Task Overview

BASICS TASK 1: [INTRODUCTION TO NETWORK SECURITY]

Introduction:

Greetings, inhabitants of cyberspace security! In the present day, this networked world has seemingly made it imperative that individuals or institutions appreciate and put in to practice very elementary ways and means of safety from different kinds of dangers that could ever be encountered within the net. Be it an individual or a small business, there is always need to have a safe network more so in cases where the network is used in handling sensitive data that needs protection as well as the data integrity . In this assignment, we will cover the definition and the importance of network security and the potential threats that may lead to its compromise. We will also outline some measures that can be used to mitigate introduction of such risks and reduce their effects.

Upon completion of this task, basic principles and concepts of network security such as identification of threats and securing a small network using the acceptable standards will have been covered. This will enable you to not only keep your network safe, but also to understand the more complex areas of network security.

In this way, we can proceed on our task of deepening our understanding of how to properly secure networks starting from the identification of threats to their management for our own safety. And with enough work and proper security practices in place, the Internet can be safe for us and everyone else that we care about.

The concept of network security must be understood as it relates to data protection, integrity and availability of network resources. Below is a brief definition of some common network threats and some elementary security solutions.

Network Threats

1) Malware – A form of software that influences illegal access to networks such as trojan horses, spyware and other malicious codes.

2) Phishing – An act of social engineering that focuses on fooling users into providing personally identifiable information in an effort to abuse it. This is done mainly via fake emails and websites.

3) DDoS Attacks – A distributed denial of service attack normally floods a network or server with too much traffic rendering it unavailable to legitimate users.

4) Man-in-the-Middle (MitM) Attacks – Involves secretly listening in and or tampering with the conversation between two parties.

5) Unauthorized access – This involves efforts to gain entry into a network or system without permission as such acts may lead to data loss or corruption.

6) Insider Threats – These are threats emanating from inside the company whether intentional or unregulated.

Basic Security Measures

1) Firewalls – A firewall serves to monitor and control the incoming and outgoing network traffic based on the predetermined security policy of the organization.

2) Antivirus – The implementation of antivirus helps prevent the intrusion of viruses, worms, malware, and trojan horses into the organization's cyberspace.

3) Regular Software Updates – The operable systems and the applications installed in the systems are vigorously needed to be updated against the weaknesses present.

4) Secure Password Practices – Strong Password policies that incorporate complexity and heighten frequencies of password change assist in mitigating unauthorized logins.

5) Network Segmentation – Alleviating the potential damage in case of a successful attack, and improving the security management as well.

6) Virtual Private Networks (VPNs) – A VPN is a tool that protects the connection of remote users to the information system by encrypting all, or selected, data that goes over the web.

7)User Education – Providing training on issues such as phishing and related threats, along with encouraging users to observe safe browsing behavior, would yield a great decrease in the level of risk present.

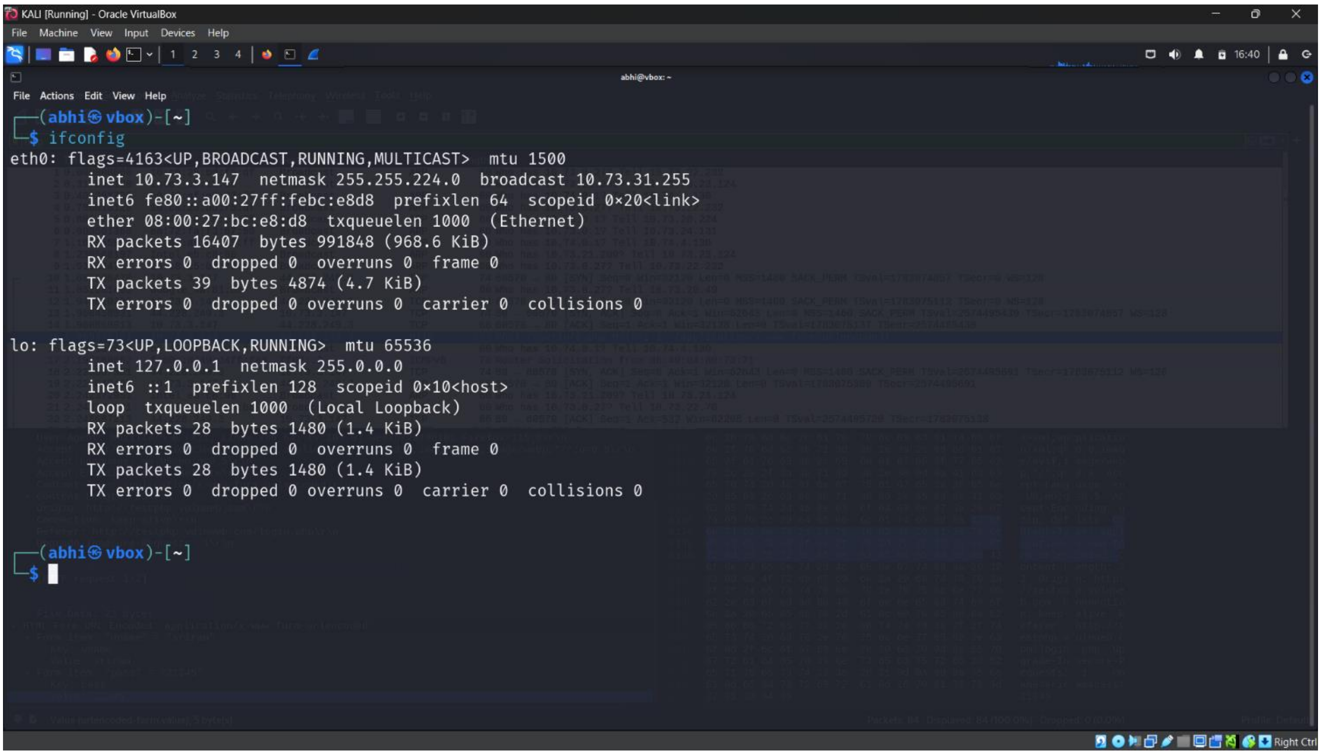
8)Backup Solutions – Having a plan in place for the backward coping of any data such backups being done frequently creates assurance that information will not be lost mostly to software like ransomware.

Tools and methods:

Firewall (Windows Defender Firewall or a basic hardware firewall), Wireshark.

Steps taken to complete the task:

1.Type 'ifconfig' and click enter key. This should display your Kali ip address.

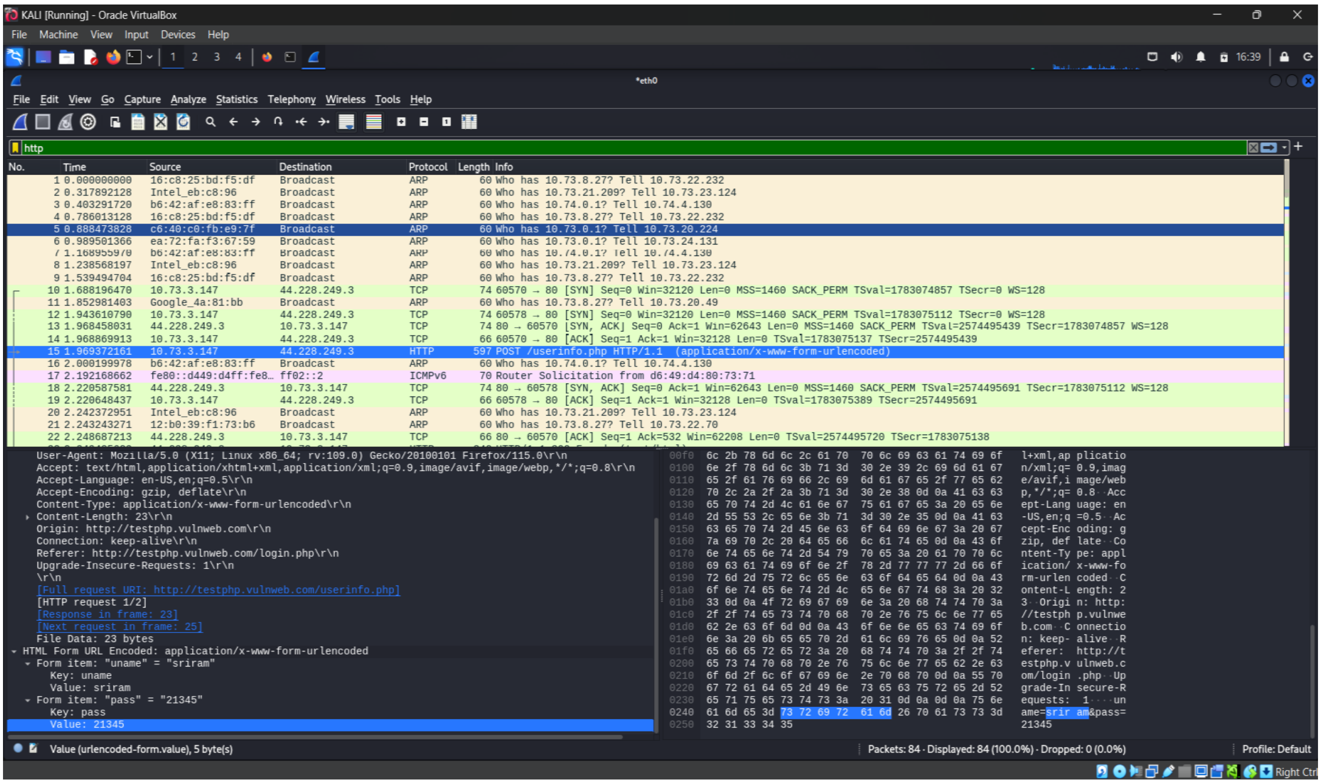

KALI [Running] - Oracle VirtualBox
File Machine View Input Devices Help
abhi@vbox: ~
File Actions Edit View Help
16:40
Right Ctrl

```
┌──(abhi㉿vbox)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.73.3.147  netmask 255.255.224.0  broadcast 10.73.31.255
        inet6 fe80::a00:27ff:febc:e8d8  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bc:e8:d8  txqueuelen 1000  (Ethernet)
        RX packets 16407  bytes 991848 (968.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39  bytes 4874 (4.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 28  bytes 1480 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 1480 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(abhi㉿vbox)-[~]
└─$ ▌
```

2.Launch wireshark on your host system, configure to capture traffic based on your network connections.


KALI [Running] - Oracle VirtualBox
File Machine View Input Devices Help
16:39
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Right Ctrl

```
No.  Time          Source                Destination     Protocol  Length Info
   1 0.000000000   16:c8:25:bd:f5:df     Broadcast       ARP       60 Who has 10.73.8.27? Tell 10.73.22.232
   2 0.317892128   Intel_eb:c8:96        Broadcast       ARP       60 Who has 10.73.21.209? Tell 10.73.23.124
   3 0.403291720   b6:42:af:e8:83:ff     Broadcast       ARP       60 Who has 10.74.0.1? Tell 10.74.4.130
   4 0.786013128   16:c8:25:bd:f5:df     Broadcast       ARP       60 Who has 10.73.8.27? Tell 10.73.22.232
   5 0.888473828   c6:40:c0:fb:e9:7f     Broadcast       ARP       60 Who has 10.73.0.1? Tell 10.73.20.224
   6 0.989501366   ea:72:fa:f3:67:59     Broadcast       ARP       60 Who has 10.73.0.1? Tell 10.73.24.131
   7 1.168955970   b6:42:af:e8:83:ff     Broadcast       ARP       60 Who has 10.74.0.1? Tell 10.74.4.130
   8 1.238568197   Intel_eb:c8:96        Broadcast       ARP       60 Who has 10.73.21.209? Tell 10.73.23.124
   9 1.539494704   16:c8:25:bd:f5:df     Broadcast       ARP       60 Who has 10.73.8.27? Tell 10.73.22.232
  10 1.688196470   10.73.3.147           44.228.249.3    TCP       74 60570 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1783074857 TSecr=0 WS=128
  11 1.852981403   Google_4a:81:bb       Broadcast       ARP       60 Who has 10.73.8.27? Tell 10.73.20.49
  12 1.943610790   10.73.3.147           44.228.249.3    TCP       74 60578 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1783075112 TSecr=0 WS=128
  13 1.968458031   44.228.249.3          10.73.3.147     TCP       74 80 → 60570 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM TSval=2574495439 TSecr=1783074857 WS=128
  14 1.968869913   10.73.3.147           44.228.249.3    TCP       66 60570 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1783075137 TSecr=2574495439
  15 1.969372161   10.73.3.147           44.228.249.3    HTTP     597 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
  16 2.000199978   b6:42:af:e8:83:ff     Broadcast       ARP       60 Who has 10.74.0.1? Tell 10.74.4.130
  17 2.192168662   fe80::d449:d4ff:fe8…  ff02::2         ICMPv6    70 Router Solicitation from d6:49:d4:80:73:71
  18 2.220587581   44.228.249.3          10.73.3.147     TCP       74 80 → 60578 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM TSval=2574495691 TSecr=1783075112 WS=128
  19 2.220648437   10.73.3.147           44.228.249.3    TCP       66 60578 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1783075389 TSecr=2574495691
  20 2.242372951   Intel_eb:c8:96        Broadcast       ARP       60 Who has 10.73.21.209? Tell 10.73.23.124
  21 2.243243271   12:b0:39:f1:73:b6     Broadcast       ARP       60 Who has 10.73.8.27? Tell 10.73.22.70
  22 2.248687213   44.228.249.3          10.73.3.147     TCP       66 80 → 60570 [ACK] Seq=1 Ack=532 Win=62208 Len=0 TSval=2574495720 TSecr=1783075138
```

```
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  ▸ Content-Length: 23\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 1/2]
    [Response in frame: 23]
    [Next request in frame: 25]
    File Data: 23 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "uname" = "sriram"
      Key: uname
      Value: sriram
  ▾ Form item: "pass" = "21345"
      Key: pass
      Value: 21345
```

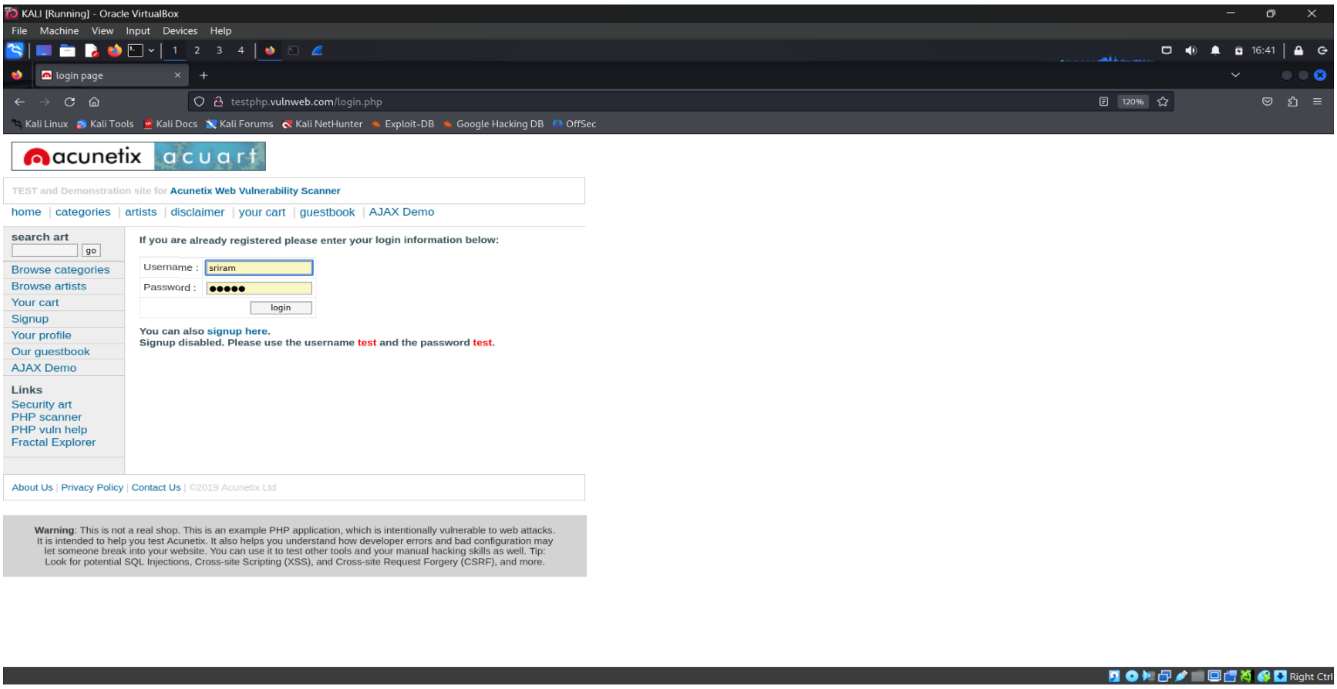
```
00f0  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
0100  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 69 6d 61 67   n/xml;q= 0.9,imag
0110  65 2f 61 76 69 66 2c 69  6d 61 67 65 2f 77 65 62   e/avif,i mage/web
0120  70 2c 2a 2f 2a 3b 71 3d  30 2e 38 0d 0a 41 63 63   p,*/*;q= 0.8··Acc
0130  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Lang uage: en
0140  2d 55 53 2c 65 6e 3b 71  3d 30 2e 35 0d 0a 41 63   -US,en;q =0.5··Ac
0150  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
0160  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 43 6f   zip, def late··Co
0170  6e 74 65 6e 74 2d 54 79  70 65 3a 20 61 70 70 6c   ntent-Ty pe: appl
0180  69 63 61 74 69 6f 6e 2f  78 2d 77 77 77 2d 66 6f   ication/ x-www-fo
0190  72 6d 2d 75 72 6c 65 6e  63 6f 64 65 64 0d 0a 43   rm-urlen coded··C
01a0  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 32   ontent-L ength: 2
01b0  33 0d 0a 4f 72 69 67 69  6e 3a 20 68 74 74 70 3a   3··Origi n: http:
01c0  2f 2f 74 65 73 74 70 68  70 2e 76 75 6c 6e 77 65   //testph p.vulnwe
01d0  62 2e 63 6f 6d 0d 0a 43  6f 6e 6e 65 63 74 69 6f   b.com··C onnectio
01e0  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 52   n: keep- alive··R
01f0  65 66 65 72 65 72 3a 20  68 74 74 70 3a 2f 2f 74   eferer:  http://t
0200  65 73 74 70 68 70 2e 76  75 6c 6e 77 65 62 2e 63   estphp.v ulnweb.c
0210  6f 6d 2f 6c 6f 67 69 6e  2e 70 68 70 0d 0a 55 70   om/login .php··Up
0220  67 72 61 64 65 2d 49 6e  73 65 63 75 72 65 2d 52   grade-In secure-R
0230  65 71 75 65 73 74 73 3a  20 31 0d 0a 0d 0a 75 6e   equests:  1····un
0240  61 6d 65 3d 73 72 69 72  61 6d 26 70 61 73 73 3d   ame=srir am&pass=
0250  32 31 33 34 35                                     21345
```

Value (urlencoded-form.value), 5 byte(s)

Packets: 84 · Displayed: 84 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

3.Visit http://testphp.vulnweb.com/ login page in your Kali Linux.



KALI [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
16:41
login page
testphp.vulnweb.com/login.php
120%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuart
Right Ctrl

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art [ ] go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

If you are already registered please enter your login information below:

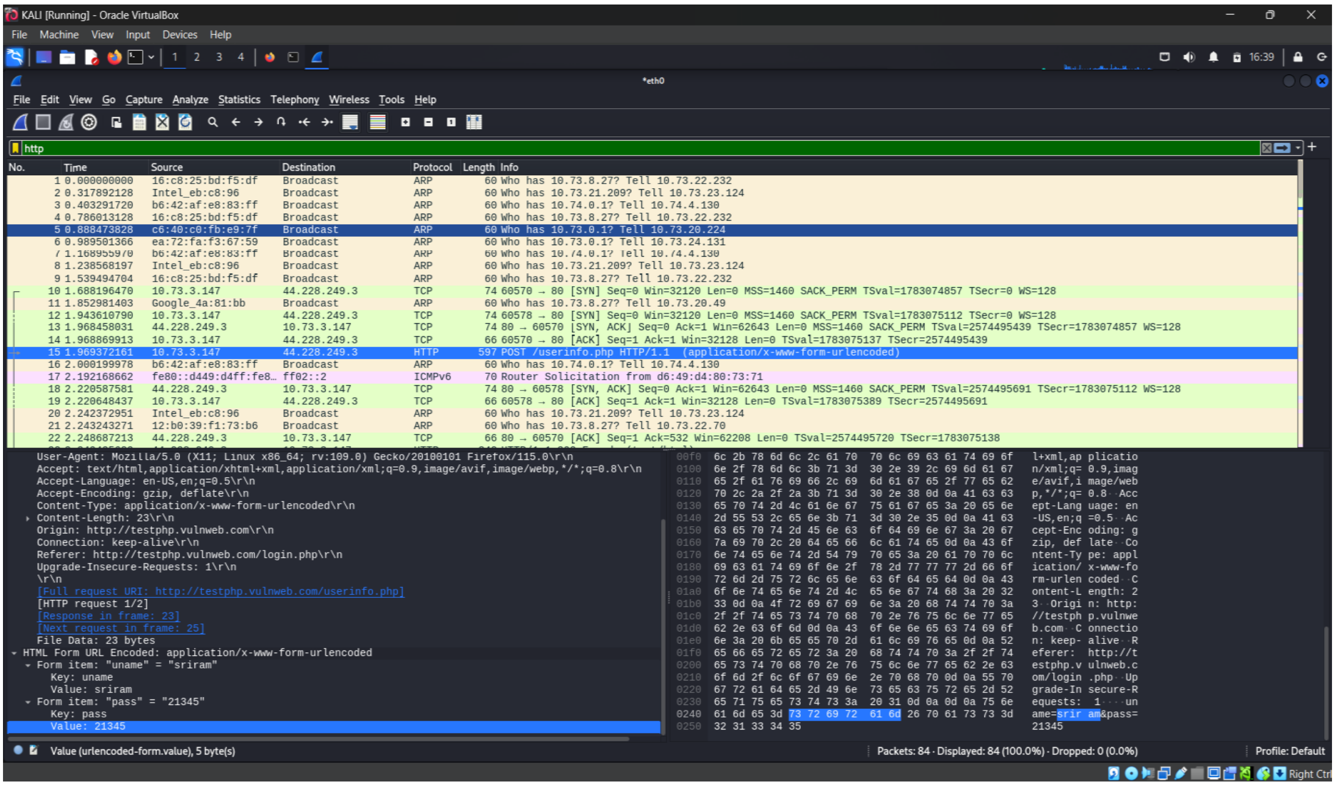
Username : sriram
Password : ●●●●●
login

You can also signup here.
Signup disabled. Please use the username test and the password test.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

4.the username is "Sriram" and the password is "21345" and Login with the credential, Capture the traffic using your wireshark. Filter for 'http' and find post request, Right click on post request and follow the tcp stream.You should clearly see the credentials you entered on the login page you visited in your Kali.



KALI [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
16:39
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Right Ctrl

http

```
No.   Time        Source              Destination    Protocol Length Info
    1 0.000000000 16:c8:25:bd:f5:df   Broadcast      ARP      60 Who has 10.73.8.27? Tell 10.73.22.232
    2 0.317892128 Intel_eb:c8:96      Broadcast      ARP      60 Who has 10.73.21.209? Tell 10.73.23.124
    3 0.403291720 b6:42:af:e8:83:ff   Broadcast      ARP      60 Who has 10.74.0.1? Tell 10.74.4.130
    4 0.786013128 16:c8:25:bd:f5:df   Broadcast      ARP      60 Who has 10.73.8.27? Tell 10.73.22.232
    5 0.888473828 c6:40:c0:fb:e9:7f   Broadcast      ARP      60 Who has 10.73.0.1? Tell 10.73.20.224
    6 0.989501366 ea:72:fa:f3:67:59   Broadcast      ARP      60 Who has 10.73.0.1? Tell 10.73.24.131
    7 1.168955970 b6:42:af:e8:83:ff   Broadcast      ARP      60 Who has 10.74.0.1? Tell 10.74.4.130
    8 1.238568197 Intel_eb:c8:96      Broadcast      ARP      60 Who has 10.73.21.209? Tell 10.73.23.124
    9 1.539494704 16:c8:25:bd:f5:df   Broadcast      ARP      60 Who has 10.73.8.27? Tell 10.73.22.232
   10 1.688196470 10.73.3.147         44.228.249.3   TCP      74 60570 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1783074857 TSecr=0 WS=128
   11 1.852981403 Google_4a:81:bb     Broadcast      ARP      60 Who has 10.73.8.27? Tell 10.73.20.49
   12 1.943610790 10.73.3.147         44.228.249.3   TCP      74 60578 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1783075112 TSecr=0 WS=128
   13 1.968458031 44.228.249.3        10.73.3.147    TCP      74 80 → 60570 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM TSval=2574495439 TSecr=1783074857 WS=128
   14 1.968869913 10.73.3.147         44.228.249.3   TCP      66 60570 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1783075137 TSecr=2574495439
   15 1.969372161 10.73.3.147         44.228.249.3   HTTP    597 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
   16 2.000199978 b6:42:af:e8:83:ff   Broadcast      ARP      60 Who has 10.74.0.1? Tell 10.74.4.130
   17 2.192168662 fe80::d449:d4ff:fe8… ff02::2       ICMPv6   70 Router Solicitation from d6:49:d4:80:73:71
   18 2.220587581 44.228.249.3        10.73.3.147    TCP      74 80 → 60578 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM TSval=2574495691 TSecr=1783075112 WS=128
   19 2.220648437 10.73.3.147         44.228.249.3   TCP      66 60578 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1783075389 TSecr=2574495691
   20 2.242372951 Intel_eb:c8:96      Broadcast      ARP      60 Who has 10.73.21.209? Tell 10.73.23.124
   21 2.243243271 12:b0:39:f1:73:b6   Broadcast      ARP      60 Who has 10.73.8.27? Tell 10.73.22.70
   22 2.248687213 44.228.249.3        10.73.3.147    TCP      66 80 → 60570 [ACK] Seq=1 Ack=532 Win=62208 Len=0 TSval=2574495720 TSecr=1783075138
```

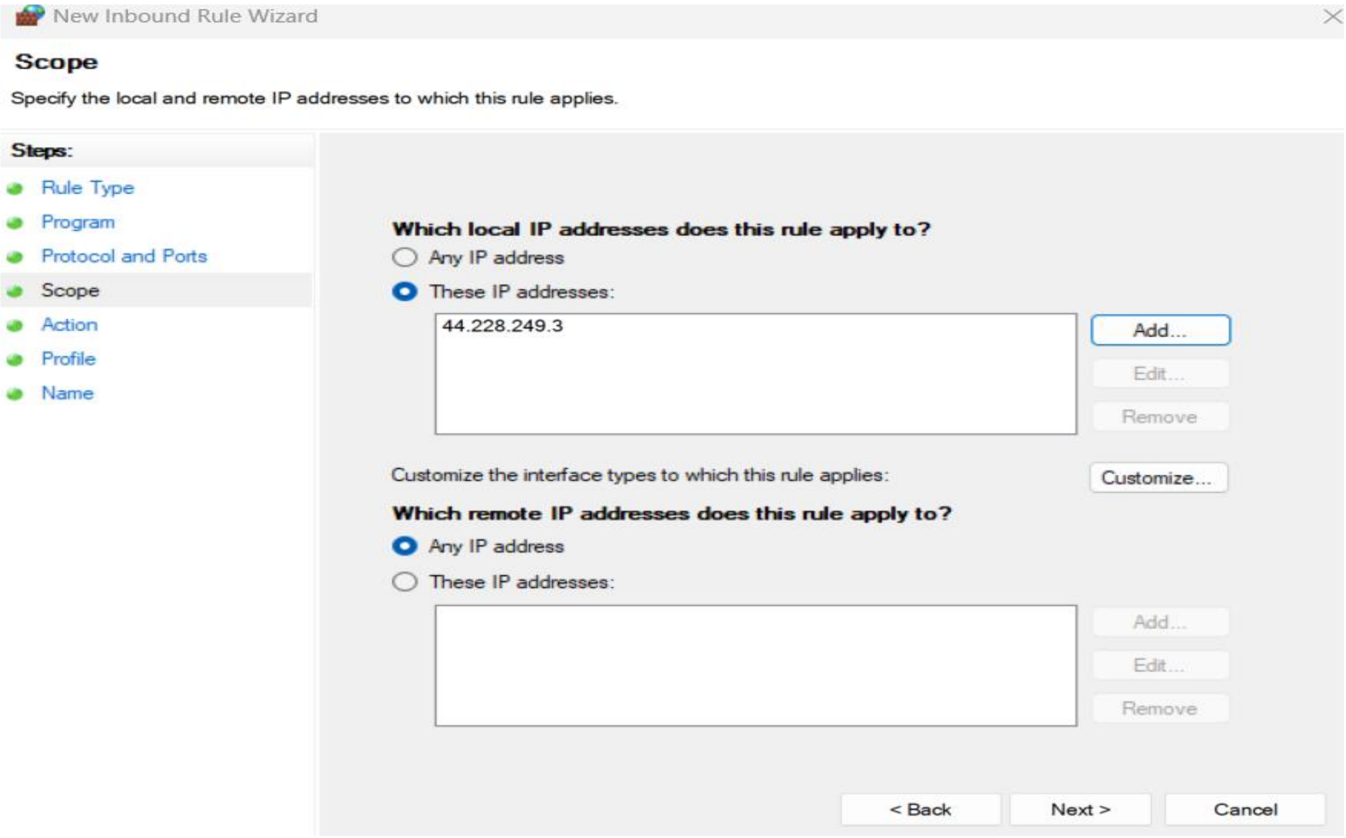
```
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  › Content-Length: 23\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 1/2]
    [Response in frame: 23]
    [Next request in frame: 25]
    File Data: 23 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "uname" = "sriram"
      Key: uname
      Value: sriram
  ▾ Form item: "pass" = "21345"
      Key: pass
      Value: 21345
```

```
00f0  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
0100  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 69 6d 61 67   n/xml;q= 0.9,imag
0110  65 2f 61 76 69 66 2c 69  6d 61 67 65 2f 77 65 62   e/avif,i mage/web
0120  70 2c 2a 2f 2a 3b 71 3d  30 2e 38 0d 0a 41 63 63   p,*/*;q= 0.8··Acc
0130  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Lang uage: en
0140  2d 55 53 2c 65 6e 3b 71  3d 30 2e 35 0d 0a 41 63   -US,en;q =0.5··Ac
0150  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
0160  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 43 6f   zip, def late··Co
0170  6e 74 65 6e 74 2d 54 79  70 65 3a 20 61 70 70 6c   ntent-Ty pe: appl
0180  69 63 61 74 69 6f 6e 2f  78 2d 77 77 77 2d 66 6f   ication/ x-www-fo
0190  72 6d 2d 75 72 6c 65 6e  63 6f 64 65 64 0d 0a 43   rm-urlen coded··C
01a0  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 32   ontent-L ength: 2
01b0  33 0d 0a 4f 72 69 67 69  6e 3a 20 68 74 74 70 3a   3··Origi n: http:
01c0  2f 2f 74 65 73 74 70 68  70 2e 76 75 6c 6e 77 65   //testph p.vulnwe
01d0  62 2e 63 6f 6d 0d 0a 43  6f 6e 6e 65 63 74 69 6f   b.com··C onnectio
01e0  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 52   n: keep- alive··R
01f0  65 66 65 72 65 72 3a 20  68 74 74 70 3a 2f 2f 74   eferer:  http://t
0200  65 73 74 70 68 70 2e 76  75 6c 6e 77 65 62 2e 63   estphp.v ulnweb.c
0210  6f 6d 2f 6c 6f 67 69 6e  2e 70 68 70 0d 0a 55 70   om/login .php··Up
0220  67 72 61 64 65 2d 49 6e  73 65 63 75 72 65 2d 52   grade-In secure-R
0230  65 71 75 65 73 74 73 3a  20 31 0d 0a 0d 0a 75 6e   equests:  1····un
0240  61 6d 65 3d 73 72 69 72  61 6d 26 70 61 73 73 3d   ame=srir am&pass=
0250  32 31 33 34 35                                     21345
```

Value (urlencoded-form.value), 5 byte(s)   Packets: 84 · Displayed: 84 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

This is visible because http protocol is unsecured.

5.To implement security measures using window Firewall on host system. Click on window firewall icon goto- advanced setting- Inbound Rules, Click on new ruleSelect 'custom' from rule, typeClick on 'Scope' You have local and remote ip address sections. Set rule on local ip address Input your desired device ip address which you intend to block it access to your local network.



New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

○ Any IP address

● These IP addresses:

44.228.249.3

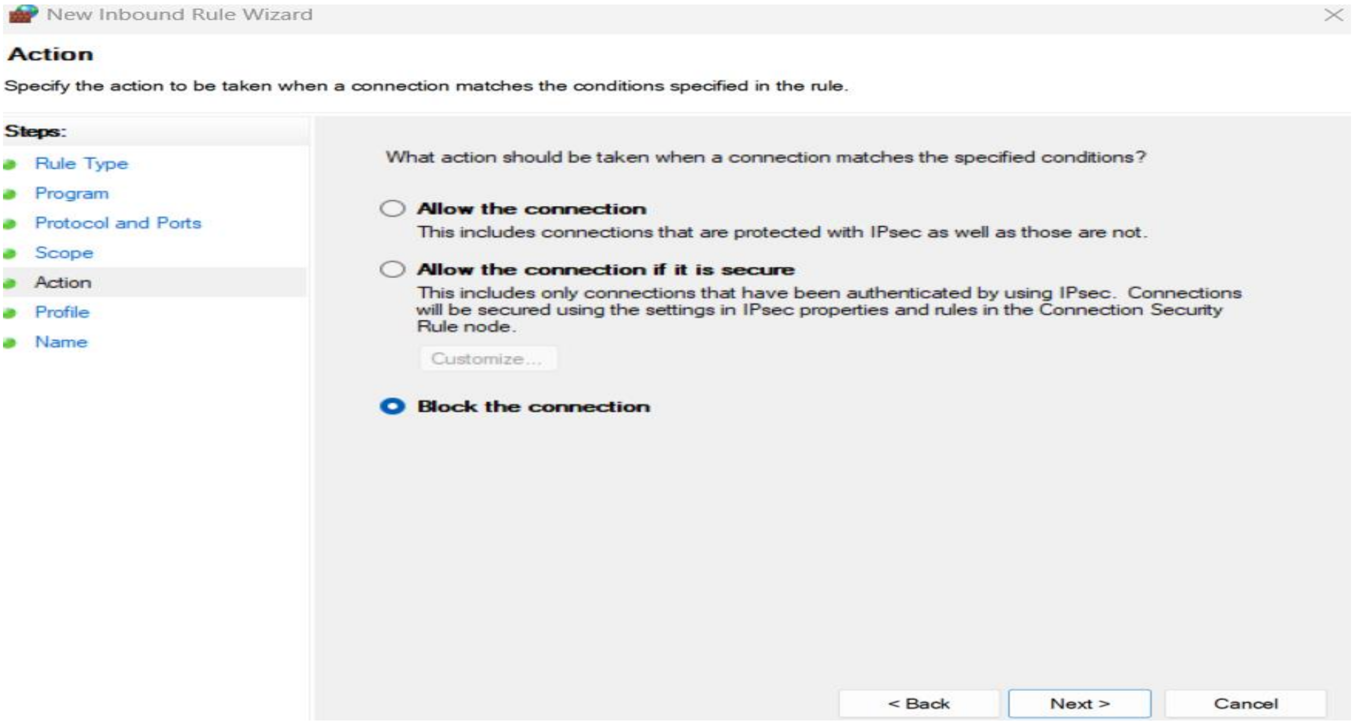
Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

6.Click on block the connection.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

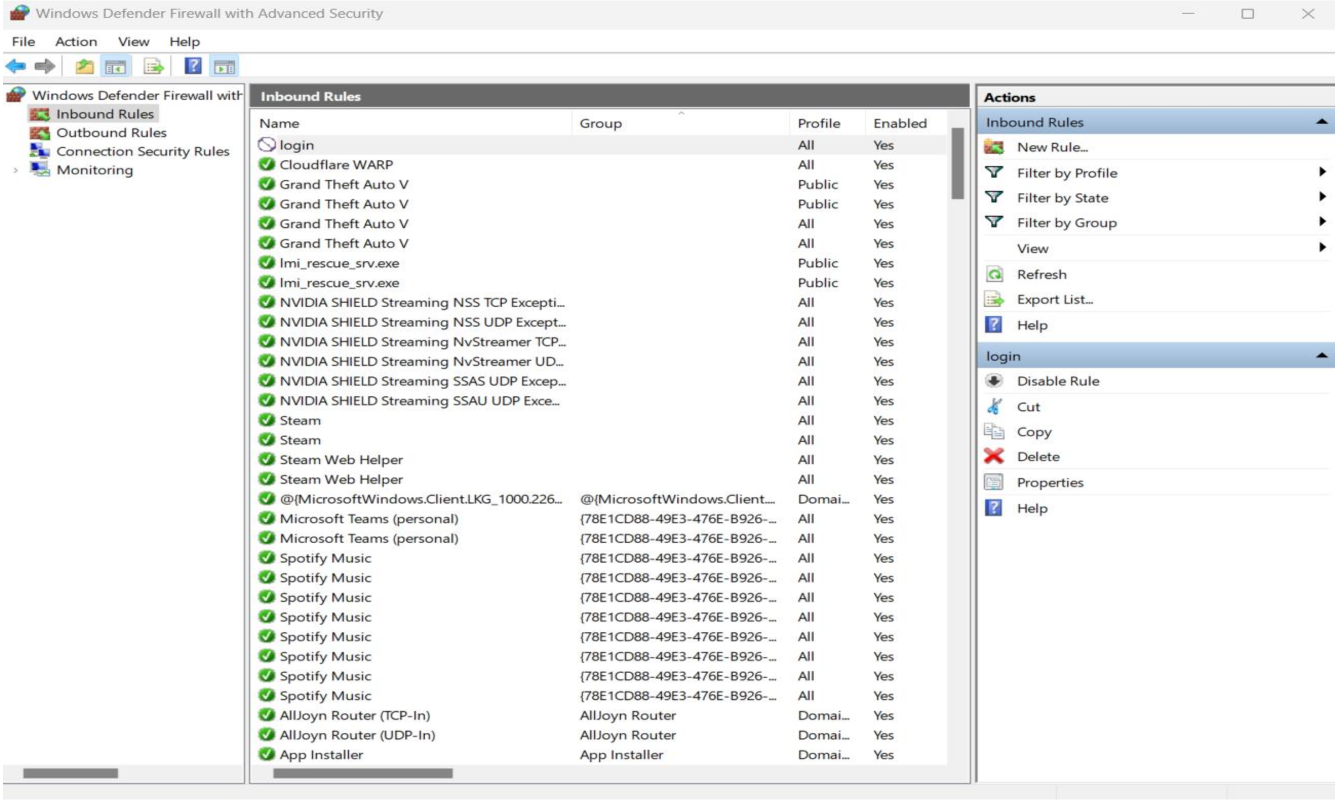
What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

7.Input name (login) to identify the rule you just created, Click finish. Your window firewall will block the device ip address you provided preventing access to your network.



Inbound Rules

Name	Group	Profile	Enabled
login		All	Yes
Cloudflare WARP		All	Yes
Grand Theft Auto V		Public	Yes
Grand Theft Auto V		Public	Yes
Grand Theft Auto V		All	Yes
Grand Theft Auto V		All	Yes
lmi_rescue_srv.exe		Public	Yes
lmi_rescue_srv.exe		Public	Yes
NVIDIA SHIELD Streaming NSS TCP Excepti...		All	Yes
NVIDIA SHIELD Streaming NSS UDP Except...		All	Yes
NVIDIA SHIELD Streaming NvStreamer TCP...		All	Yes
NVIDIA SHIELD Streaming NvStreamer UD...		All	Yes
NVIDIA SHIELD Streaming SSAS UDP Excep...		All	Yes
NVIDIA SHIELD Streaming SSAU UDP Exce...		All	Yes
Steam		All	Yes
Steam		All	Yes
Steam Web Helper		All	Yes
Steam Web Helper		All	Yes
@{MicrosoftWindows.Client.LKG_1000.226...	@{MicrosoftWindows.Client....	Domai...	Yes
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes
Spotify Music	{78E1CD88-49E3-476E-B926-...	All	Yes
Spotify Music	{78E1CD88-49E3-476E-B926-...	All	Yes
Spotify Music	{78E1CD88-49E3-476E-B926-...	All	Yes
Spotify Music	{78E1CD88-49E3-476E-B926-...	All	Yes
Spotify Music	{78E1CD88-49E3-476E-B926-...	All	Yes
Spotify Music	{78E1CD88-49E3-476E-B926-...	All	Yes
Spotify Music	{78E1CD88-49E3-476E-B926-...	All	Yes
Spotify Music	{78E1CD88-49E3-476E-B926-...	All	Yes
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes
App Installer	App Installer	Domai...	Yes

Conclusion:

In today's world, practicing network security in every endeavor is paramount as it helps one to safeguard their private data from being misused by malicious individuals. Appropriately, it is possible to mitigate and even erase chances of unauthorized access to information or impersonation by using rudimentary solutions such as strong authentication, firewalls, and locked networks especially known as WPA3 for Wi-Fi connection. Hence, encouraging others to adopt such practices increases the rates of internet security. Of utmost importance is the need to be active and offensive at all times, as there will always be threats in the domain, that aim to violate the privacy of individual, utopian cyberspace interactions. Tsiatsos, Vasilakos, & Symeonidis (2017) underscore that, network security is not the concern only of IT managers but rather everyone in the modern society should have basic knowledge of it. To this end, cybercriminals have been known to utilize various strategies ranging from fake websites to spear phishing and online harassment to compromise a person or service for the purpose of gaining unauthorized access or even overthrowing it. Good habits of network security such as updating programs, using hard to guess passwords, and keeping away from link which looks fishy helps in the protection of both work and personal information. Safeguarding the network comprises of implementing such protective security measures as

placing a firewall and encryption so that the information traversing the network is kept safe. Education and awareness are also significant in combating these cyber dangers thereby contributing to a safer experience for all web users.