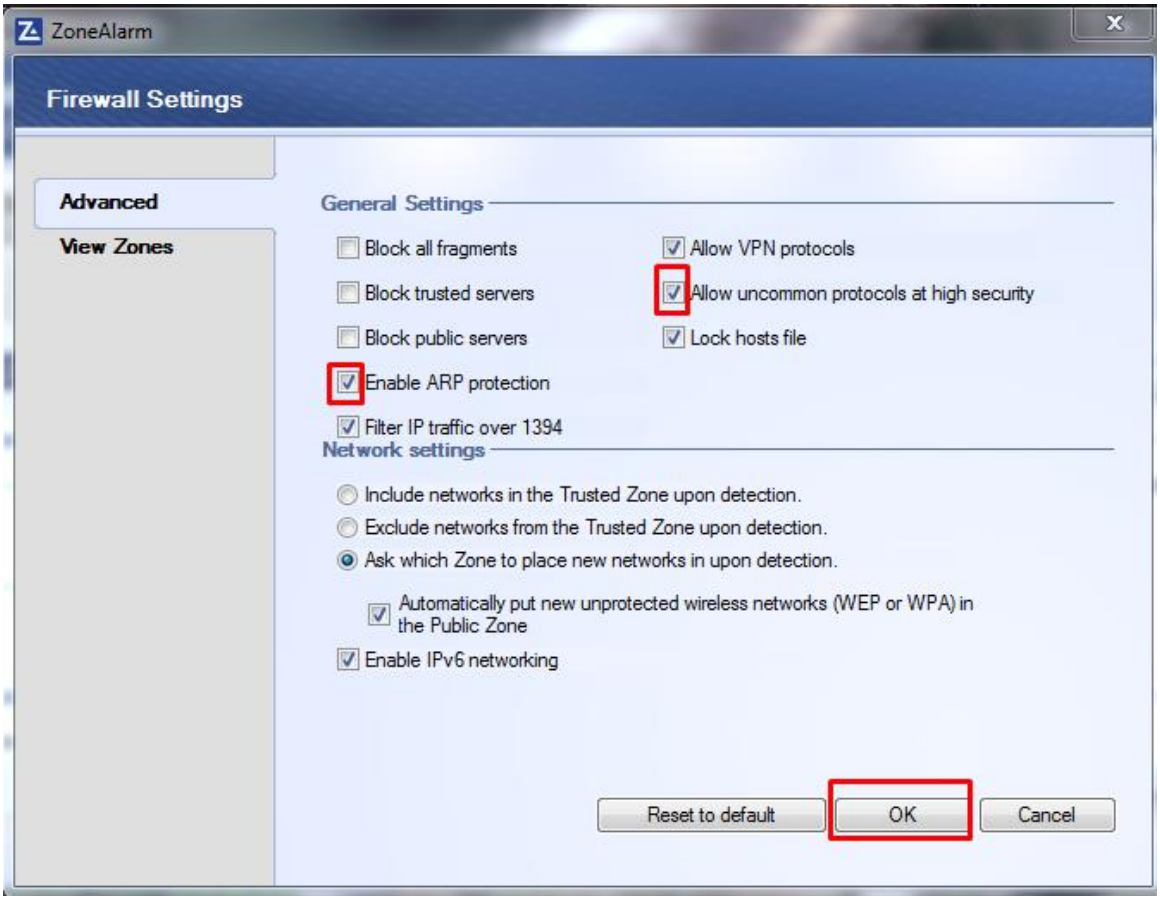


To customize the ZoneAlarm firewall, click on ***View Details*** under ***Firewall*** and follow below images.

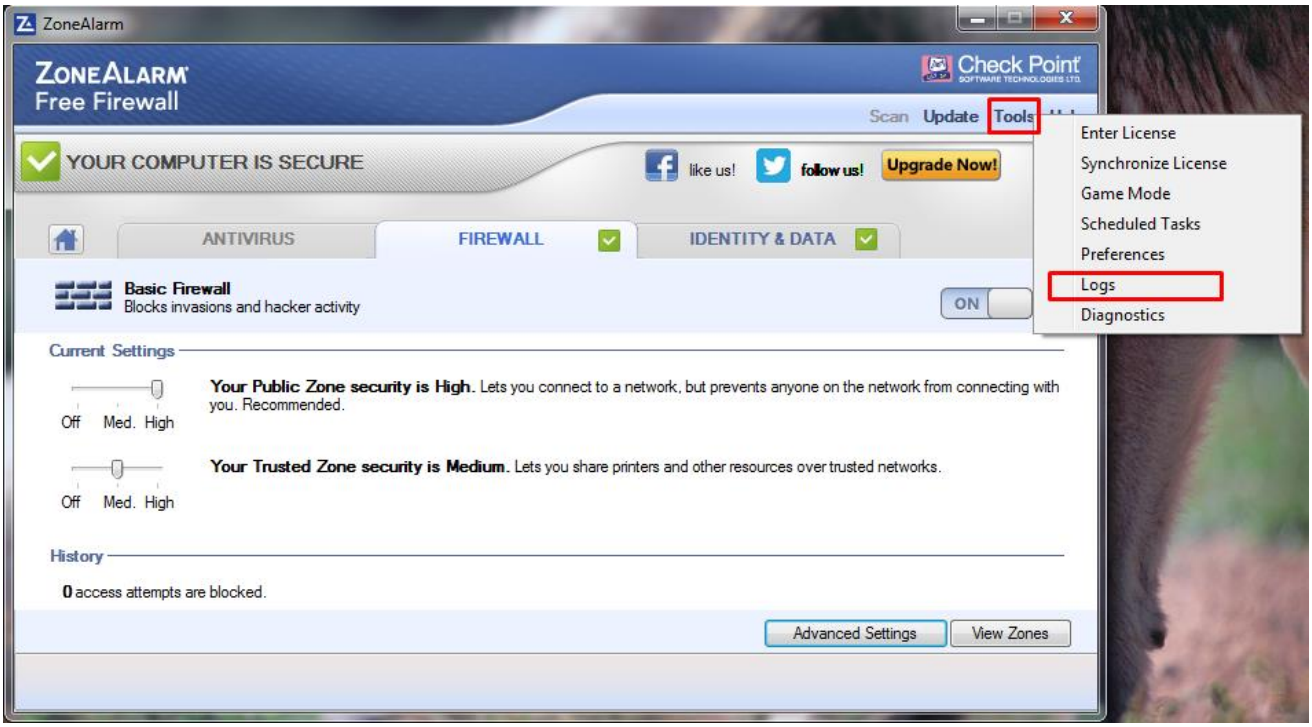


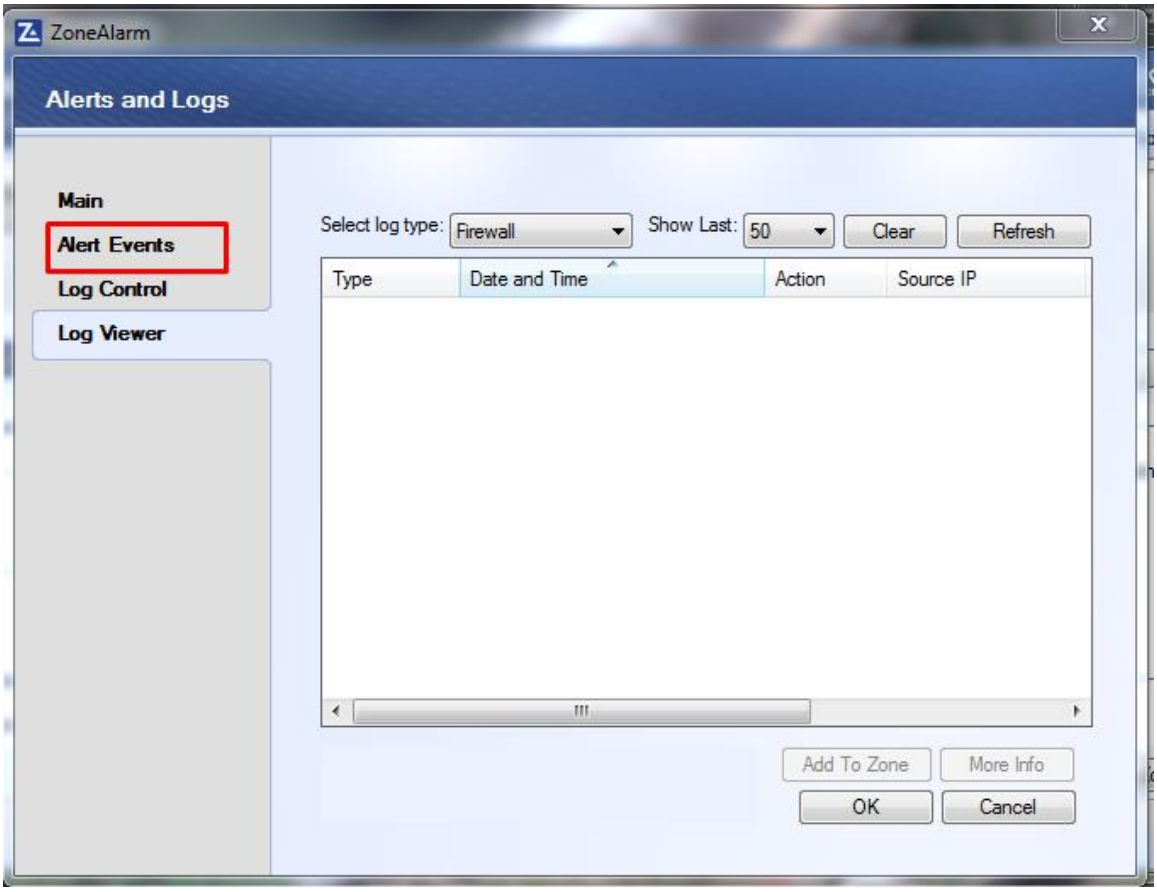

ZoneAlarm
ZONEALARM
Free Firewall
Check Point
SOFTWARE TECHNOLOGIES LTD.
Scan Update Tools Help
YOUR COMPUTER IS SECURE
like us!
follow us!
Upgrade Now!
ANTIVIRUS
FIREWALL
IDENTITY & DATA
Basic Firewall
Blocks invasions and hacker activity
0 access attempts blocked
ON
View Zones
Settings
Application Control
Blocks dangerous behaviors and unauthorized Internet transmissions
73 programs secured
ON
Settings

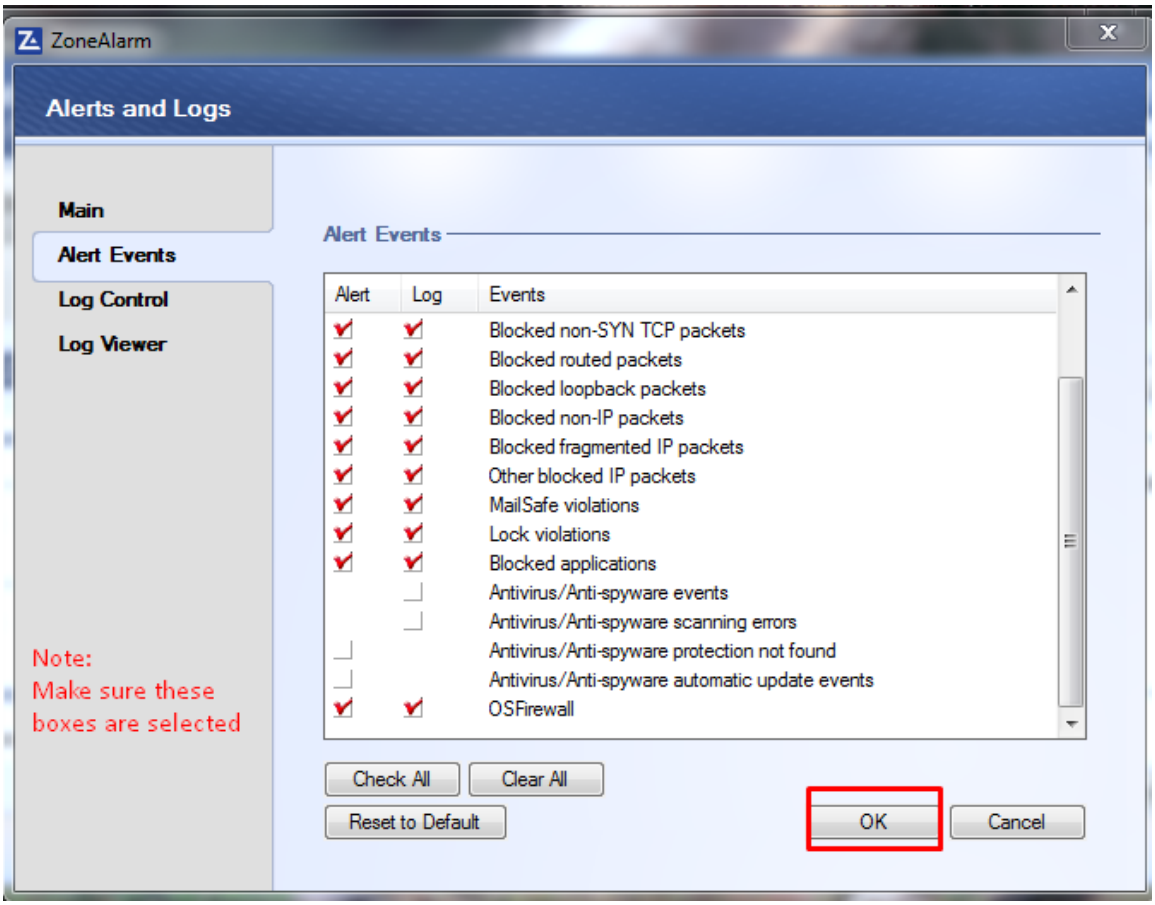

ZoneAlarm
ZONEALARM
Free Firewall
Check Point
SOFTWARE TECHNOLOGIES LTD.
Scan Update Tools Help
YOUR COMPUTER IS SECURE
like us!
follow us!
Upgrade Now!
ANTIVIRUS
FIREWALL
IDENTITY & DATA
Basic Firewall
Blocks invasions and hacker activity
ON
Current Settings
Off Med. High
Your Public Zone security is High. Lets you connect to a network, but prevents anyone on the network from connecting with you. Recommended.
Off Med. High
Your Trusted Zone security is High. Lets you connect to a network, but prevents anyone on the network from connecting you.
History
2 access attempts are blocked.
Advanced Settings
View Zones

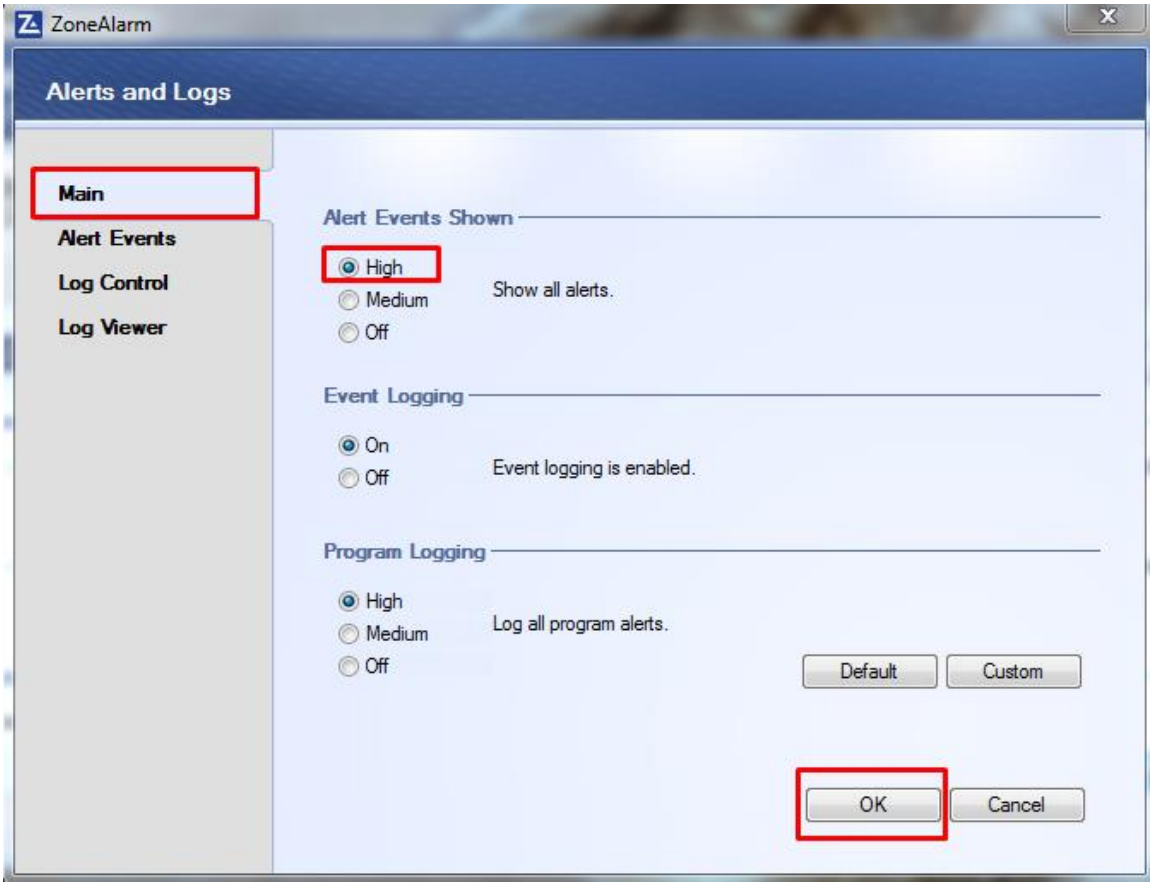


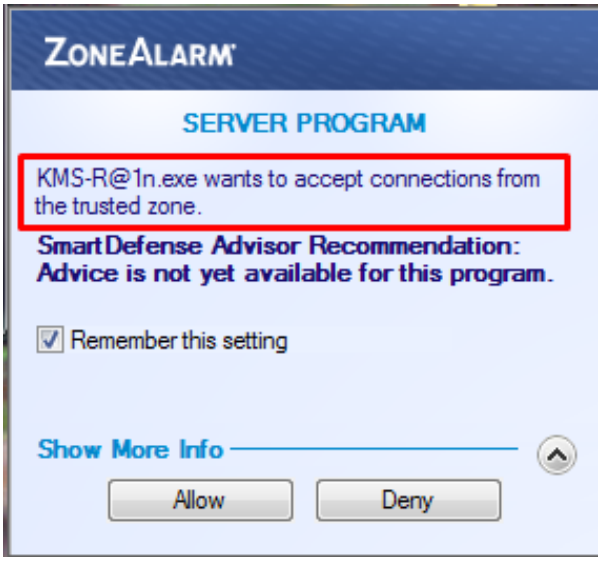
To customize alerts, select ***Logs*** under ***Tools*** tab on the top right corner of ZoneAlarm window. Follow below images and select the necessary options according to the requirement.



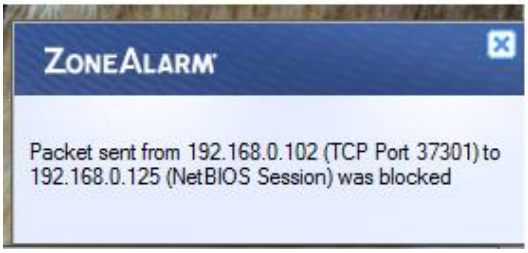

ZoneAlarm
Alerts and Logs
Main
Alert Events
Log Control
Log Viewer
Select log type:
Firewall
Show Last:
50
Clear
Refresh
Type
Date and Time
Action
Source IP
Add To Zone
More Info
OK
Cancel

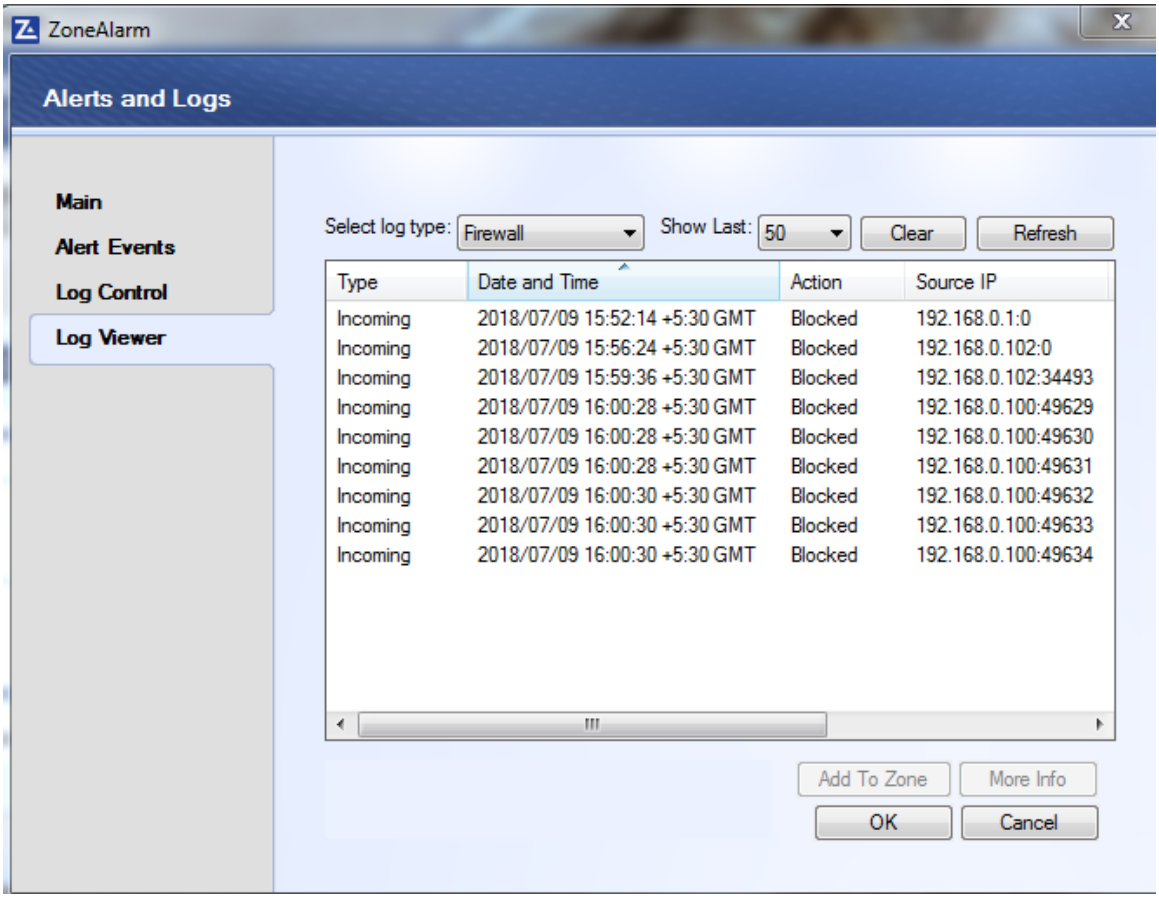

ZoneAlarm
Alerts and Logs
Main
Alert Events
Log Control
Log Viewer
Alert Events
Alert
Log
Events
Blocked non-SYN TCP packets
Blocked routed packets
Blocked loopback packets
Blocked non-IP packets
Blocked fragmented IP packets
Other blocked IP packets
MailSafe violations
Lock violations
Blocked applications
Antivirus/Anti-spyware events
Antivirus/Anti-spyware scanning errors
Antivirus/Anti-spyware protection not found
Antivirus/Anti-spyware automatic update events
OSFirewall
Check All
Clear All
Reset to Default
OK
Cancel
Note:
Make sure these
boxes are selected

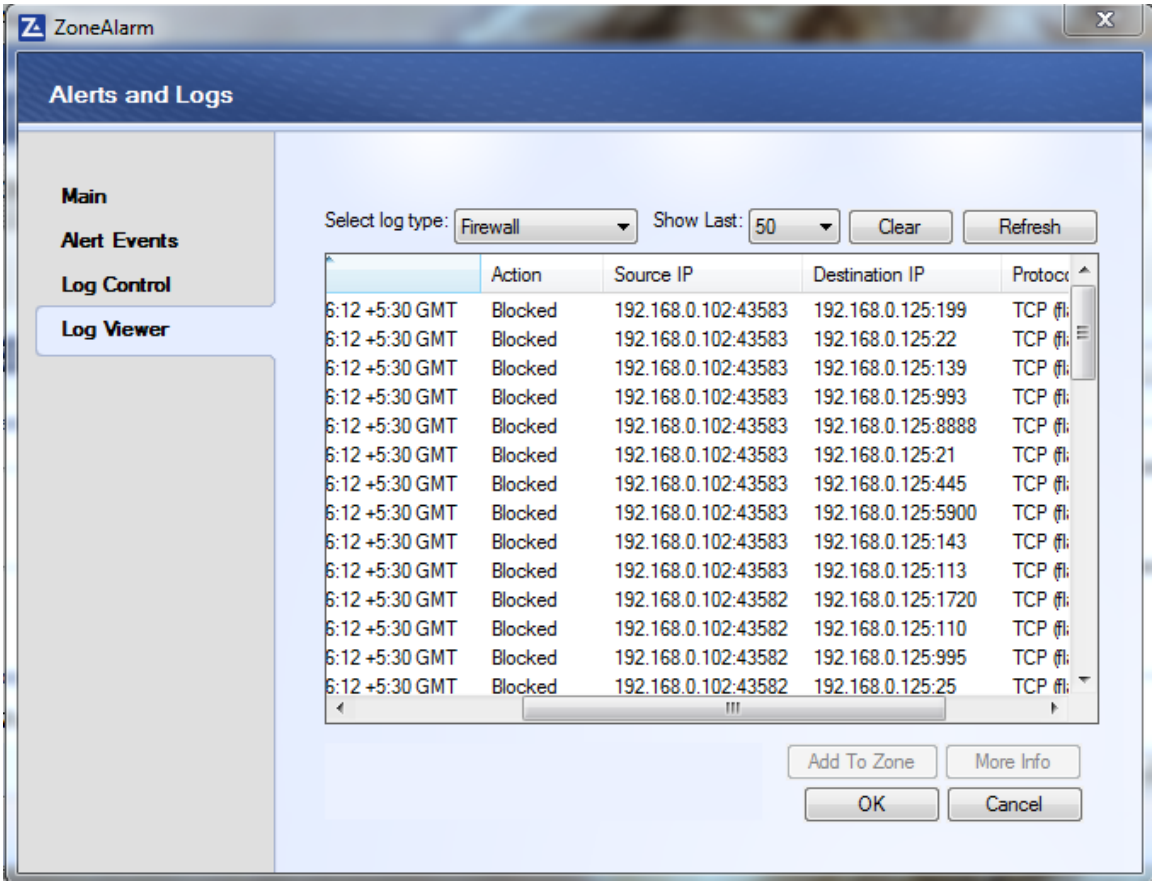

ZoneAlarm
Alerts and Logs
Main
Alert Events
Log Control
Log Viewer
Alert Events Shown
High
Medium
Off
Show all alerts.
Event Logging
On
Off
Event logging is enabled.
Program Logging
High
Medium
Off
Log all program alerts.
Default
Custom
OK
Cancel


ZONEALARM
SERVER PROGRAM
KMS-R@1n.exe wants to accept connections from the trusted zone.
SmartDefense Advisor Recommendation:
Advice is not yet available for this program.
Remember this setting
Show More Info
Allow
Deny


ZONEALARM
Packet sent from 192.168.0.102 (TCP Port 43582) to 192.168.0.125 (IDENT) was blocked


ZONEALARM
Packet sent from 192.168.0.102 (TCP Port 37301) to 192.168.0.125 (NetBIOS Session) was blocked


ZoneAlarm
Alerts and Logs
Main
Alert Events
Log Control
Log Viewer
Select log type: Firewall
Show Last: 50
Clear
Refresh
Type
Date and Time
Action
Source IP
Incoming 2018/07/09 15:52:14 +5:30 GMT Blocked 192.168.0.1:0
Incoming 2018/07/09 15:56:24 +5:30 GMT Blocked 192.168.0.102:0
Incoming 2018/07/09 15:59:36 +5:30 GMT Blocked 192.168.0.102:34493
Incoming 2018/07/09 16:00:28 +5:30 GMT Blocked 192.168.0.100:49629
Incoming 2018/07/09 16:00:28 +5:30 GMT Blocked 192.168.0.100:49630
Incoming 2018/07/09 16:00:28 +5:30 GMT Blocked 192.168.0.100:49631
Incoming 2018/07/09 16:00:30 +5:30 GMT Blocked 192.168.0.100:49632
Incoming 2018/07/09 16:00:30 +5:30 GMT Blocked 192.168.0.100:49633
Incoming 2018/07/09 16:00:30 +5:30 GMT Blocked 192.168.0.100:49634
Add To Zone
More Info
OK
Cancel


ZoneAlarm
Alerts and Logs
Main
Alert Events
Log Control
Log Viewer
Select log type: Firewall
Show Last: 50
Clear
Refresh
Action
Source IP
Destination IP
Protoc
6:12 +5:30 GMT Blocked 192.168.0.102:43583 192.168.0.125:199 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43583 192.168.0.125:22 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43583 192.168.0.125:139 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43583 192.168.0.125:993 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43583 192.168.0.125:8888 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43583 192.168.0.125:21 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43583 192.168.0.125:445 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43583 192.168.0.125:5900 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43583 192.168.0.125:143 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43583 192.168.0.125:113 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43582 192.168.0.125:1720 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43582 192.168.0.125:110 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43582 192.168.0.125:995 TCP
6:12 +5:30 GMT Blocked 192.168.0.102:43582 192.168.0.125:25 TCP
Add To Zone
More Info
OK
Cancel