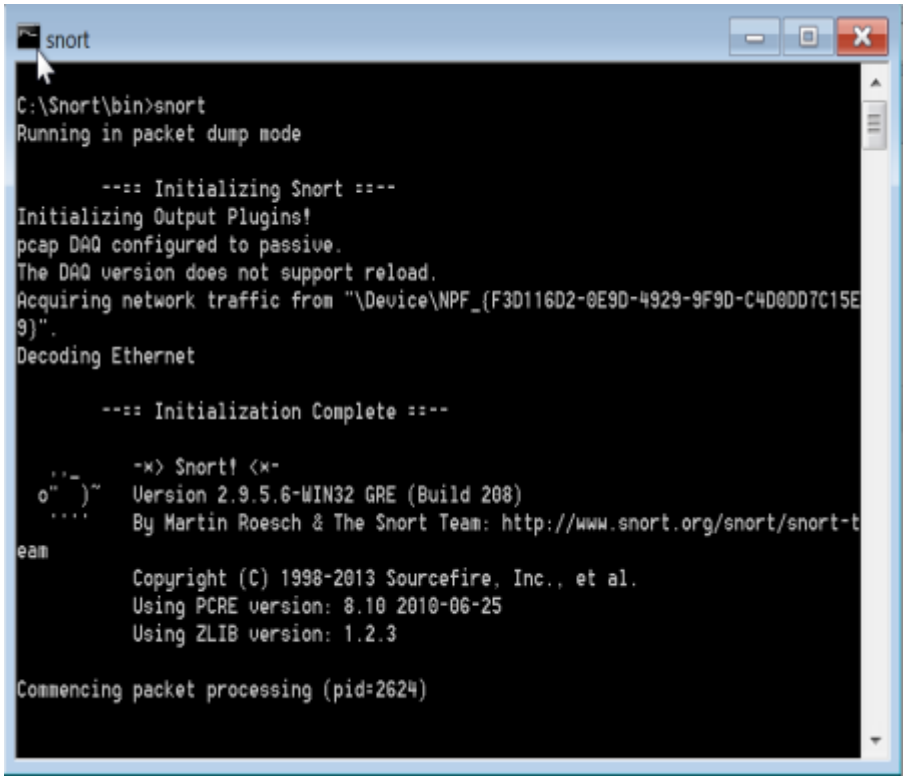
Evading IDS, Firewalls, and Honeypots
Lab Assignment (Module 12)

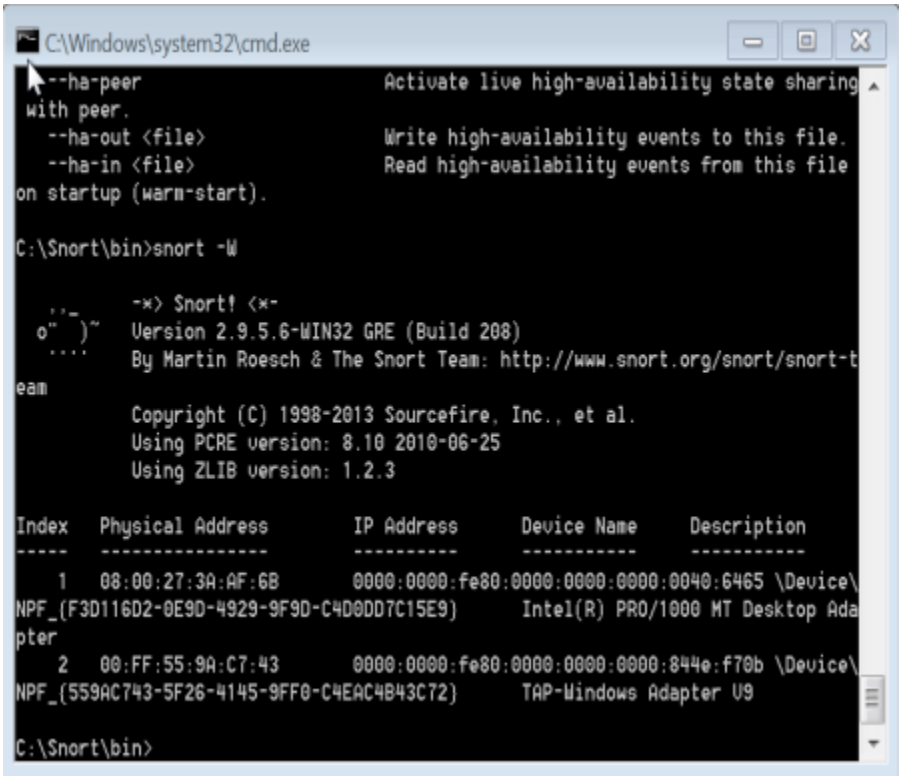
Name : Sachin Saj T K
Roll No : CB.EN.P2CEN18012
Date of Submission: 22/06/2019

Detecting Intrusions using Snort

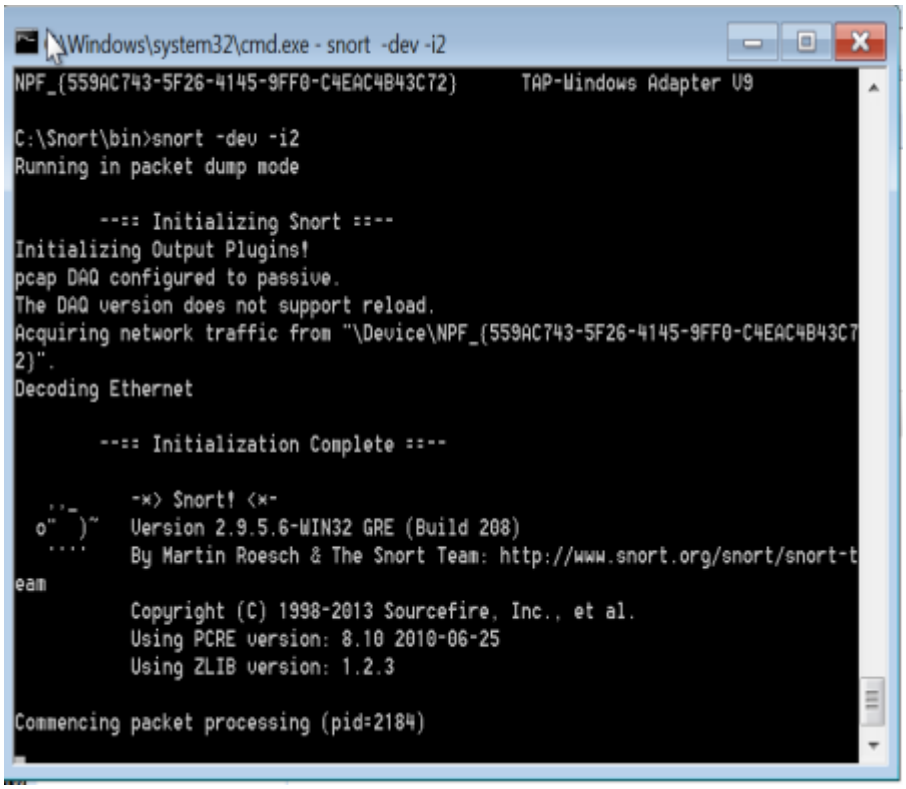
1. Open snort .



2. Snort –W list machine physical address, IP address and Ethernet Drivers



3. Now for enabling Ethernet Driver and make sure it is working properly snort –dev –i2



4. Now edit snort.conf using Notepad++

```
# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]

# other variables, these should not be modified
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.

# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH C:\Snort\rules
var SO_RULE_PATH C:\Snort\so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
```

```
##################################################
config paf_max: 16000

##################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
##################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so
```

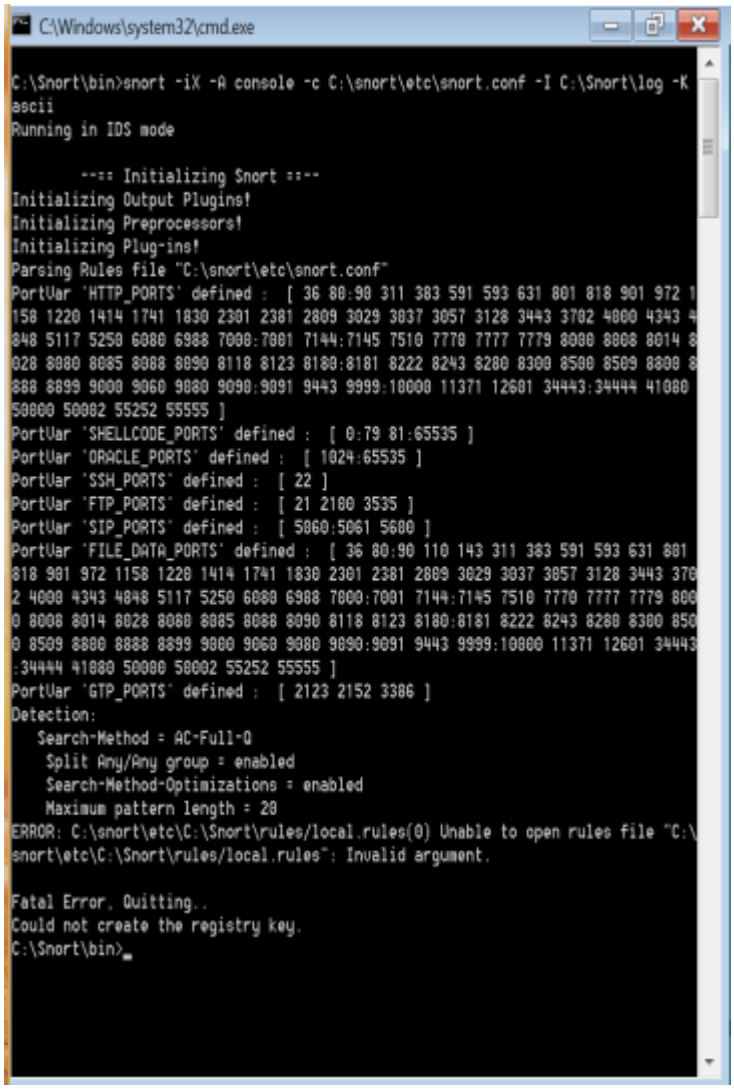
```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries
dynamicdetection directory /usr/local/lib/snort_dynamicrules

##################################################
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
##################################################
```

5. Now type snort –iX –A console –c C:\Snort\etc\snort.conf –I C:\Snort\log –K asci



```
C:\Windows\system32\cmd.exe
C:\Snort\bin>snort -iX -A console -c C:\snort\etc\snort.conf -I C:\Snort\log -K
ascii
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 36 80:90 311 383 591 593 631 801 818 901 972 1
158 1220 1414 1741 1830 2301 2381 2809 3029 3037 3057 3128 3443 3702 4000 4343 4
848 5117 5250 6080 6988 7000:7001 7144:7145 7510 7778 7777 7779 8000 8008 8014 8
028 8080 8085 8088 8090 8118 8123 8180:8181 8222 8243 8280 8300 8500 8509 8800 8
888 8899 9000 9060 9080 9090:9091 9443 9999:10000 11371 12601 34443:34444 41080
50000 50002 55252 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 36 80:90 110 143 311 383 591 593 631 801
818 901 972 1158 1220 1414 1741 1830 2301 2381 2809 3029 3037 3057 3128 3443 370
2 4000 4343 4848 5117 5250 6080 6988 7000:7001 7144:7145 7510 7778 7777 7779 800
0 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8222 8243 8280 8300 850
0 8509 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999:10000 11371 12601 34443
:34444 41080 50000 50002 55252 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
ERROR: C:\snort\etc\C:\Snort\rules/local.rules(0) Unable to open rules file "C:\
snort\etc\C:\Snort\rules/local.rules": Invalid argument.

Fatal Error, Quitting..
Could not create the registry key.
C:\Snort\bin>_
```

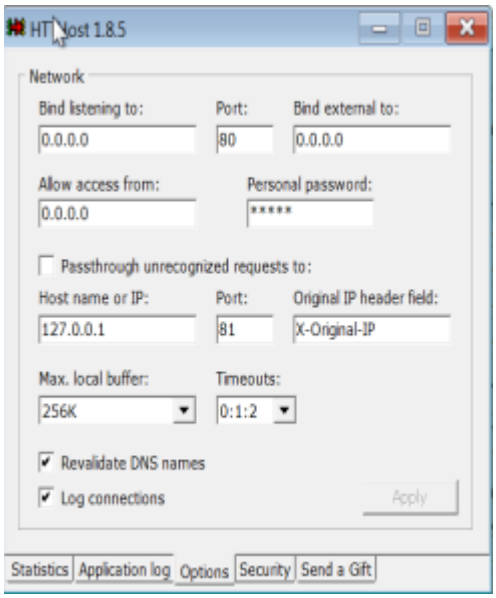
Note: Fatal error, this shows that, there was some error in editing snort.conf file.

Lab Analysis

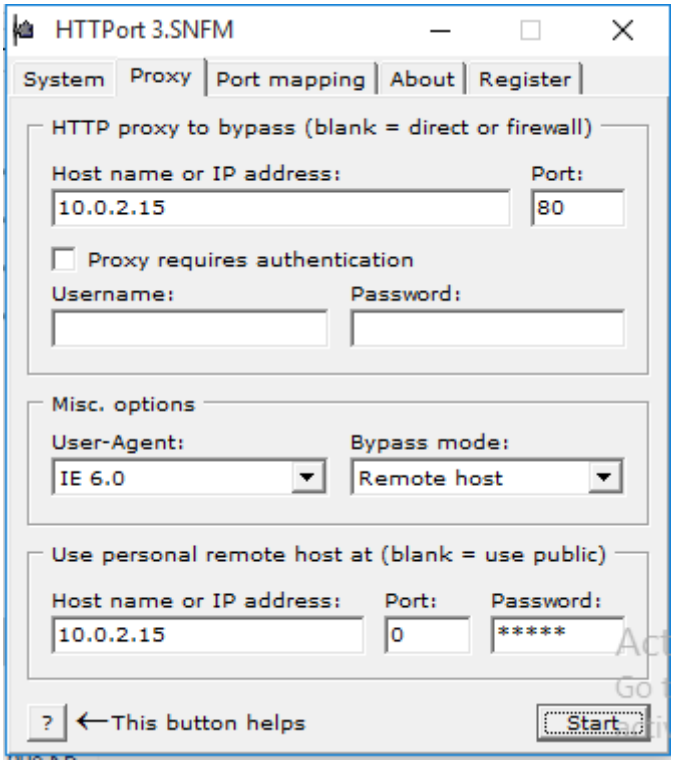
Tool/Utility	**Information Collected/Objective Achieved**
Snort	Output: Victim machine log were not captured

HTTP Tunneling Using HTTPort

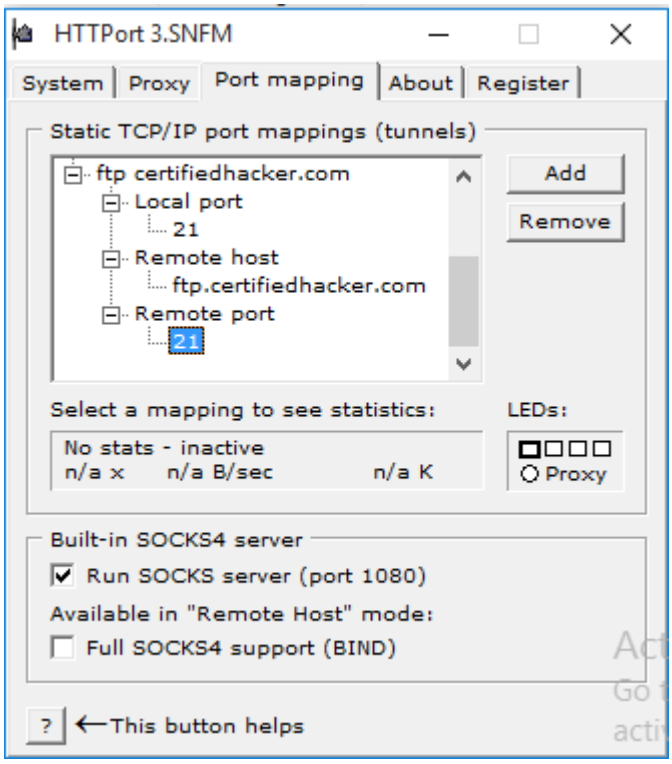
1. Now first start HTTHost in one virtual box.



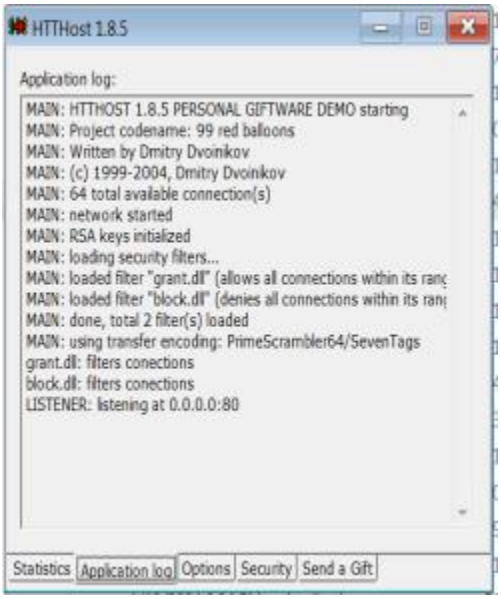
2. Now, in another virtual box open HTTPort, enter the host IP address and port number of the targeted machine.



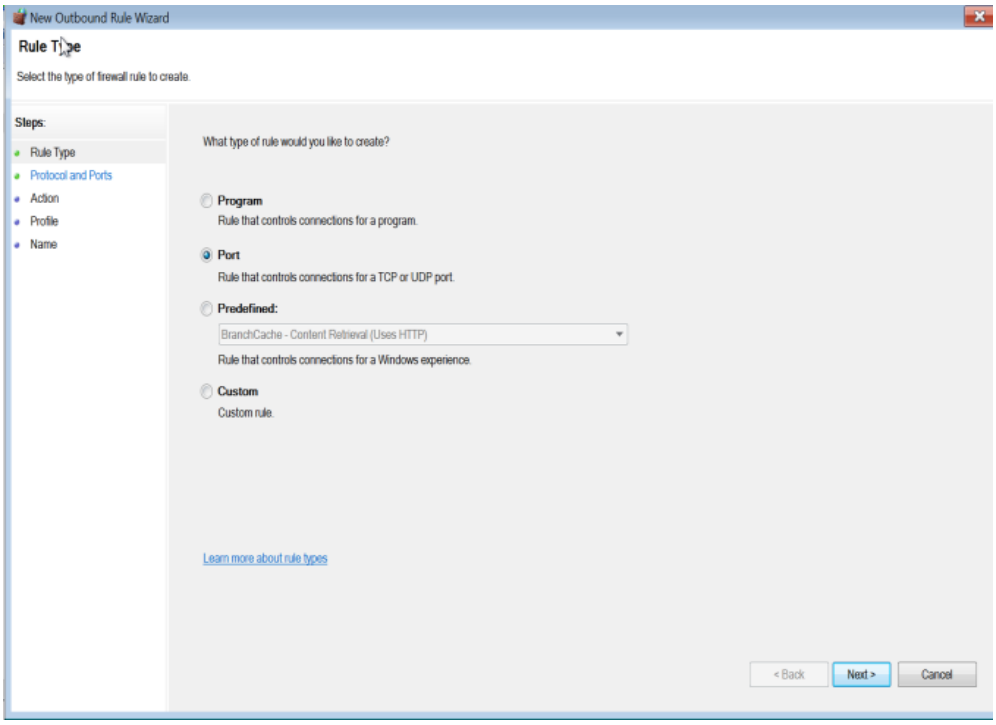
3. Now do port mapping

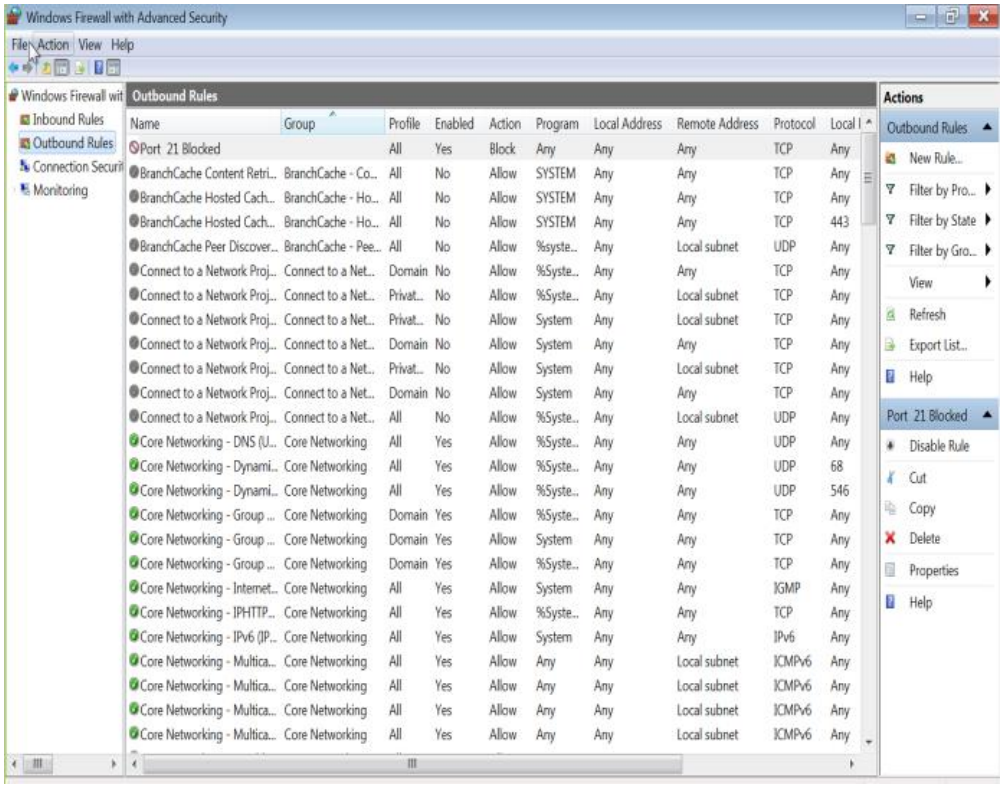


4. Now check whether the listener is listening at 0.0.0.0:80 (running properly)

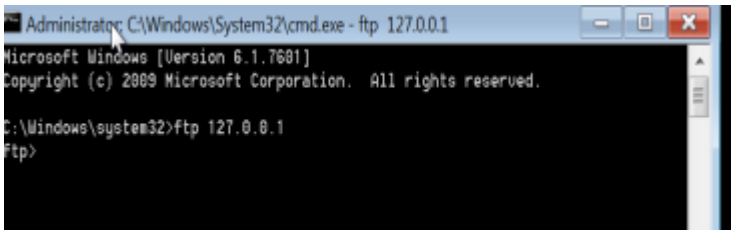


5. Now go to windows firewall with advanced security, in outbound rules, create new rule.





6. Now type ftp 127.0.0.1 in command prompt, we can see the connection is blocked at the local host



Lab Analysis

Tool/Utility	**Information Collected/Objective Achieved**
HTTPort	**Proxy server used**: 10.0.0.4
	Port Scanned: 80
	Result : ftp 127.0.0.1 connected to 127.0.0.1