Cyber Competition

Blue Team Report

By

Kranthi Kumar Manda

The University of Tampa

About Competition:

In CYB 660 – Penetration Testing course, we had a cyber competition where two teams participated. Red teamers attempted to attack the Windows server, while blue teamers like me defended using various techniques. Although this competition favored the red teamers, given the nature of the Penetration Testing course, I applied my best efforts to safeguard assigned host and server throughout this competition.

Introduction:

As a blue team, our primary goal is to defend our systems. To achieve this, we dedicated our efforts to securing them comprehensively. Understanding that effective security requires identifying vulnerabilities, we initiated a process of attacking our systems to gain insights into the overall security posture. During this exploration, we discovered several potential points of exploitation and vulnerabilities that could be exploited by malicious actors. These vulnerabilities were like fruits ready for hackers to pluck. In response, we took proactive measures to enhance our system's security. Our security measures included actions such as removing unnecessary users, closing unused ports, and updating outdated services and software. Through these deliberate steps, we successfully minimized the attack surface, making it more challenging for potential threats to compromise our systems.

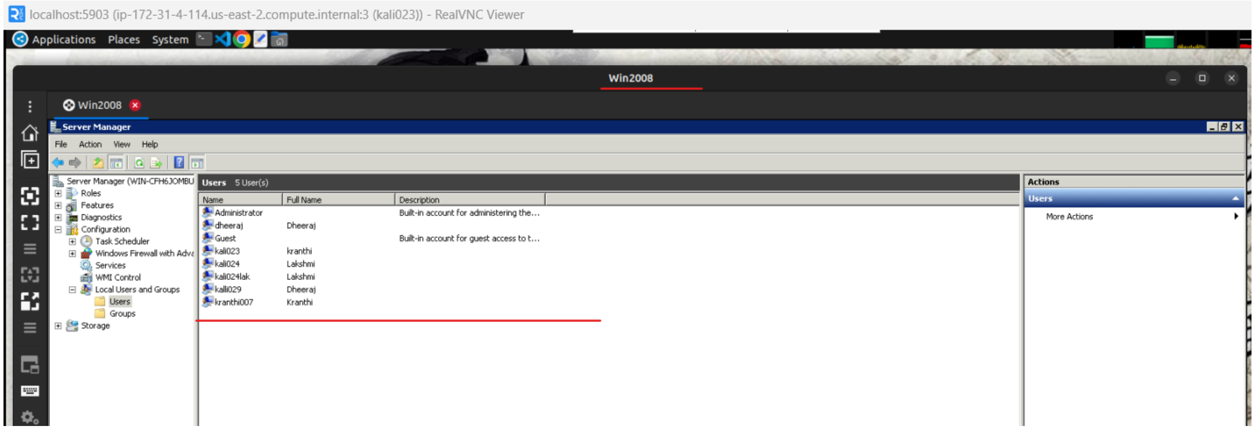
Planning:

Our plan involved collecting information, such as the number of users and their access levels. We aimed to identify potential risks specific to Windows 2008. We also planned to stop or disable unnecessary services, prioritizing based on the level of risk. Additionally, we planned to conduct patch management to address vulnerabilities. Lastly, we intended to thoroughly analyze and monitor the system logs using Suricata IDS.

Cyber Defense Work:

As a blue team (Group3), we initiated the process of securing the Windows 2008 machine by implementing various known methods. Initially, we accessed the system using the default credentials 'vagrant: vagrant'. Subsequently, we created new admin user accounts for our team's use and promptly removed any unnecessary user accounts.

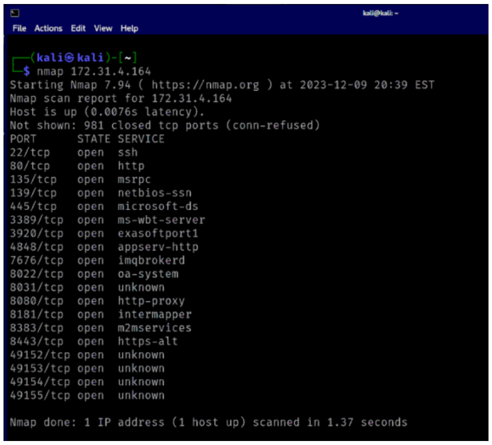
Additionally, we enhanced security by updating the passwords for the 'Administrator' and 'Guest' users with strong 12-character long passwords.



Users 5 User(s)

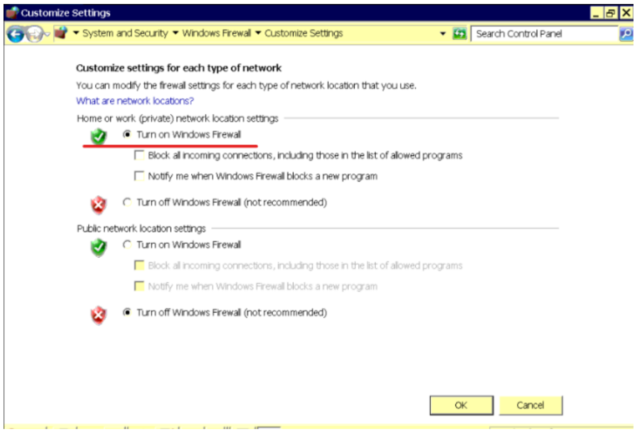
Name	Full Name	Description
Administrator		Built-in account for administering the...
dheeraj	Dheeraj	
Guest		Built-in account for guest access to t...
kali023	kranthi	
kali024	Lakshmi	
kali024lak	Lakshmi	
kalli029	Dheeraj	
kranthi007	Kranthi	

To identify the open ports on the host IP, we conducted an Nmap scan. The results revealed several open ports with associated running services.



```
┌──(kali㉿kali)-[~]
└─$ nmap 172.31.4.164
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 20:39 EST
Nmap scan report for 172.31.4.164
Host is up (0.0076s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3920/tcp  open  exasoftport1
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
```



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

□ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Public network location settings

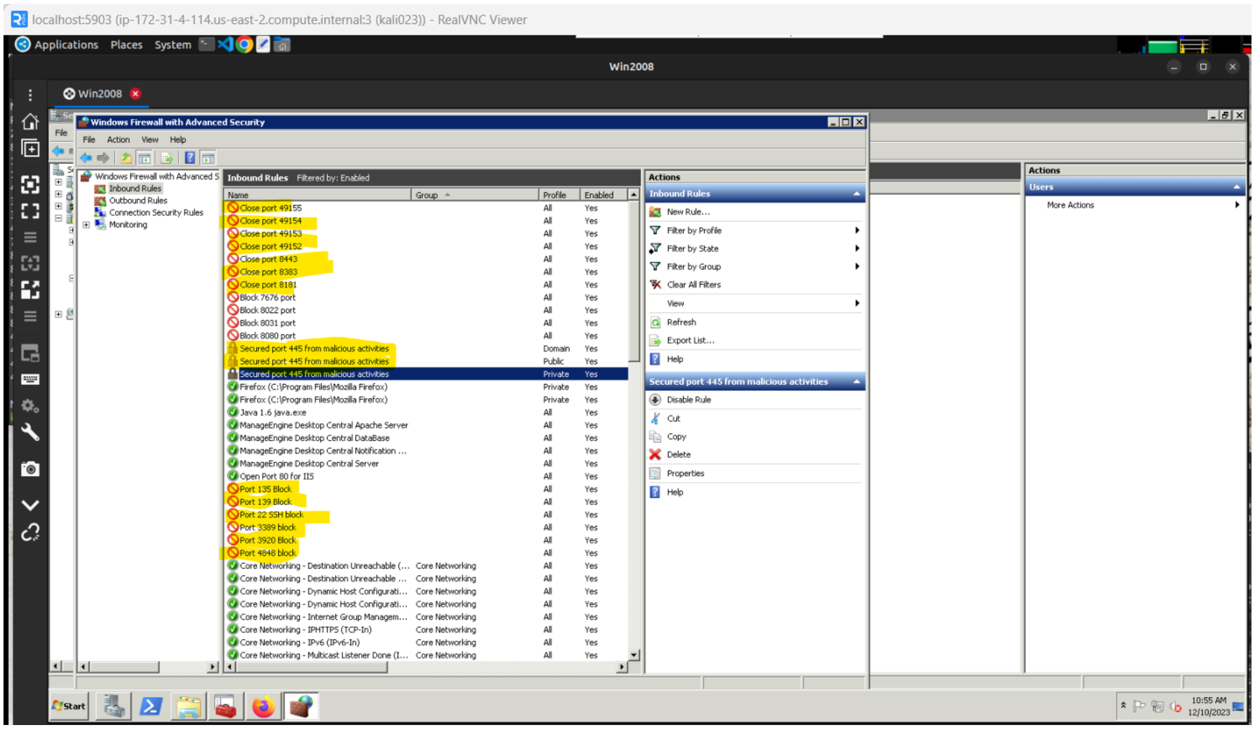
○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

□ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

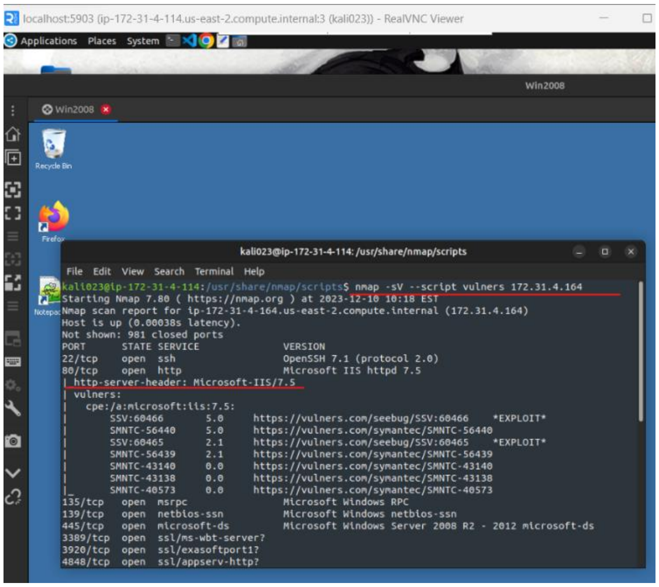
Notably, we observed that the firewall was initially turned off. Taking action on it, we activated the firewall and proceeded to configure inbound rules. In this step, we created rules to close all unnecessary ports, while ensuring that ports 80, 443, and 445 remained open as instructed.



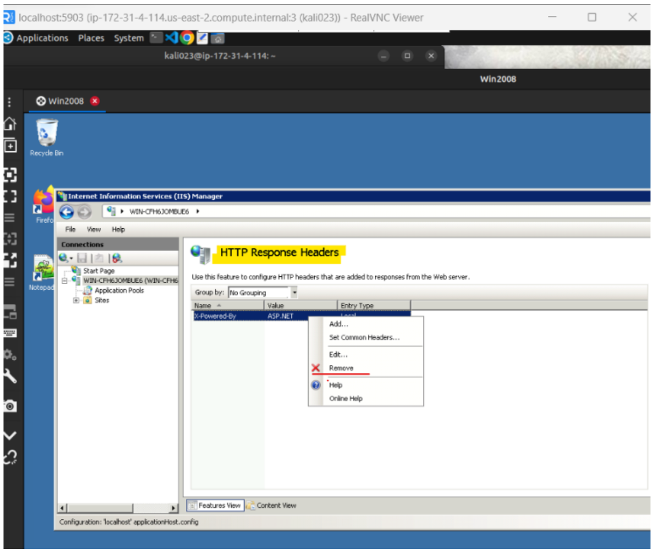
Inbound Rules Filtered by: Enabled

Name	Group	Profile	Enabled
Close port 49155		All	Yes
Close port 49154		All	Yes
Close port 49153		All	Yes
Close port 49152		All	Yes
Close port 8443		All	Yes
Close port 8383		All	Yes
Close port 8181		All	Yes
Block 7676 port		All	Yes
Block 8022 port		All	Yes
Block 8031 port		All	Yes
Block 8080 port		All	Yes
Secured port 445 from malicious activities		Domain	Yes
Secured port 445 from malicious activities		Public	Yes
Secured port 445 from malicious activities		Private	Yes
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes
Java 1.6 java.exe		All	Yes
ManageEngine Desktop Central Apache Server		All	Yes
ManageEngine Desktop Central DataBase		All	Yes
ManageEngine Desktop Central Notification ...		All	Yes
ManageEngine Desktop Central Server		All	Yes
Open Port 80 for IIS		All	Yes
Port 135 Block		All	Yes
Port 139 Block		All	Yes
Port 22 SSH block		All	Yes
Port 3389 block		All	Yes
Port 3920 Block		All	Yes
Port 4848 block		All	Yes
Core Networking - Destination Unreachable (...	Core Networking	All	Yes
Core Networking - Destination Unreachable ...	Core Networking	All	Yes
Core Networking - Dynamic Host Configurati...	Core Networking	All	Yes
Core Networking - Dynamic Host Configurati...	Core Networking	All	Yes
Core Networking - Internet Group Managem...	Core Networking	All	Yes
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Done (I...	Core Networking	All	Yes

We conducted an Nmap scan using Vulners scripts, focusing on identifying vulnerabilities. We discovered that on port 80, the HTTP service is running with the version Microsoft IIS httpd 7.5, which is vulnerable. To mitigate this, we removed the HTTP server header. While this action won't cause any issues, it prevents attackers from seeing the service version and header.


localhost:5903 (ip-172-31-4-114.us-east-2.compute.internal:3 (kali023)) - RealVNC Viewer
Applications Places System
Win2008
Recycle Bin
Firefox
Notepad
kali023@ip-172-31-4-114: /usr/share/nmap/scripts
File Edit View Search Terminal Help

```
kali023@ip-172-31-4-114:/usr/share/nmap/scripts$ nmap -sV --script vulners 172.31.4.164
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-10 10:18 EST
Nmap scan report for ip-172-31-4-164.us-east-2.compute.internal (172.31.4.164)
Host is up (0.00038s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE            VERSION
22/tcp    open  ssh                OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http               Microsoft IIS httpd 7.5
| http-server-header: Microsoft-IIS/7.5
| vulners:
|   cpe:/a:microsoft:iis:7.5:
|       SSV:60466     5.0    https://vulners.com/seebug/SSV:60466    *EXPLOIT*
|       SMNTC-56440   5.0    https://vulners.com/symantec/SMNTC-56440
|       SSV:60465     2.1    https://vulners.com/seebug/SSV:60465    *EXPLOIT*
|       SMNTC-56439   2.1    https://vulners.com/symantec/SMNTC-56439
|       SMNTC-43140   0.0    https://vulners.com/symantec/SMNTC-43140
|       SMNTC-43138   0.0    https://vulners.com/symantec/SMNTC-43138
|_      SMNTC-40573   0.0    https://vulners.com/symantec/SMNTC-40573
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
3920/tcp  open  ssl/exasoftport1?
4848/tcp  open  ssl/appserv-http?
```


localhost:5903 (ip-172-31-4-114.us-east-2.compute.internal:3 (kali023)) - RealVNC Viewer
Applications Places System
kali023@ip-172-31-4-114: ~
Win2008
Recycle Bin
Internet Information Services (IIS) Manager
WIN-CFH6JOMBUE6
File View Help
Connections
Start Page
WIN-CFH6JOMBUE6 (WIN-CFH6
Application Pools
Sites
HTTP Response Headers
Add...
Set Common Headers...
Edit...
Remove
Help
Online Help
Features View
Content View

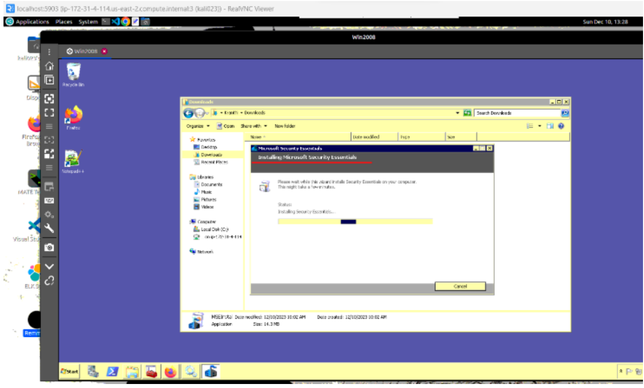
Use this feature to configure HTTP headers that are added to responses from the Web server.

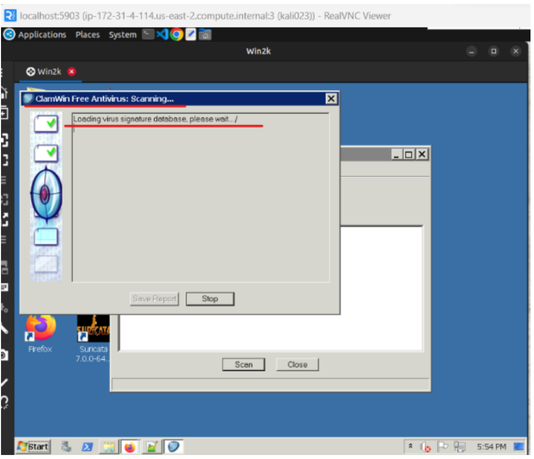
Group by: No Grouping

Name	Value	Entry Type
X-Powered-By	ASP.NET	Local

Configuration: 'localhost' applicationHost.config

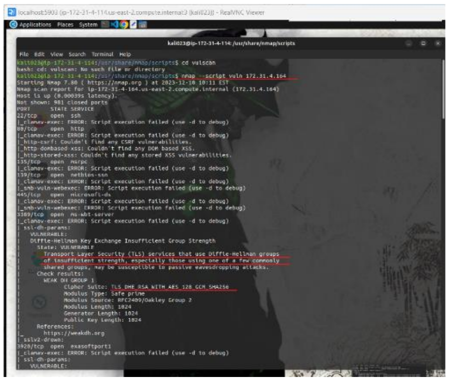
We also installed Microsoft Security Essentials and 'Calmwin' anti-virus software to mitigate the risk of web application vulnerabilities, such as brute force and common injection attacks.


localhost:5903 (ip-172-31-4-114.us-east-2.compute.internal:3 (kali023)) - RealVNC Viewer
Win2008
Microsoft Security Essentials
Installing Microsoft Security Essentials
Cancel


localhost:5903 (ip-172-31-4-114.us-east-2.compute.internal:3 (kali023)) - RealVNC Viewer
Applications Places System
Win2k
ClamWin Free Antivirus: Scanning...
Save Report
Stop
Scan
Close
Firefox
Suricata 7.0.0-64...
Start
5:54 PM

Loading virus signature database, please wait... /

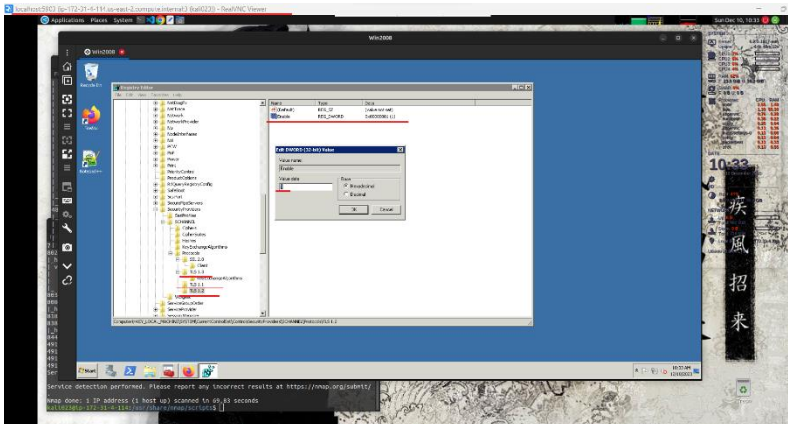
Additionally, we identified a vulnerability in TLS certificate 1.0 and promptly updated it to the latest version, TLS 1.3. We added the updated certificates to the protocols in the Windows Registry Editor. We identified a vulnerability in the Apache Tomcat server on port 443 due to its outdated version. Addressing this issue became a priority, and we successfully updated the Apache Tomcat server to enhance its security.



localhost:5903 (ip-172-31-4-114.us-east-2.compute.internal:3 (kali023)) - RealVNC Viewer

kali023@ip-172-31-4-114: /usr/share/nmap/scripts

```
kali023@ip-172-31-4-114:/usr/share/nmap/scripts$ cd vulscan
bash: cd: vulscan: No such file or directory
kali023@ip-172-31-4-114:/usr/share/nmap/scripts$ nmap --script vuln 172.31.4.164
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-10 10:11 EST
Nmap scan report for ip-172-31-4-164.us-east-2.compute.internal (172.31.4.164)
Host is up (0.00039s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-webexec: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-webexec: ERROR: Script execution failed (use -d to debug)
3389/tcp  open  ms-wbt-server
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 1024
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| sslv2-drown:
3920/tcp  open  exasoftport1
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
```



localhost:5903 (ip-172-31-4-114.us-east-2.compute.internal:3 (kali023)) - RealVNC Viewer

Win2008

Registry Editor

Name	Type	Data
(Default)	REG_SZ	(value not set)
Enable	REG_DWORD	0x00000001 (1)

Edit DWORD (32-bit) Value

Value name: Enable

Value data: 1

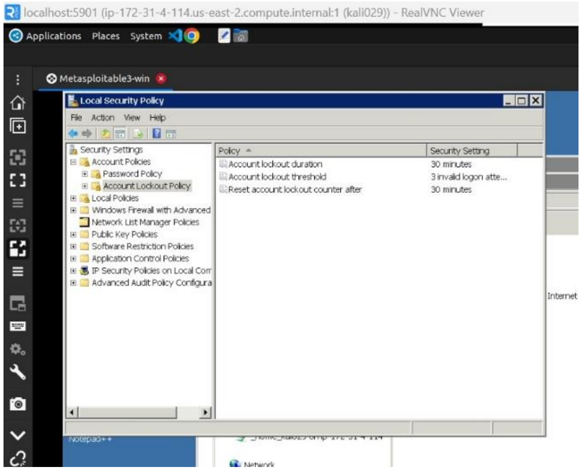
Base: ● Hexadecimal ○ Decimal

OK Cancel

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.83 seconds
kali023@ip-172-31-4-114:/usr/share/nmap/scripts$
```

Since Suricata IDS didn't function properly for our team, we opted to install Snort IDS on the Windows 2008 machine. We configured Snort rules to generate alerts for specific HTTP requests and to notify us of any port scans on the system. Additionally, we implemented an account lockout policy, essentially a rate-limiting measure, to decrease the number of failed login attempts.



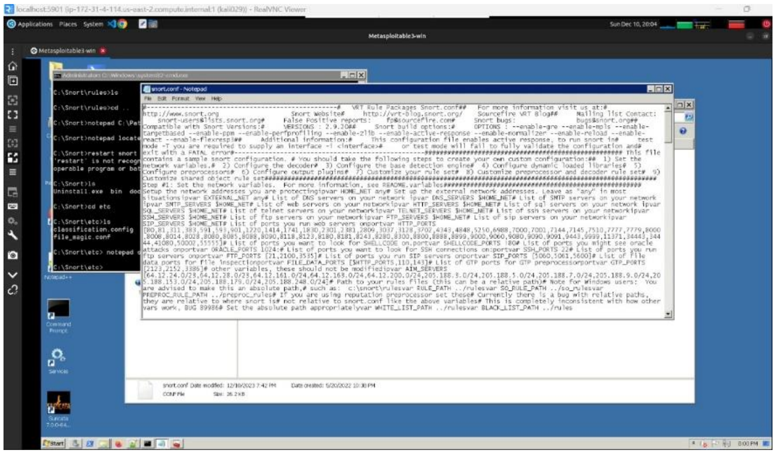
localhost:5901 (ip-172-31-4-114.us-east-2.compute.internal:1 (kali029)) - RealVNC Viewer

Metasploitable3-win

Local Security Policy

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon atte...
Reset account lockout counter after	30 minutes

Applications
Places
System
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Com
Advanced Audit Policy Configura
Internet
Notepad++
Network



localhost:5901 (ip-172-31-4-114.us-east-2.compute.internal:1 (kali029)) - RealVNC Viewer

Metasploitable3-win

Administrator: C:\Windows\system32\cmd.exe

```
C:\Snort\rules>ls

C:\Snort\rules>cd ..

C:\Snort>notepad C:\Pat

C:\Snort>notepad locate

C:\Snort>restart snort
'restart' is not recogn
operable program or bat

C:\Snort>ls
Uninstall.exe  bin  doc

C:\Snort>cd etc

C:\Snort\etc>ls
classification.config
file_magic.conf

C:\Snort\etc> notepad s

C:\Snort\etc>
```

snort.conf - Notepad

```
#--------------------------------------------------#   VRT Rule Packages Snort.conf##   For more information visit us at:#
http://www.snort.org                Snort Website#    http://vrt-blog.snort.org/   Sourcefire VRT Blog##     Mailing list Contact:
   snort-users@lists.snort.org#     False Positive reports:    fp@sourcefire.com#     Snort bugs:               bugs@snort.org##
Compatible with Snort Versions:#     VERSIONS : 2.9.20##     Snort build options:#     OPTIONS : --enable-gre --enable-mpls --enable-
targetbased --enable-ppm --enable-perfprofiling --enable-zlib --enable-active-response --enable-normalizer --enable-reload --enable-
react --enable-flexresp3##     Additional information:#     This configuration file enables active response, to run snort in#     test
mode -T you are required to supply an interface -i <interface>#     or test mode will fail to fully validate the configuration and#
exit with a FATAL error#-----------------------------------------------##################################################### This file
contains a sample snort configuration. # You should take the following steps to create your own custom configuration:##  1) Set the
network variables.#  2) Configure the decoder#  3) Configure the base detection engine#  4) Configure dynamic loaded libraries#  5)
Configure preprocessors#  6) Configure output plugins#  7) Customize your rule set#  8) Customize preprocessor and decoder rule set#  9)
Customize shared object rule set############################################################################################
Step #1: Set the network variables.  For more information, see README.variables##########################################
Setup the network addresses you are protectingipvar HOME_NET any# Set up the external network addresses. Leave as "any" in most
situationsipvar EXTERNAL_NET any# List of DNS servers on your network ipvar DNS_SERVERS $HOME_NET# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET# List of web servers on your networkipvar HTTP_SERVERS $HOME_NET# List of sql servers on your network ipvar
SQL_SERVERS $HOME_NET# List of telnet servers on your networkipvar TELNET_SERVERS $HOME_NET# List of ssh servers on your networkipvar
SSH_SERVERS $HOME_NET# List of ftp servers on your networkipvar FTP_SERVERS $HOME_NET# List of sip servers on your networkipvar
SIP_SERVERS $HOME_NET# List of ports you run web servers onportvar HTTP_PORTS
[80,81,311,383,591,593,901,1220,1414,1741,1830,2301,2381,2809,3037,3128,3702,4343,4848,5250,6988,7000,7001,7144,7145,7510,7777,7779,8000
,8008,8014,8028,8080,8085,8088,8090,8118,8123,8180,8181,8243,8280,8300,8800,8888,8899,9000,9060,9080,9090,9091,9443,9999,11371,34443,344
44,41080,50002,55555]# List of ports you want to look for SHELLCODE on.portvar SHELLCODE_PORTS !80# List of ports you might see oracle
attacks onportvar ORACLE_PORTS 1024:# List of ports you want to look for SSH connections on:portvar SSH_PORTS 22# List of ports you run
ftp servers onportvar FTP_PORTS [21,2100,3535]# List of ports you run SIP servers onportvar SIP_PORTS [5060,5061,5600]# List of file
data ports for file inspectionportvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]# List of GTP ports for GTP preprocessorportvar GTP_PORTS
[2123,2152,3386]# other variables, these should not be modifiedipvar AIM_SERVERS
[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,20
5.188.153.0/24,205.188.179.0/24,205.188.248.0/24]# 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\rulesvar RULE_PATH ../rulesvar SO_RULE_PATH ../so_rulesvar
PREPROC_RULE_PATH ../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# not relative to snort.conf like the above variables# This is completely inconsistent with how other
vars work, BUG 89986# Set the absolute path appropriatelyvar WHITE_LIST_PATH ../rulesvar BLACK_LIST_PATH ../rules
```

snort.conf Date modified: 12/10/2023 7:42 PM   Date created: 5/20/2022 10:38 PM
CONF File   Size: 26.2 KB

Lessons learned:

Working together as a team proved to be essential in the cybersecurity world. We learned the importance of effective communication and coordination. The practical application of security measures, such as installing antivirus software, activating firewalls, and implementing countermeasures, provided us with real-world experience in Strengthening a system against potential cyber threats. Through our defending process, we learned to identify and understand various attack surfaces within our system. This knowledge was crucial in developing effective defensive strategies to minimize vulnerabilities. Also, defending against common cyberattacks like SSH brute force, command line injection, and web application attacks allowed us to put theoretical knowledge into practice. We realized the importance of continuous monitoring and adaptation in the ever-evolving landscape of cybersecurity. By utilizing tools like Suricata.

Challenges faced:

Initially, we struggled with lack of knowledge about blue teaming, especially when it came to understanding Windows Server. Installing different software and a vulnerability scanner proved to be quite challenging. Additionally, after closing unnecessary ports using firewall inbound rules, they didn't function properly for a long period. Configuring Suricata posed a significant challenge for our team, despite numerous attempts and online tutorials, the application kept crashing. Consequently, we faced difficulties in monitoring and analyzing logs, that stopped our ability to effectively track and respond to potential threats from the attacking team.