SRI RAMAKRISHNA ENGINEERING COLLEGE

[Educational Service : SNR Sons Charitable Trust]
[Autonomous Institution, Reaccredited by NAAC with 'A+' Grade]
[Approved by AICTE and Permanently Affiliated to Anna University, Chennai]
[ISO 9001:2015 Certified and all eligible programmes Accredited by NBA]
VATTAMALAIPALAYAM, N.G.G.O. COLONY POST, COIMBATORE- 641 022.

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

Class: III B.Tech AI&DS **Semester: V**

Certified that this is the bonafide record of work done by ____________________ in the **20AD252 – AI FOR CYBER SECURITY** of this institution for V semester during the academic year 2023-2024

Faculty In-Charge Head of the Department

Roll No.

Submitted for the V Semester B.Tech. Practical Examination on _____________

INTERNAL EXAMINER **SUBJECT EXPERT**

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATASCIENCE

VISION AND MISSION

VISION

To achieve academic excellence in the domain of Artificial Intelligence and Data Scienceand produce globally competent professionals to solve futuristic societal challenges **MISSION**

- To actively engage in implementation of innovative intelligent solutions for inter disciplinary Artificial Intelligence based solutions with ethical standards
- To promote research, innovation and entrepreneurial skills through industry andacademic collaboration

PROGRAM EDUCATIONAL OBJECTIVES (PEOS)

The graduates of this program after four to five years will,

PEO 1: Design and develop solutions for real world problems based on business and societal needs, as skilled professionals or entrepreneurs.

PEO 2: Apply Artificial Intelligence and Data Science knowledge and skills to develop innovative solutions for multi-disciplinary problems, adhering to ethical standards

PEO 3: Engage in constructive research, professional development and life-long learning to adapt with emerging technologies

Program Outcomes and Program Specific Outcomes (POs and PSOs)

Program Outcomes as stated by NBA: Engineering Graduates will be able to

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions**: Design solutions for complex engineering problems and designsystem components or processes that meet the specified needs with appropriate consideration for thepublic health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems:** Use research–based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineeringand IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one’s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life–long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life–long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES:

Graduates of Artificial Intelligence and Data Science at the time of graduation will be able to

PSO 1: Analyze, design and build sustainable intelligent solutions to solve challenges imposed by industryand society.

PSO2: Demonstrate data analysis skills to achieve effective insights and decision making to solve real lifeproblems.

PSO3: Apply mathematical and statistical models to solve computational task, model real world problemsusing appropriate AI / ML algorithms.

INDEX

EX.NO: 1	**BASIC INSTALLATION OF LINUX DISTRIBUTION VM’S**
DATE:	

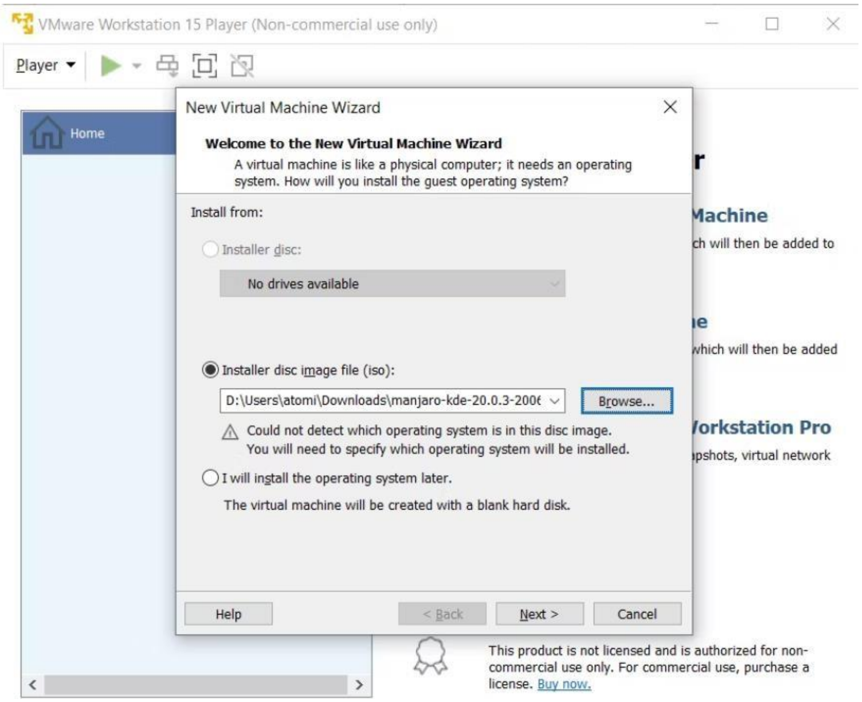
AIM:

To create a virtual machine and install a Linux distribution.

PROCEDURE:

1. Create a new virtual machine and enter a name and set the type to linux and set version as Debian 64bytes.
2. Allocate memory for your virtual machine and create a virtual hard disk.
3. Select the virtual price filetype such as virtual disk image of your preferred OS.
4. Select the physical hard drive allocation type as dynamic and static, and allocate the disk size.
5. Enable the shared clipboard and drag ‘n’ drop feature as bidirectional which will allow us to copy paste files from test machine on the file.
6. Update your virtual motherboard options and select the number of processors and enable PAE/NX and allocate the idea memory and 3D acceleration.
7. Now load the download ISO file here for sample parrot security ISO file is loaded, load the ISO file in the controller IDE option in storage.
8. Select the network connection type and enable USB 2.0 and 3.0 controllers, boot the parrot security ISO and install it using the default installer calamares.
9. Select the language, location, keyboard, layout and partition the parrot security disk create a new user account and install the parrot OS by making changes to your disk.

OUTPUT:



New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

● Installer disc image file (iso):

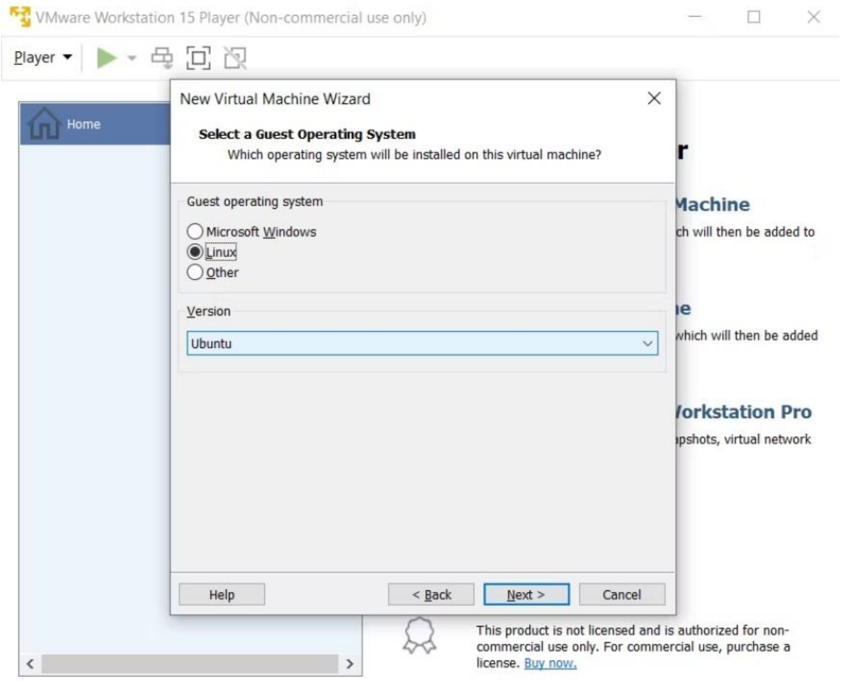
D:\Users\atomi\Downloads\manjaro-kde-20.0.3-200€

Could not detect which operating system is in this disc image. You will need to specify which operating system will be installed.

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.



New Virtual Machine Wizard

Select a Guest Operating System

Which operating system will be installed on this virtual machine?

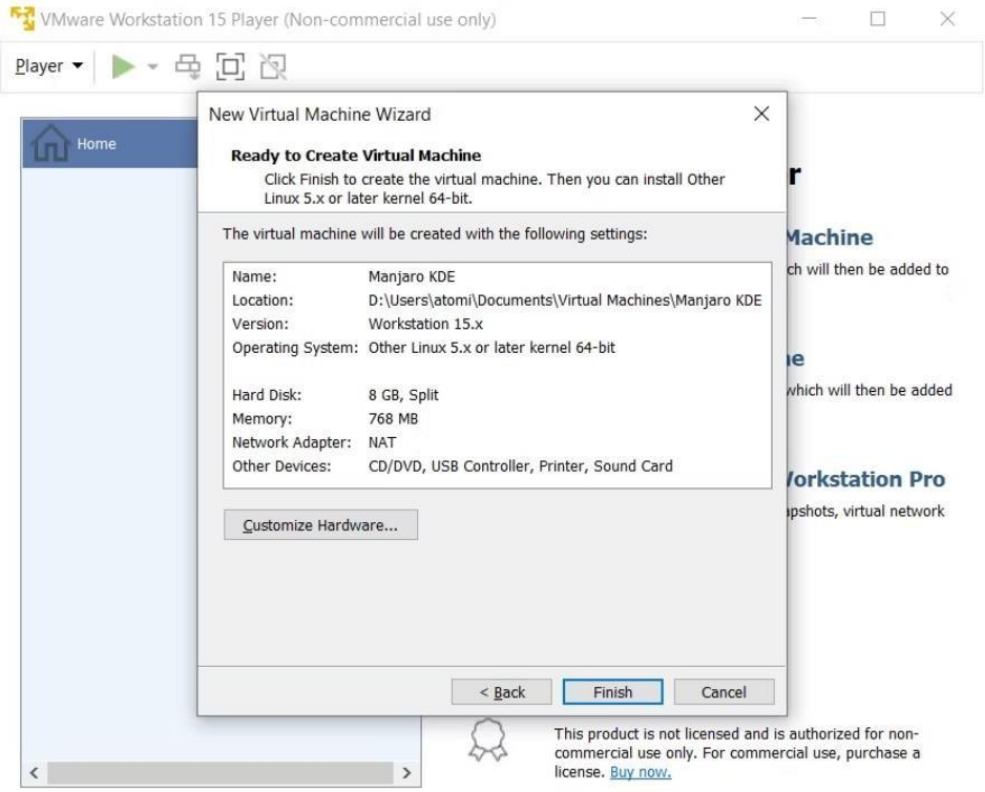
Guest operating system

○ Microsoft Windows
● Linux
○ Other

Version

Ubuntu

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.



VMware Workstation 15 Player (Non-commercial use only)
Player
Home
New Virtual Machine Wizard
Customize Hardware...
< Back
Finish
Cancel
r
Machine
ch will then be added to
ie
which will then be added
Vorkstation Pro
ipshots, virtual network
This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Other Linux 5.x or later kernel 64-bit.

The virtual machine will be created with the following settings:

```
Name:              Manjaro KDE
Location:          D:\Users\atomi\Documents\Virtual Machines\Manjaro KDE
Version:           Workstation 15.x
Operating System:  Other Linux 5.x or later kernel 64-bit

Hard Disk:         8 GB, Split
Memory:            768 MB
Network Adapter:   NAT
Other Devices:     CD/DVD, USB Controller, Printer, Sound Card
```

RESULT:

Thus, a basic Linux distribution was installed in the virtual box successfully.

EX.NO: 2	**EXPLORE THE VULNERABILITIES IN LAN ENVIRONMENT.**
DATE:	

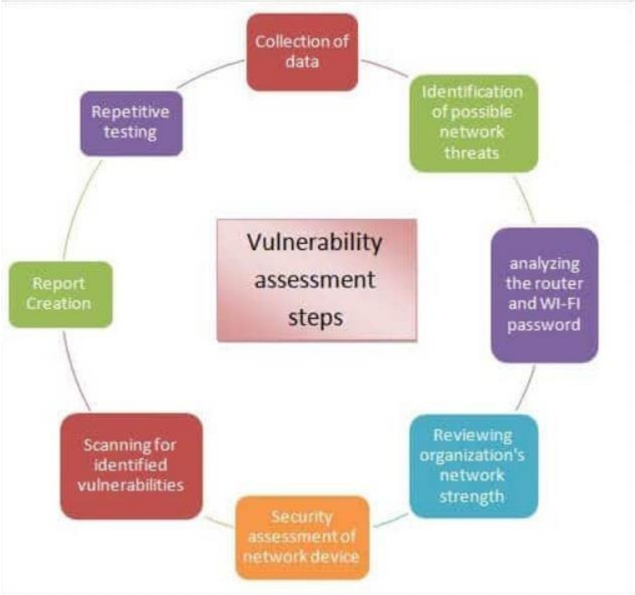
AIM:

To explore the vulnerabilities in LAN environment.

PROCEDURE:

Types Of Vulnerability:

- Hardware Vulnerability– It refers to the flaws that arise due to hardware issues like excessive humidity, dust and unprotected storage of the hardware.
- Software Vulnerability– The flaw in the design technique of the project, inappropriate testing and lack of timely audit of assets, lead to the software vulnerability.
- Network Vulnerability: Due to the use of open network connections, un protected network architecture and weak communication channel this type of issues arise.
- Physical Vulnerability: If the system is located in an area which is subject to heavy rain, flood or unstable power supply, etc. then it is prone to physical vulnerability.
- Organization Vulnerability: This vulnerability arises due to the use of inappropriate security tools, audit rules and flaws in administrative actions


Vulnerability assessment steps
Collection of data
Identification of possible network threats
analyzing the router and WI-FI password
Reviewing organization's network strength
Security assessment of network device
Scanning for identified vulnerabilities
Report Creation
Repetitive testing

Causes of Vulnerabilities:

- The complex and huge structure of the networks will be a possible cause of flawsin the architecture which will lead to vulnerability.
- Deploying the similar kind of hardware, network design, software tools, the coding system, etc. will increase the chances for the hacker to easily crack the code of the system and the system will become prone to exploitation.
- Systems which are more dependent on physical network connections and port connectivity are having more probability of vulnerability.
- The networking systems and PC's which are using weak passwords for security purpose will be easily exploited by the attacker.
- The operating systems which easily give access to any of the software program and each of the user who wants to access it get hacked easily by the attacker and they can make changes in the program for their benefits.
- Many of the websites on the Internet, when we are browsing them contain harmful malware and other viruses which can be installed on our system by them when wevisit them. Thus, the system will get infected by those viruses and any information can be leaked from the computer by those viruses.
- An exploitable software bug in the software program will lead to a software vulnerability.

RESULT:

Thus, the basic vulnerabilities in LAN environment have been explored.

EX.NO: 3	ANALYZE NETWORK PACKETS IN WIRESHARK
DATE:	

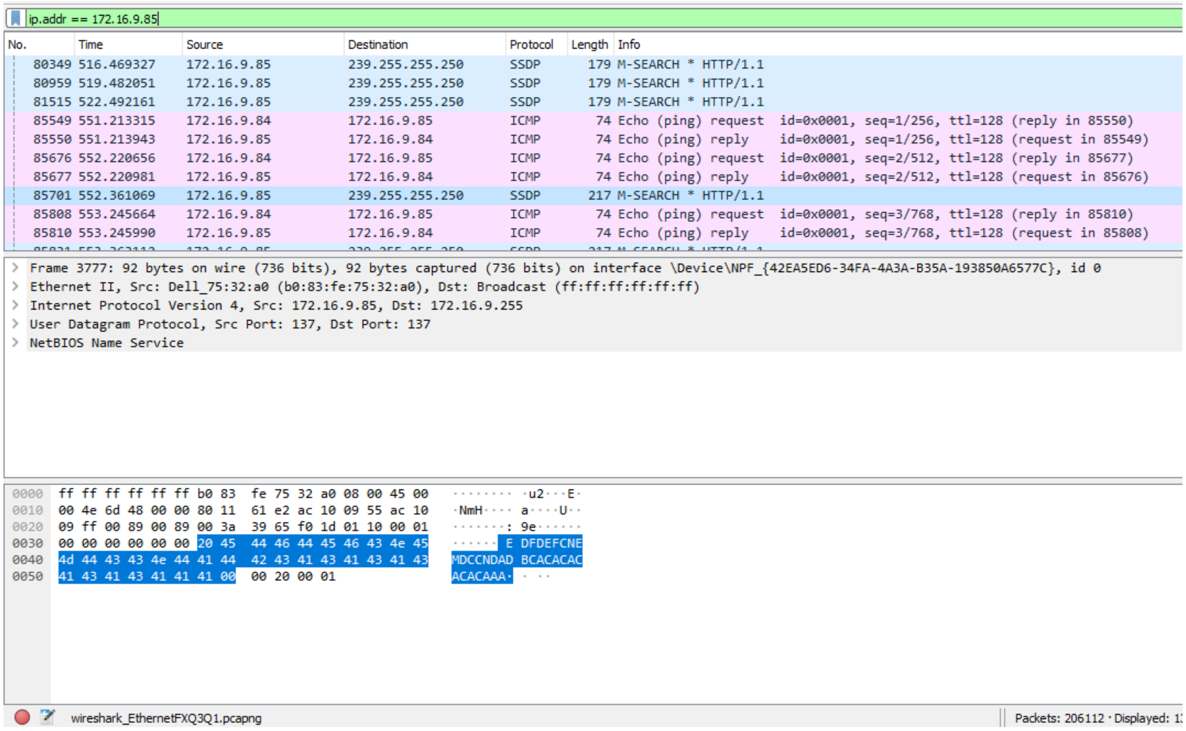
AIM:

To analyze the network packets in Wireshark.

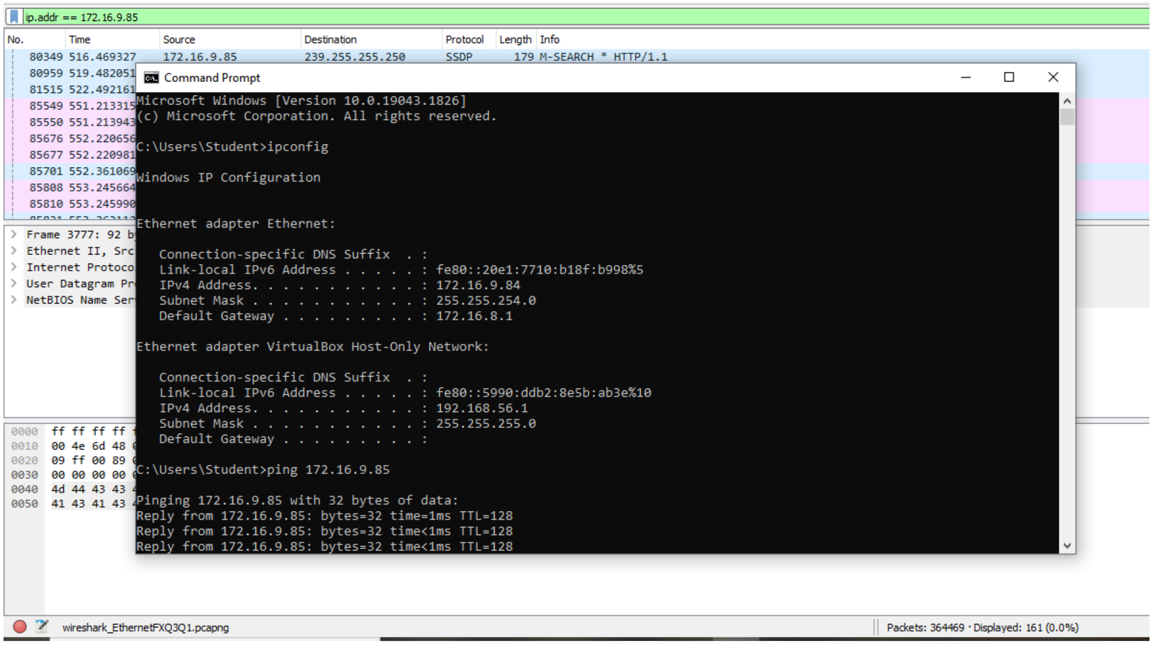
PROCEDURE:

- Whenever we want to do an analysis of any data packet the first step is to capture the packet which is coming and outgoing then we use packet analyzer tool.
- Download and install Wireshark on our machine as per our operating system.
- We need to start the Wireshark with administrative permission it will show the window, where we need to select the appropriate interface through which we want to capture the packets.
- Once we select the interface then Wireshark starts capturing packets and showing the list of packets and live to capture packet window Wireshark will keep capturing live packets we stop capturing.
- If we want to continue the will capturing then we can keep capturing the packet and if we want to stop capturing then we can click on stop capturing, packer menu in toolbar.
- We can see the various columns in the Wireshark window. i.e., no time, source, destination and protocol, etc., now we can select the appropriate packet which we want to analyze.
- As per the various packet formats we can select and analyses that how the packets are being transferred over the internet.
- When we analyze the packet, we can see which protocol is used at various layer. The size of actual message and size of header. We can also identify the various segment of the original message because large messages reach to destination from source in the form of segments.

OUTPUT:



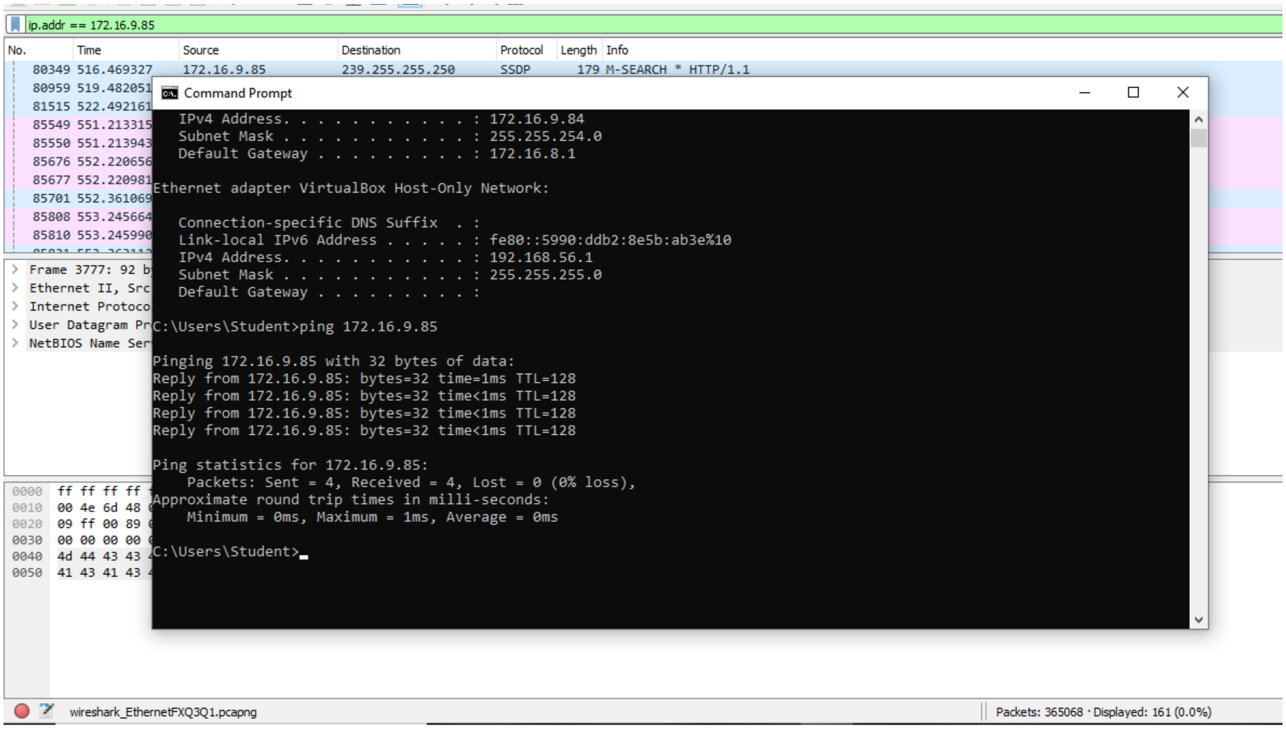
```
ip.addr == 172.16.9.85

No.    Time        Source        Destination      Protocol Length Info
 80349 516.469327  172.16.9.85   239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
 80959 519.482051  172.16.9.85   239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
 81515 522.492161  172.16.9.85   239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
 85549 551.213315  172.16.9.84   172.16.9.85      ICMP       74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 85550)
 85550 551.213943  172.16.9.85   172.16.9.84      ICMP       74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=128 (request in 85549)
 85676 552.220656  172.16.9.84   172.16.9.85      ICMP       74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 85677)
 85677 552.220981  172.16.9.85   172.16.9.84      ICMP       74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=128 (request in 85676)
 85701 552.361069  172.16.9.85   239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
 85808 553.245664  172.16.9.84   172.16.9.85      ICMP       74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 85810)
 85810 553.245990  172.16.9.85   172.16.9.84      ICMP       74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=128 (request in 85808)

> Frame 3777: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{42EA5ED6-34FA-4A3A-B35A-193850A6577C}, id 0
> Ethernet II, Src: Dell_75:32:a0 (b0:83:fe:75:32:a0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.16.9.85, Dst: 172.16.9.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service

0000  ff ff ff ff ff ff b0 83  fe 75 32 a0 08 00 45 00   ········ ·u2···E·
0010  00 4e 6d 48 00 00 80 11  61 e2 ac 10 09 55 ac 10   ·NmH···· a····U··
0020  09 ff 00 89 00 89 00 3a  39 65 f0 1d 01 10 00 01   ·······: 9e······
0030  00 00 00 00 00 00 20 45  44 46 44 45 46 43 4e 45   ······ E DFDEFCNE
0040  4d 44 43 43 4e 44 41 44  42 43 41 43 41 43 41 43   MDCCNDAD BCACACAC
0050  41 43 41 43 41 41 41 00  00 20 00 01               ACACAAA· · ··

wireshark_EthernetFXQ3Q1.pcapng                          Packets: 206112 · Displayed: 1
```



```
ip.addr == 172.16.9.85

No.    Time        Source        Destination      Protocol Length Info
 80349 516.469327  172.16.9.85   239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
```

```
Command Prompt

Microsoft Windows [Version 10.0.19043.1826]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Student>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::20e1:7710:b18f:b998%5
   IPv4 Address. . . . . . . . . . . : 172.16.9.84
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 172.16.8.1

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5990:ddb2:8e5b:ab3e%10
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\Student>ping 172.16.9.85

Pinging 172.16.9.85 with 32 bytes of data:
Reply from 172.16.9.85: bytes=32 time=1ms TTL=128
Reply from 172.16.9.85: bytes=32 time<1ms TTL=128
Reply from 172.16.9.85: bytes=32 time<1ms TTL=128
```

```
wireshark_EthernetFXQ3Q1.pcapng                          Packets: 364469 · Displayed: 161 (0.0%)
```



```
ip.addr == 172.16.9.85

No.    Time        Source         Destination       Protocol  Length Info
 80349 516.469327  172.16.9.85    239.255.255.250   SSDP         179 M-SEARCH * HTTP/1.1
 80959 519.482051
 81515 522.492161
 85549 551.213315
 85550 551.213943
 85676 552.220656
 85677 552.220981
 85701 552.361069
 85808 553.245664
 85810 553.245990

> Frame 3777: 92 by
> Ethernet II, Src
> Internet Protoco
> User Datagram Pr
> NetBIOS Name Ser

0000  ff ff ff ff
0010  00 4e 6d 48
0020  09 ff 00 89
0030  00 00 00 00
0040  4d 44 43 43
0050  41 43 41 43

wireshark_EthernetFXQ3Q1.pcapng          Packets: 365068 · Displayed: 161 (0.0%)
```

Command Prompt

```
   IPv4 Address. . . . . . . . . . . : 172.16.9.84
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 172.16.8.1

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5990:ddb2:8e5b:ab3e%10
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\Student>ping 172.16.9.85

Pinging 172.16.9.85 with 32 bytes of data:
Reply from 172.16.9.85: bytes=32 time=1ms TTL=128
Reply from 172.16.9.85: bytes=32 time<1ms TTL=128
Reply from 172.16.9.85: bytes=32 time<1ms TTL=128
Reply from 172.16.9.85: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.9.85:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Student>
```

RESULT:

Thus, the network packets are captured and analyzed successfully using the analyzer tool Wireshark.

EX.NO: 4	**EXPLORE OSINT TOOLS**
DATE:	

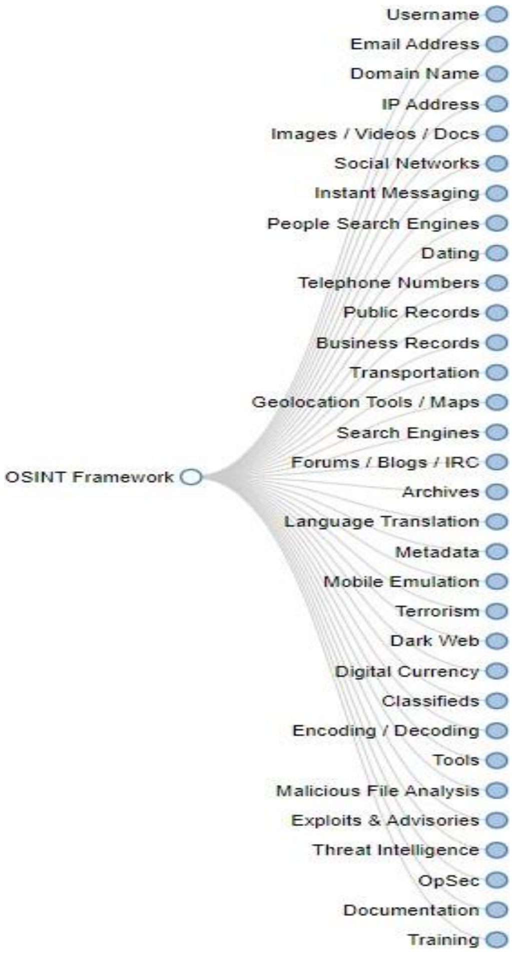
AIM:

To explore OSINT (Open-Source Intelligence Tool) tools.

WHAT ARE OSINT TOOLS?

Open-Source Intelligence software, abbreviated as OSINT software, is a tool that allows the collection of information that is publicly available or open-source. The goal of OSINT software is mainly to learn more about someone or a business.

OSINT FRAMEWORK:



TOOLS:

1) MALTEGO – INVESTIGATIONS VIA JAVA GRAPHS

Maltego is a Java application that claims to simplify and expedite your investigations. Howexactly? Thanks to its fantastic access to databases and visualization tools. Whether you're in trust and safety, law enforcement, or cybersecurity, the company lets you runone-click investigations that deliver easy-to-understand results.

At the time of writing, Maltego lets you view up to 1 million entities on a graph, with access to 58data sources. You can even connect your own public databases and upload data sources manually.

Once all the information is loaded in the program, you can choose from different visualizationlayouts, such as blocks, hierarchical, or circular, using weights and notes to adjust the graphs.

Finally, Maltego isn't just a great tool; the company also has a fantastic collection of hand-pickedresources on OSINT tools and techniques to help you get even more from their product. In fact, there is even a Maltego foundations course you can purchase online.

Maltego pricing:

- Maltego offers online courses which vary in price. There is a free personal plan for limited searches, but the pro version of the software costs around $1000 per year.

Maltego pros:

- Great graph visualization tools
- Multiple data viz options

Maltego cons:

- Java application only
- Dated UI

2) SEON – BEST FOR SOCIAL AND DIGITAL SIGNAL CHECKS

Confirming someone's identity by checking for linked social media and online platform accounts isbecoming increasingly popular for a number of good reasons:

- It's a high barrier of entry for fraudsters, who don't have the time or resources to create fake profiles.
- It's a fantastic way to gather a user's digital footprint.
- It can help establish an idea of someone's socioeconomic background, even in markets where financial information is scarce.
- The type of social media linked to the user can also reveal more about who they are.

Of course, you can manually search directly into your target network, by typing a name into LinkedIn, Facebook, or Twitter. For scalability reasons, however, it's easier to use a specialist solution. This is where SEON shines.

SEON is the only fraud prevention tool that checks more than 50 social and online signals. Thesechecks are based on an email address, IP address or phone number.

Because they're part of our email and phone data enrichment modules, you'll get a lot more information, including a risk score. The other good news is that you do get complete flexibility inhow you query the service: manually, via API, or through a Google Chrome extension.

SEON pricing:

- Starts at $299 per month – book a live product demo or self-onboard for a free 14-day trial to see how we can help your business.

SEON pros:

- Gather social media information
- Scalable thanks to API calls
- Real-time results
- Enrich data based on an email address, phone number or IP address
- Additional velocity checks, behavior checks, device fingerprinting

SEON cons:

- Not free. While there is a free trial, you have to pay a subscription to access the APIs.

3) LAMPYRE – DUE DILIGENCE AND CYBERTHREAT INTELLIGENCE

Lampyre is a paid application designed specifically for OSINT. It's particularly useful for due diligence, cyber threat intelligence, crime analysis, and financial analytics. You can install it onyour PC or run it online.

The key selling point of Lampyre is that it's a one-click application. Start with single data points such as a company registration number, full name, or phone number, and Lampyre will sift throughhuge amounts of data to extract interesting information.

The company automatically processes 100+ regularly updated data sources, and you can access them via PC software or API calls if needed. The SaaS product is called Lighthouse, and you payper API call.
An important point here: As with many OSINT tools, you have to perform your due diligence tocheck if the databases are really open source. Lampyre may automate searches, but you may stillhave to double-check where the information comes from, as well as who exactly it is that is sourcing it for you, as one researcher found out.

Lampyre pricing:

- Lampyre is affordable. You can try a one-monthdemo license, which then turns into a standard subscription. You can also purchase a $300 yearly version. SaaS pricing is viathe Lighthouse subscription, priced $3.25-$130 per month, depending on the number ofcalls you make.

Lampyre pros:

- Great for cybersecurity as well as due diligence
- Gather data from 100+ sources
- Affordable subscription or yearly purchase

Lampyre cons:

- Lampyre and its Lighthouse SaaS aren't the most intuitive pieces of software to use, so there is a bit of a learning curve.

4) GOOGLE – FREE OSINT (IF YOU KNOW HOW TO USE IT)

Search engines such as Google, Bing, or DuckDuckGo are perfectly adequate free OSINT tools. That is, if you know how to use advanced filters. In short, it's about refining your search to benefitfrom the indexing power of some of the best algorithms on the planet.
Over the years, talented investigators have learned how to reverse-engineer search engines. The method is called Google dorking, or Google hacking, and it uses search operators or functions toexpand the capacity of the tools (it works with search engines beyond Google, too).

The method is controversial, because it may cross the line in terms of how "public" the informationis.

For instance, you may find a link to a PDF file containing a list of passwords, but downloading itmay be a prosecutable offense.

Examples of search operators include:

- specific file types
- searching for terms on a specific site
- finding RSS feeds related to a term
- finding files created between specific dates
- etc.

An example of Google dorking would be to search, e.g. company.website.domain for PDF files, which you would do by typing "site:company.website.domain filetype:pdf". You'd be surprised atthe number of documents that are openly available if you know how to get Google to fetch them for you.

You can read more about known Google Dork operators here.

Google Pricing:

- It’s completely free (but comes with concerns about your personal data).

Google pros:

- The free price, obviously
- Limited results
- Requires a lot of trial-and-error

Google cons:

- Privacy issues
- May fall into a grey area when it comes to the legality of obtaining certain documents

5) RECON-NG – AN OPEN SOURCE OSINT FRAMEWORK

Recon-ng initially started as a free and open-source script for gathering technical information about website domains. Since its creation, it has evolved into a full framework, which you can access via a command-line interface on Kali Linux, or as a web application.

Its interface is similar to Metasploitable, another computer security project designed for penetrationtesting, and has similar goals: to assess and identify web vulnerabilities. Its features include GeoIP lookup, DNS lookup, and port scanning, among others.

While it’s certainly one of the more technical tools featured on this list, you’ll find plenty of resources online to learn how Recon-ng can locate sensitive files such as robots.txt, identify hiddensubdomains, look for SQL errors, and get information about a company’s CMS or WHOIS.

Recon-ng pricing:

- It’s free and open source – but obviously limited in the type of information it can return for you.

Recon-ng pros:

- Free and open-source
- Great for cybersecurity

Recon-ng cons:

- Command-line interface only
- Not suitable for less tech-savvy investigators

6) SPIDERFOOT – CYBERSECURITY INTELLIGENCE

SpiderFoot is an OSINT tool designed specifically for investigation professionals. It’s loved bycybersecurity intelligence experts who need to perform regular asset discovery or attack surfacemonitoring. SpiderFoot was acquired by Intel471 in November 2022, with the company announcing that it plans to integrate SpiderFoot’s capabilities into its solutions.

The tool can access hundreds of open data sources and monitor the results in real-time. The keydifference with other OSINT tools, however, is how you can use SpiderFoot.

You can choose to self-host it as a true open-source version. You can also purchase the hostedversion, which is completely managed by SpiderFoot.

There are numerous advantages to the latter. For instance, you'll get better performance, full teamcollaboration, and the ability to see correlations in your investigation. All the modules and third- party tools will come preinstalled and preconfigured.

Spiderfoot pricing:

- SpiderFoot recently removed all pricing information from the website, so there is a chance the tiered-level pricing system has changed. Please contact SpiderFoot for specifics if you are interested.

Spiderfoot pros:

- Affordable plans or open source version
- Team collaboration
- Loved by intelligence experts

Spiderfoot cons:

- Steep learning curve

7) SPOKEO – CHECK US CITIZEN RECORDS

When it comes to checking US citizens' records, there are plenty of services offering more or lessthe same features at the same price range. You might hear of BeenVerified, Pip, or Intelius.

Spokeo offers an easy-to-use interface and the results seem to be more accurate upon testing. You can also use Spokeo as a reverse email lookup, phone lookup tool, and postal address lookup, to getinfo based on a single data point.
The service is available online, and there's even an Android app to perform searches directly fromyour smartphone.

You'll be able to access billions of records such as property deeds, court records, and evenhistorical records and social networks.

The only downside is that it tends to be very US-centric, so if you're looking for someone locatedelsewhere, you might have to use another tool.

Spokeo pricing:

- Spokeo lets you perform one search as a free trial, and you're then invited to purchase a monthly subscription. They've hidden the pricing from their website so you'll need to contact them directly for a quote, but expect to pay $8–$15 per month depending on thefeatures you choose.

Spokeo pros:

- Great for US-based due diligence
- Access historical and court records
- Offers reverse email or address lookup.

Spokeo cons:

- Checks are slow
- Not as free as they claim
- US-centric

8) EMAIL HIPPO – MX RECORDS CHECKS FOR EMAIL LOOKUP

Email Hippo, which you can also access through VerifyEmailAddress.io, has been operating since2009. However, it recently underwent a complete overhaul and is now far from free and open.

Instead, the solution is split into CORE, MORE, ASSESS AND WHOIS, covering use cases suchas data enrichment for investigations, marketing and fraud prevention.

Unfortunately, this sea change in the way the product positions itself has rendered it much more complicated to comprehend. However, the free trial does not require a credit card and lasts 14 days,which can help figure out whether it is for you.

Email Hippo pricing:

- Depends entirely on the product you choose and the frequency of payment or the number of requests sent. CORE, for instance, will set you back $9.88 a month for 1,000checks.

Email Hippo pros:

- An established name in email intelligence with deep insights.

Email Hippo cons:

- Perhaps no longer as useful to OSINT researchers as it once was.

RESULT:

Thus, the OSINT tools were explored successfully.

EX.NO: 5	DBSCAN FOR RISK WARE DATASET
DATE:	

AIM:

To implement DBSCAN for any risk ware dataset in python.

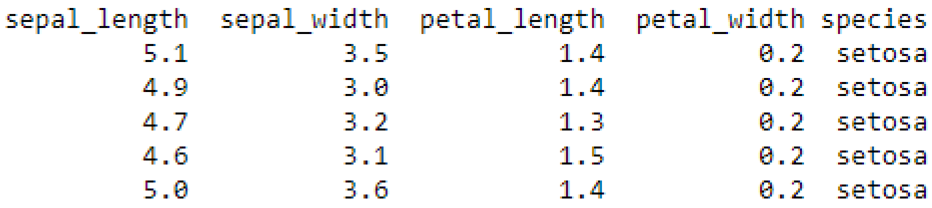
PROCEDURE:

1. Start the program
2. Import libraries, data wrangling, import data
3. run DBSCAN without any parameter optimization
4. plot our K-distance graph and find the value of epsilon
5. visualize the results from the model
6. Creating an outlier’s data frame
7. Stop the program

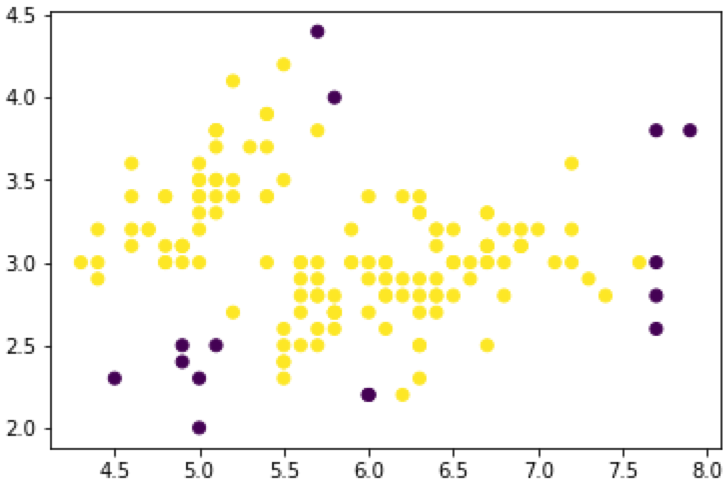
PROGRAM:

```
 import pandas as pd
 import matplotlib.pyplot as plt
 from sklearn.cluster import DBSCAN
 df = pd.read_csv("https://raw.githubusercontent.com/uiuc-cse/data-
 fa14/gh-pages/data/iris.csv")# import data
 print(df.head())
data = df[["sepal_length", "sepal_width"]] # input data
 model = DBSCAN(eps = 0.4, min_samples =
 10).fit(data)colors = model.labels_
 plt.scatter(data["sepal_length"], data["sepal_width"], c =
 colors)outliers = data[model.labels_ == -1] # outliers
 dataframe print(outliers)
```

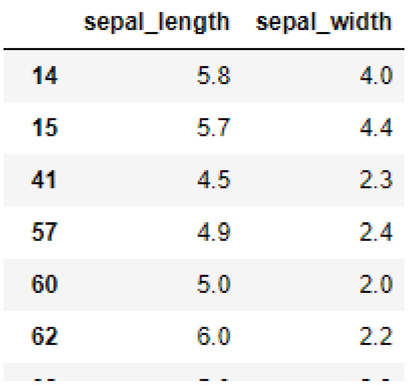
OUTPUT:



```
sepal_length  sepal_width  petal_length  petal_width species
         5.1          3.5           1.4          0.2  setosa
         4.9          3.0           1.4          0.2  setosa
         4.7          3.2           1.3          0.2  setosa
         4.6          3.1           1.5          0.2  setosa
         5.0          3.6           1.4          0.2  setosa
```



Outlier values detected in purple color



	sepal_length	sepal_width
14	5.8	4.0
15	5.7	4.4
41	4.5	2.3
57	4.9	2.4
60	5.0	2.0
62	6.0	2.2

Dataframe of outliers

RESULT:

Thus, DBSCAN for risk ware dataset has been successfully implemented in python.

EX.NO: 6	**PERFORM LOG ANALYSIS USING SPLUNK**
DATE:	

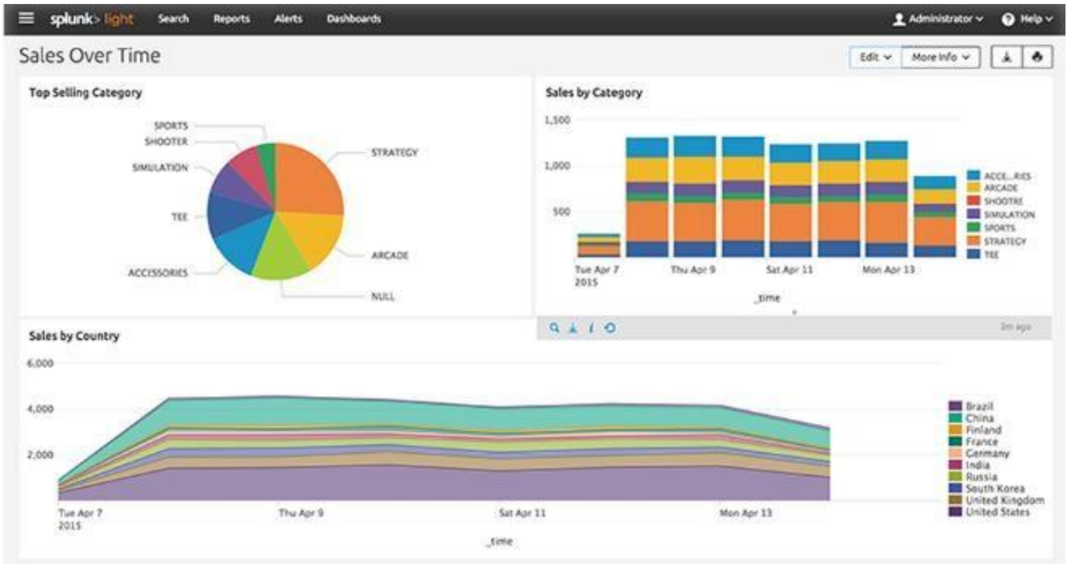
AIM:

To perform log analysis using Splunk

PROCEDURE:

1. Analyzes the aggregate of logs from a big service cluster
2. Finds real-time logs and with faster speed
3. Generates report and alerts for the desired search
4. Provides enhanced GUI and real-time visibility in dashboard in various formats
5. Provides quick results by reducing the time to troubleshoot and resolve issues
6. Works like a monitoring, reporting and analysis tool and provides insights
7. Does not require other dependent services (like database)
8. Requires minimum HW resources
9. Easy to setup and low-cost maintenance
10. Accepts any data type including .csv, JSON log formats etc.
11. Monitors AWS infrastructure
12. Uploads and indexes log data from a local PC to Splunk directly

OUTPUT :



RESULT:

Thus, the log analysis using Splunk was executed successfully.

EX.NO: 7	**FIREWALL IMPLEMENTATION AND TESTING**
DATE:	

AIM:

To explore about firewall and its implementation and testing on the system.

FIREWALL:

Firewall is a system designed to prevent unauthorized access to or from a private network. They can be implemented in both hardware and software, or a combination of both. All datagrams entering or leaving the intranet pass through the firewall, which examines each datagram and blocks those that do not meet the specified security criteria. Our objective is to build a firewall that blocks unauthorized access while permitting authorized communications using packet filtering.

FIREWALL IMPLEMENTATION:

There are different types of environments where a firewall can be implemented ranging from a simple packet filter to combination of several firewalls.

- **Implementation of firewall in Intranet**:

  An Intranet is a network that employs the same types of applications, services, and protocols that are present in an internet, without external connectivity. The Firewall protects the intranet by checking the traffic flow from the interconnected intranets.

- **Implementation of Firewall in Extranet**:

  An Extranet is usually a business-to-business intranet. The Control access is provided to the remote user based on the authentication and authorization as provided by a VPN.

- **Implementation of firewall in VPN:**

  Virtual Private Network (VPN) is a private network that uses public network to connect remote sites or users together. The VPN is created by establishing a virtual point-to-point through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.

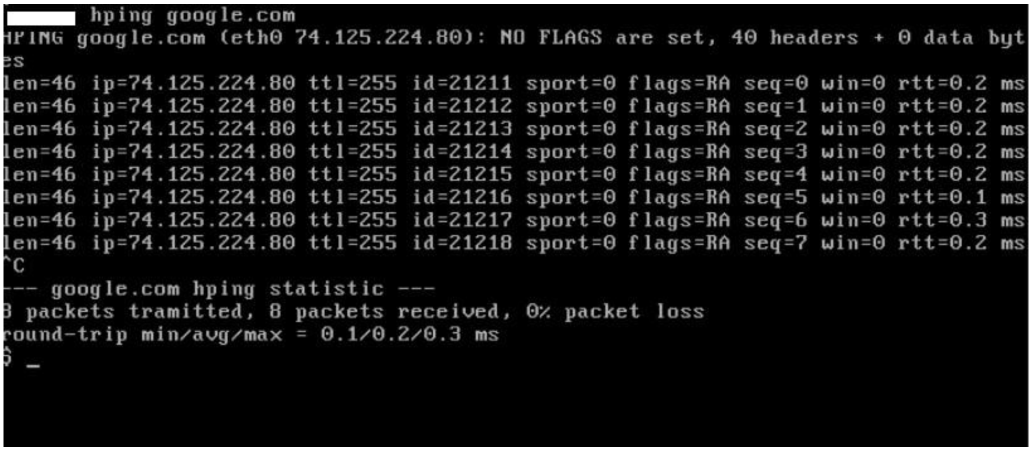
FIREWALL TESTING:

Firewall penetration testing is the process of locating, investigating and penetrating a certain firewall in order to reach the internal trusted network of a certain system.

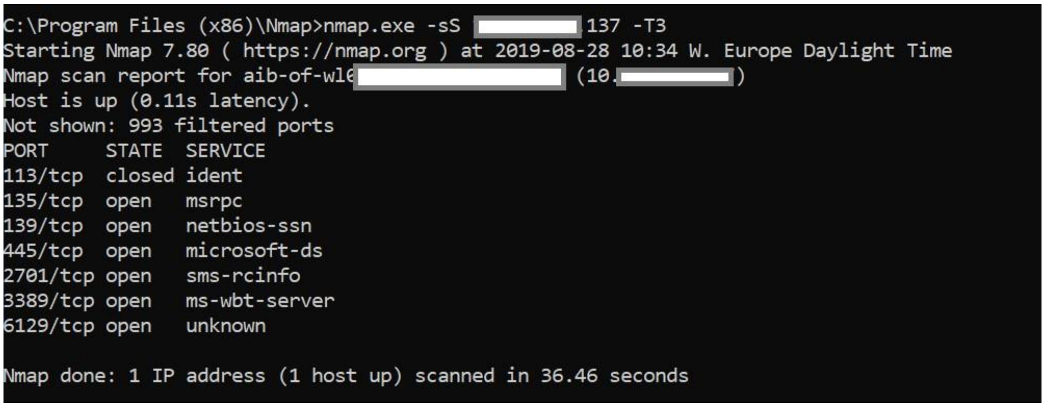
There are 13 steps in firewall testing as follows:

1. Locating the firewall
2. Running traceroute
3. Scanning ports
4. Banner grabbing
5. Access control enumeration
6. Identifying the firewall architecture
7. Testing the firewall policy
8. Firewalking
9. Port redirection
10. Internal and external testing
11. Testing for covert channels
12. HTTP tunneling, and
13. Identifying firewall specific vulnerabilities

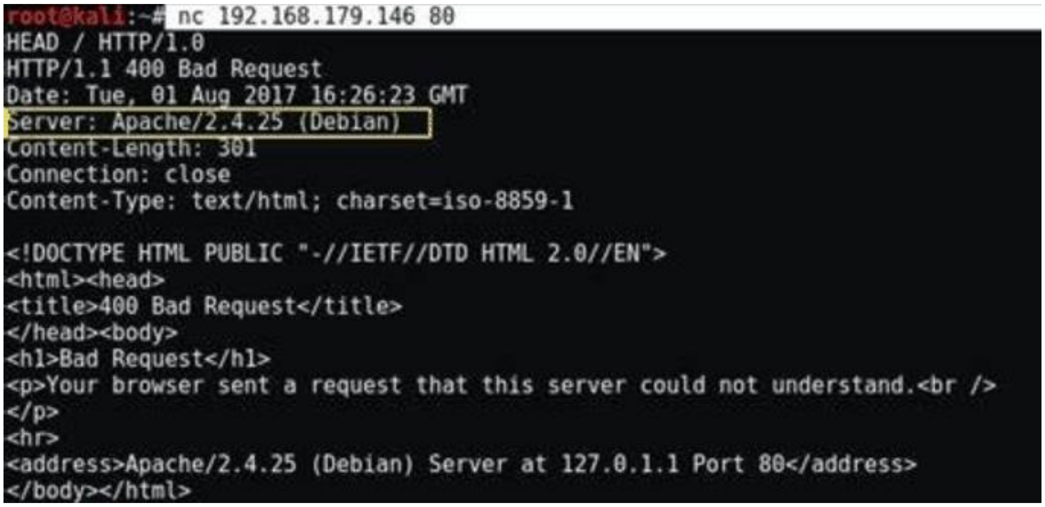
OUTPUT:



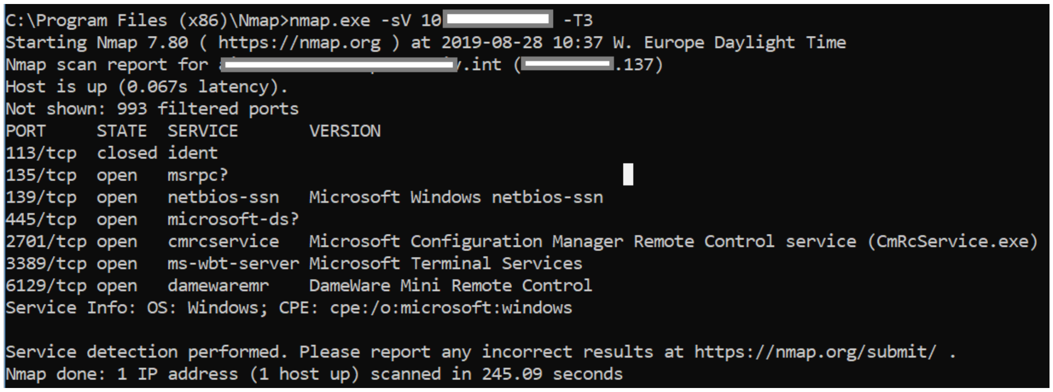
```
[redacted] hping google.com
HPING google.com (eth0 74.125.224.80): NO FLAGS are set, 40 headers + 0 data byt
es
len=46 ip=74.125.224.80 ttl=255 id=21211 sport=0 flags=RA seq=0 win=0 rtt=0.2 ms
len=46 ip=74.125.224.80 ttl=255 id=21212 sport=0 flags=RA seq=1 win=0 rtt=0.2 ms
len=46 ip=74.125.224.80 ttl=255 id=21213 sport=0 flags=RA seq=2 win=0 rtt=0.2 ms
len=46 ip=74.125.224.80 ttl=255 id=21214 sport=0 flags=RA seq=3 win=0 rtt=0.2 ms
len=46 ip=74.125.224.80 ttl=255 id=21215 sport=0 flags=RA seq=4 win=0 rtt=0.2 ms
len=46 ip=74.125.224.80 ttl=255 id=21216 sport=0 flags=RA seq=5 win=0 rtt=0.1 ms
len=46 ip=74.125.224.80 ttl=255 id=21217 sport=0 flags=RA seq=6 win=0 rtt=0.3 ms
len=46 ip=74.125.224.80 ttl=255 id=21218 sport=0 flags=RA seq=7 win=0 rtt=0.2 ms
^C
--- google.com hping statistic ---
8 packets tramitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.2/0.3 ms
$ _
```



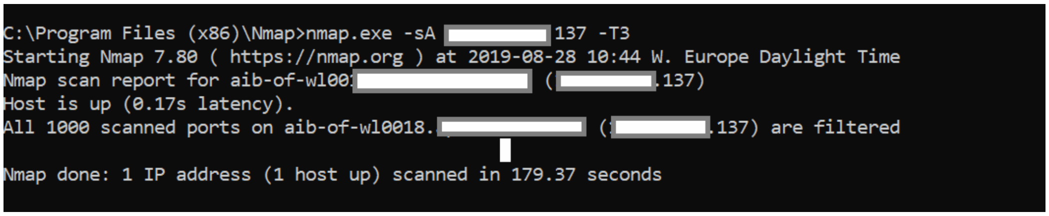
```
C:\Program Files (x86)\Nmap>nmap.exe -sS [redacted]137 -T3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-28 10:34 W. Europe Daylight Time
Nmap scan report for aib-of-wl[redacted] (10.[redacted])
Host is up (0.11s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE
113/tcp  closed ident
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
2701/tcp open   sms-rcinfo
3389/tcp open   ms-wbt-server
6129/tcp open   unknown

Nmap done: 1 IP address (1 host up) scanned in 36.46 seconds
```



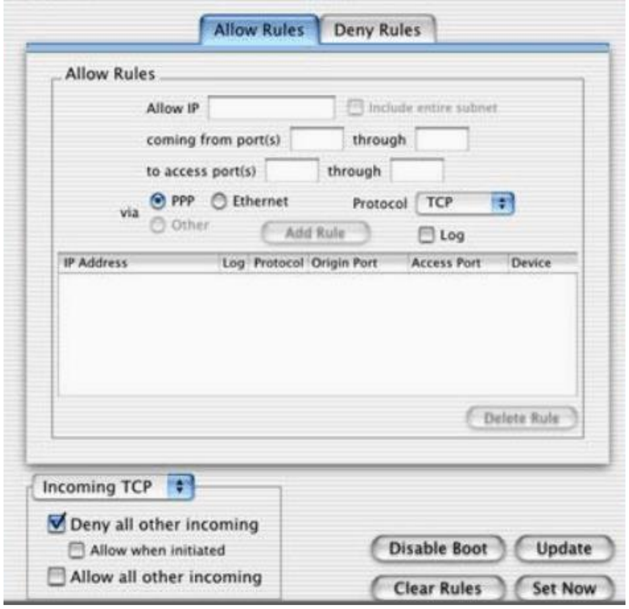
```
root@kali:~# nc 192.168.179.146 80
HEAD / HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Tue, 01 Aug 2017 16:26:23 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.25 (Debian) Server at 127.0.1.1 Port 80</address>
</body></html>
```



```
C:\Program Files (x86)\Nmap>nmap.exe -sV 10[redacted] -T3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-28 10:37 W. Europe Daylight Time
Nmap scan report for [redacted].int ([redacted].137)
Host is up (0.067s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE       VERSION
113/tcp  closed ident
135/tcp  open   msrpc?
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds?
2701/tcp open   cmrcservice   Microsoft Configuration Manager Remote Control service (CmRcService.exe)
3389/tcp open   ms-wbt-server Microsoft Terminal Services
6129/tcp open   damewaremr    DameWare Mini Remote Control
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 245.09 seconds
```



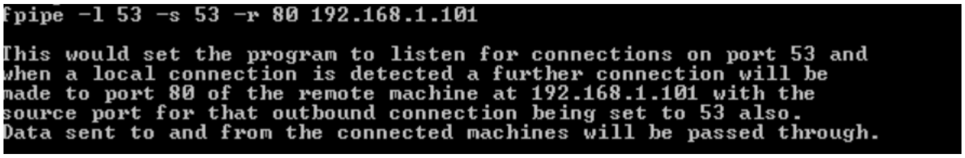
```
C:\Program Files (x86)\Nmap>nmap.exe -sA [redacted]137 -T3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-28 10:44 W. Europe Daylight Time
Nmap scan report for aib-of-wl00[redacted] ([redacted].137)
Host is up (0.17s latency).
All 1000 scanned ports on aib-of-wl0018.[redacted] ([redacted].137) are filtered

Nmap done: 1 IP address (1 host up) scanned in 179.37 seconds
```



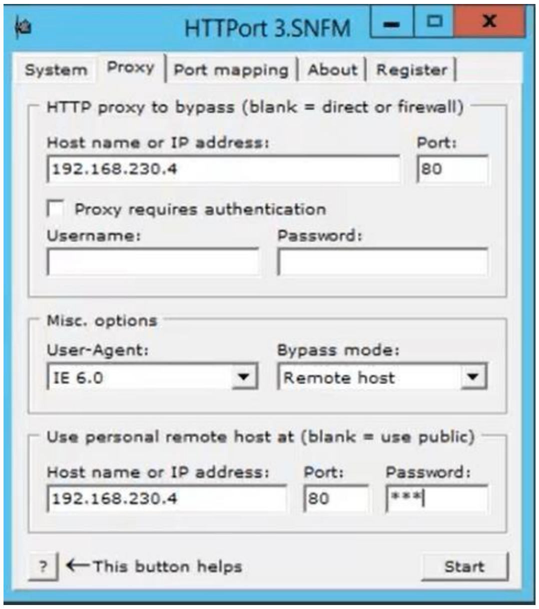
☑ Deny all other incoming

☐ Allow when initiated

☐ Allow all other incoming



```
fpipe -l 53 -s 53 -r 80 192.168.1.101

This would set the program to listen for connections on port 53 and
when a local connection is detected a further connection will be
made to port 80 of the remote machine at 192.168.1.101 with the
source port for that outbound connection being set to 53 also.
Data sent to and from the connected machines will be passed through.
```



HTTPort 3.SNFM
System
Proxy
Port mapping
About
Register
HTTP proxy to bypass (blank = direct or firewall)
Misc. options
Use personal remote host at (blank = use public)
?
←This button helps
Start

Host name or IP address: 192.168.230.4

Port: 80

☐ Proxy requires authentication

Username:

Password:

User-Agent: IE 6.0

Bypass mode: Remote host

Host name or IP address: 192.168.230.4

Port: 80

Password: ***

RESULT:

Thus the 13 steps to check the firewall performance has been implemented successfully.

EX.NO: 8	WEB PENETRATION TESTING USING BURPSUIT
DATE:	

AIM:

To implement the Web Penetration Testing using Burpsuite.

BURPSUITE:

Burp or Burpsuite is a set of tools used for penetration testing of web applications. It has also progressed to the point that it can now detect bugs in APIs and mobile apps. Burp Suite, like most other software, comes in a variety of formats. Different users can have different requirements, and one size does not necessarily suit everything. Burp Suite is available in three different editions to meet the needs of different users.

- COMMUNITY EDITION
- PROFESSIONAL EDITION
- ENTERPRISE EDITION.

TOOLS IN BURPSUITE:

Burp Suite includes a number of tools for performing various research activities. The tools work well together, and you can transfer interesting requests between them while you work to complete various tasks.

- **Target**: This tool provides detailed information about your target applications and allows you to control the vulnerability testing process.
- **Proxy**: This is a man-in-the-middle web proxy that intercepts traffic between the end browser and the target web application.
- **Scanner**: This is a sophisticated web vulnerability scanner that can crawl content and audit it for a variety of vulnerabilities. And is available only in professional version.
- **Intruder**: It is a versatile tool for automating and customizing web application attacks. It can be used to automate a variety of tasks that occur during the testing of software.
- **Decoder**: This is a useful tool for decoding and encoding application data manually or intelligently.
- **Extender**: This enables you to load Burp plugins, which you can use to expand Burp's

features with your own or third-party code.

PROCEDURE:

Burpsuite Installation:

i. We must first ensure that Java is installed on the device before installing or running the Burp Suite. It's a must-have for Burp Suite to work. Once java is installed the next step is to install Bur Suite.

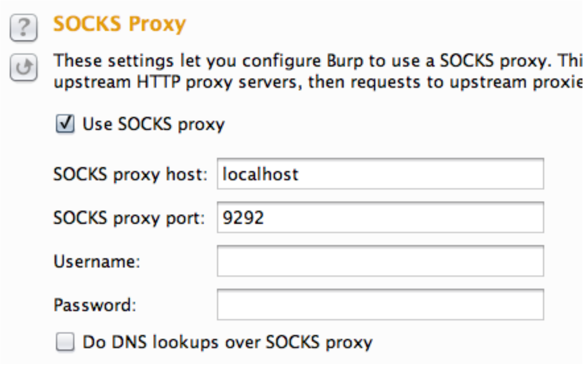
ii. After downloading just open the downloaded file and the popup window.

iii. Choose where you want the Burp suite to be installed on your computer, select the start menu option for the Burp Suite.

iv. Now installation will begin, you can start the Burp suite after it has been successfully mounted.

v. Accept the certificate in order to continue with the start-up, if you're using the community version of Burp Suite, you'll need to create a Temporary project.

OUTPUT:



SOCKS Proxy

These settings let you configure Burp to use a SOCKS proxy. Thi
upstream HTTP proxy servers, then requests to upstream proxie

☑ Use SOCKS proxy

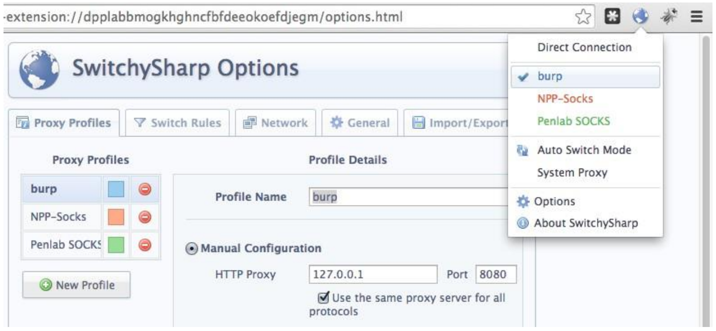
SOCKS proxy host: localhost

SOCKS proxy port: 9292

Username:

Password:

☐ Do DNS lookups over SOCKS proxy



-extension://dpplabbmogkhghncfbfdeeokoefdjegm/options.html

SwitchySharp Options

Proxy Profiles: burp, NPP-Socks, Penlab SOCKS

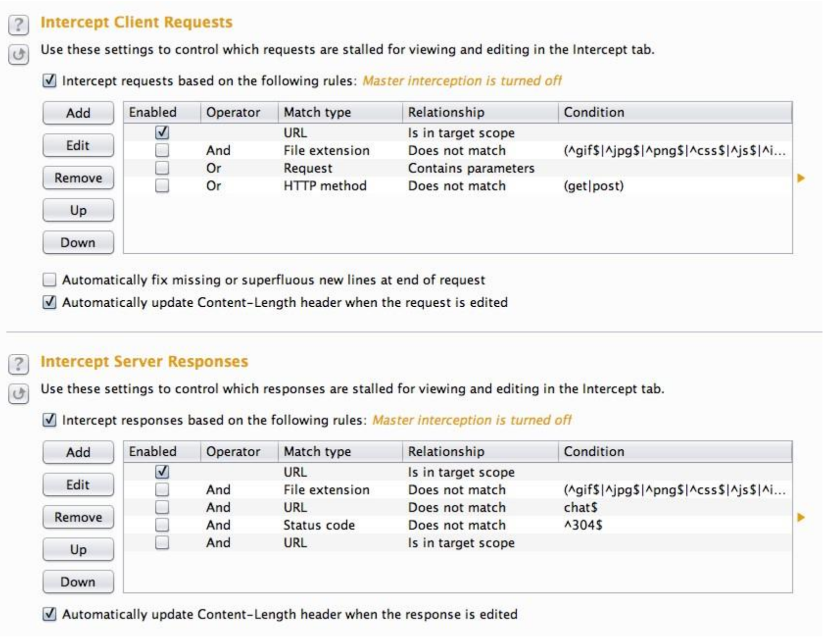
Profile Details

Profile Name: burp

● Manual Configuration

HTTP Proxy: 127.0.0.1 Port: 8080

☑ Use the same proxy server for all protocols



Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
☑		URL	Is in target scope	
□	And	File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$|^i...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)

□ Automatically fix missing or superfluous new lines at end of request

☑ Automatically update Content-Length header when the request is edited

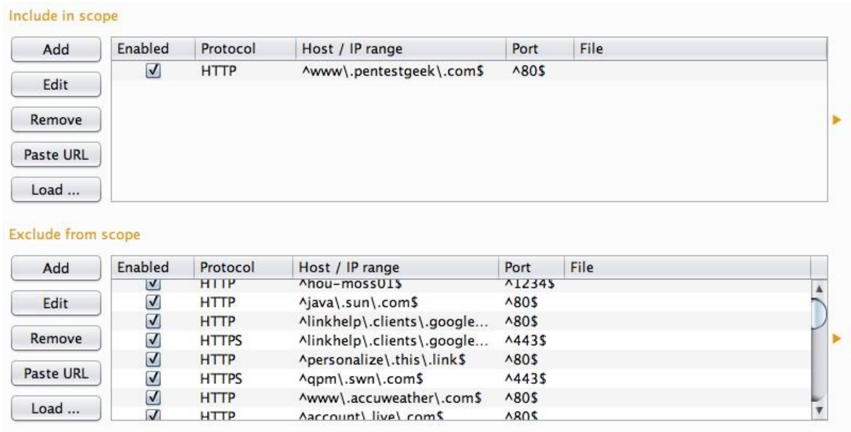
Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☑ Intercept responses based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
☑		URL	Is in target scope	
□	And	File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$|^i...
□	And	URL	Does not match	chat$
□	And	Status code	Does not match	^304$
□	And	URL	Is in target scope	

☑ Automatically update Content-Length header when the response is edited

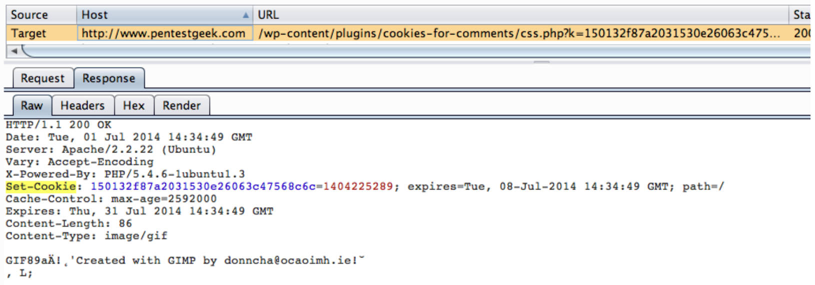


Include in scope

Enabled	Protocol	Host / IP range	Port	File
☑	HTTP	^www\.pentestgeek\.com$	^80$	

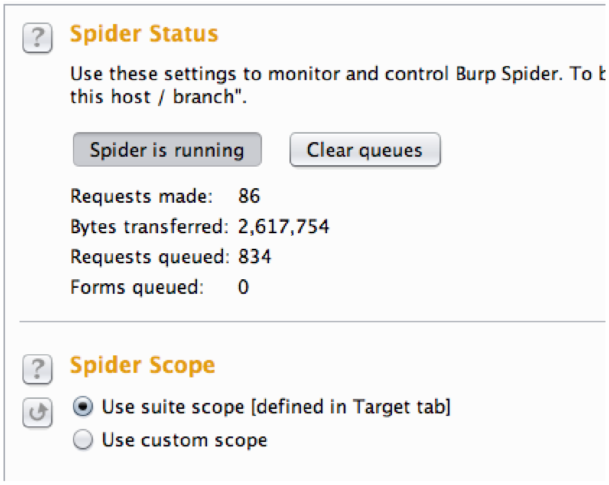
Exclude from scope

Enabled	Protocol	Host / IP range	Port	File
☑	HTTP	^hou-moss01$	^1234$	
☑	HTTP	^java\.sun\.com$	^80$	
☑	HTTP	^linkhelp\.clients\.google...	^80$	
☑	HTTPS	^linkhelp\.clients\.google...	^443$	
☑	HTTP	^personalize\.this\.link$	^80$	
☑	HTTPS	^qpm\.swn\.com$	^443$	
☑	HTTP	^www\.accuweather\.com$	^80$	
☑	HTTP	^account\.live\.com$	^80$	



Source	Host	URL	Sta
Target	http://www.pentestgeek.com	/wp-content/plugins/cookies-for-comments/css.php?k=150132f87a2031530e26063c475...	20(

```
HTTP/1.1 200 OK
Date: Tue, 01 Jul 2014 14:34:49 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.6-1ubuntu1.3
Set-Cookie: 150132f87a2031530e26063c47568c6c=1404225289; expires=Tue, 08-Jul-2014 14:34:49 GMT; path=/
Cache-Control: max-age=2592000
Expires: Thu, 31 Jul 2014 14:34:49 GMT
Content-Length: 86
Content-Type: image/gif

GIF89aÄ!¸'Created with GIMP by donncha@ocaoimh.ie!˜
, L;
```



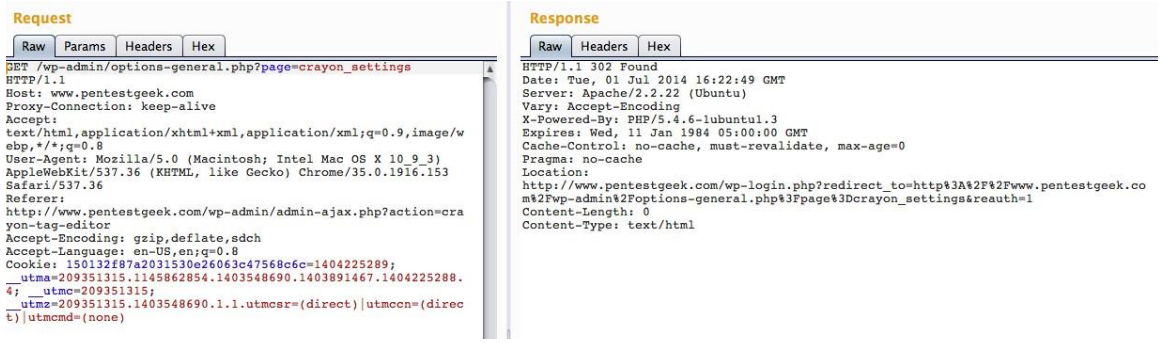
Spider Status

Use these settings to monitor and control Burp Spider. To b
this host / branch".

Requests made: 86
Bytes transferred: 2,617,754
Requests queued: 834
Forms queued: 0

Spider Scope

● Use suite scope [defined in Target tab]
○ Use custom scope

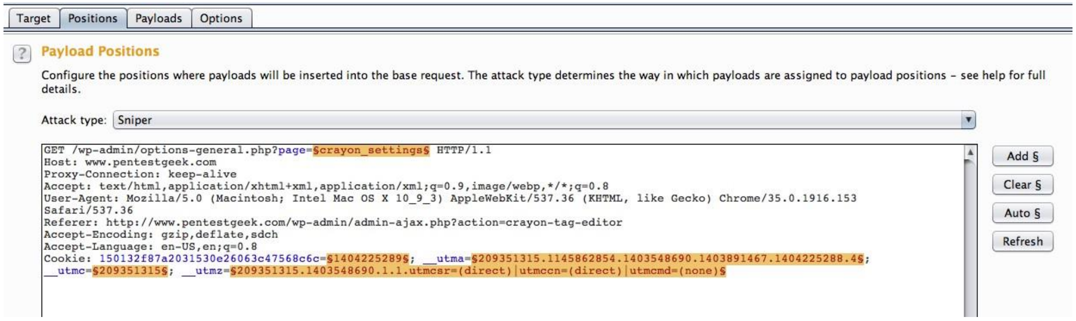


Request

```
GET /wp-admin/options-general.php?page=crayon_settings
HTTP/1.1
Host: www.pentestgeek.com
Proxy-Connection: keep-alive
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/w
ebp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153
Safari/537.36
Referer:
http://www.pentestgeek.com/wp-admin/admin-ajax.php?action=cra
yon-tag-editor
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: 150132f87a2031530e26063c47568c6c=1404225289;
__utma=209351315.1145862854.1403548690.1403891467.1404225288.
4; __utmc=209351315;
__utmz=209351315.1403548690.1.1.utmcsr=(direct)|utmccn=(direc
t)|utmcmd=(none)
```

Response

```
HTTP/1.1 302 Found
Date: Tue, 01 Jul 2014 16:22:49 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.6-1ubuntu1.3
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
Location:
http://www.pentestgeek.com/wp-login.php?redirect_to=http%3A%2F%2Fwww.pentestgeek.co
m%2Fwp-admin%2Foptions-general.php%3Fpage%3Dcrayon_settings&reauth=1
Content-Length: 0
Content-Type: text/html
```

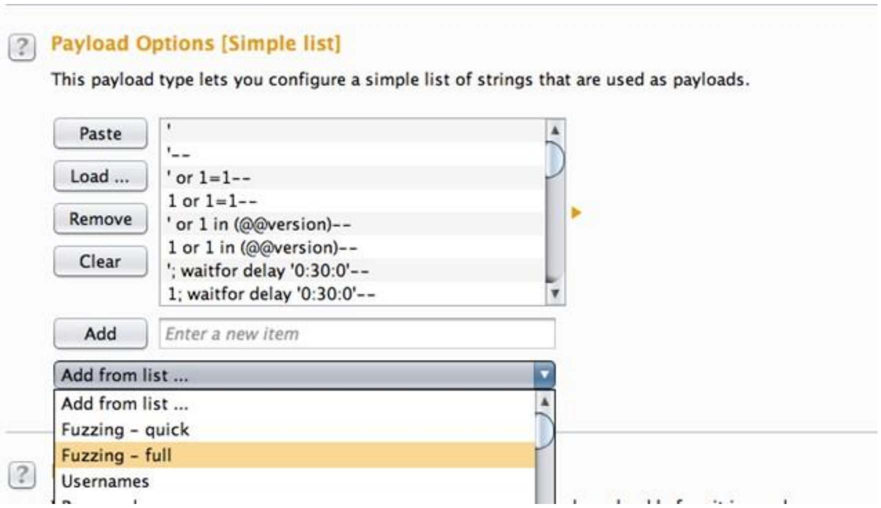


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions – see help for full details.

Attack type: Sniper

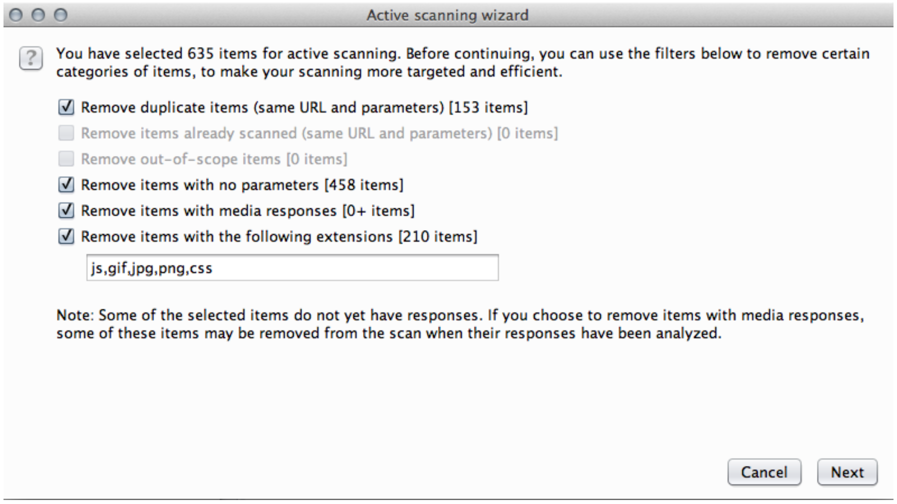
```
GET /wp-admin/options-general.php?page=§crayon_settings§ HTTP/1.1
Host: www.pentestgeek.com
Proxy-Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153
Safari/537.36
Referer: http://www.pentestgeek.com/wp-admin/admin-ajax.php?action=crayon-tag-editor
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: 150132f87a2031530e26063c47568c6c=§1404225289§; __utma=§209351315.1145862854.1403548690.1403891467.1404225288.4§;
__utmc=§209351315§; __utmz=§209351315.1403548690.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)§
```



Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
'
'--
' or 1=1--
1 or 1=1--
' or 1 in (@@version)--
1 or 1 in (@@version)--
'; waitfor delay '0:30:0'--
1; waitfor delay '0:30:0'--
```



You have selected 635 items for active scanning. Before continuing, you can use the filters below to remove certain categories of items, to make your scanning more targeted and efficient.

☑ Remove duplicate items (same URL and parameters) [153 items]

□ Remove items already scanned (same URL and parameters) [0 items]

□ Remove out-of-scope items [0 items]

☑ Remove items with no parameters [458 items]

☑ Remove items with media responses [0+ items]

☑ Remove items with the following extensions [210 items]

js,gif,jpg,png,css

Note: Some of the selected items do not yet have responses. If you choose to remove items with media responses, some of these items may be removed from the scan when their responses have been analyzed.

RESULT:

Thus, Web penetration testing using Burpsuit was performed successfully.

CASE STUDY
AI IN CYBER SECURITY

FORTUNE 500 TELCO USING SNORKEL FLOW TO CLASSIFY ENCRYPTED NETWORK DATA FLOWS

A globally-recognized Fortune 500 telecom company used Snorkel Flow to classify encrypted network data flows into their associated application categories. The customer's data science team faced a number of challenges for this task, including:

1. Their past experience of **labeling network traffic data by hand was too slow, noisy, and expensive**, requiring precious time from network data experts.
2. Their existing probe used a static set of rules based on a fixed set of Service Name Indicators (SNIs), leading to a **brittle solution that was difficult to adapt**.
3. Their previous approach also struggled to accommodate changing data distributions, such as responding to network trouble tickets or alarms.
4. Multiple tools were required to cover the end-to-end machine learning pipeline, from data exploration and labeling, to model training and analysis.

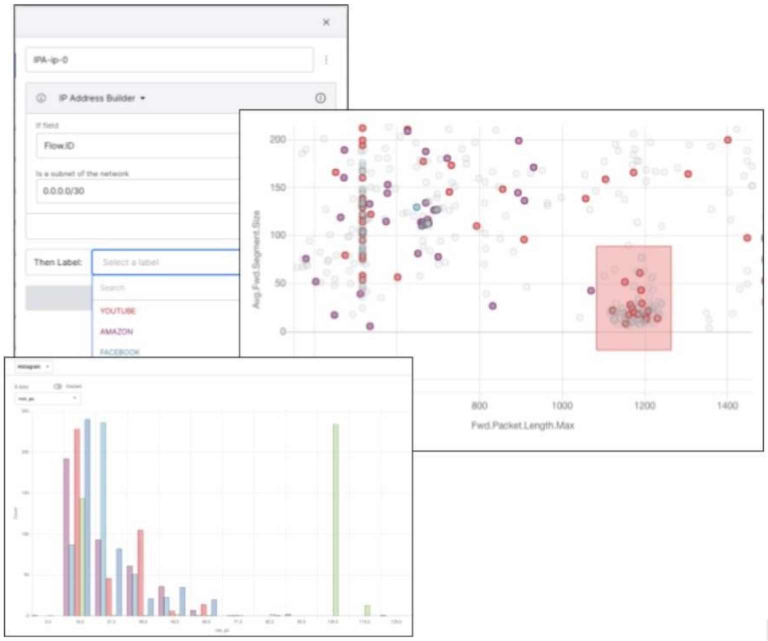
TASK DESCRIPTION: CLASSIFYING NETWORK DATA FLOWS:

To evaluate Snorkel Flow's ability to accelerate the development of ML models and AI applications for network data use cases, this customer compared a new solution they developed in Snorkel Flow against an existing solution based on a fully-supervised ML model trained on 178,000 ground-truth data examples. The Snorkel Flow solution was also compared against a baseline model trained on a subset of 2,000 examples from this ground-truth dataset. The goal was to see whether Snorkel Flow could enable this organization to produce a solution capable of replacing the fully-supervised ML in a fraction of the time required to manually label a ground-truth training dataset.

In this data, individual flows contained categorical and text features like source/destination port and IP address, SNIs, and forward/backward packets. Flows were then preprocessed to include statistical features, such as forward/backward inter-arrival time (IAT) statistics, flow bytes per second, and flow packets per second. Users of varying skill levels combined a number of different strategies for this effort, including creating no-code labeling functions with Snorkel Flow's built-in network data visualization tools, writing code-based labeling functions using Snorkel Flow's Python SDK, and leveraging Snorkel Flow's ability to auto-generate labeling functions based on self-training and semi-supervised methods.

RESULTS WITH SNORKEL FLOW:

An initial subset of only 2,000 ground-truth labeled examples, this telecom customer used Snorkel Flow to produce an additional 198,000 programmatically-labeled examples. A model trained in Snorkel Flow on this 200,000-example training dataset was 26.2% more accurate than a baseline model trained on the subset of 2,000 examples, and within 0.2% accuracy of a fully-supervised model trained on all 178,000 ground-truth examples. For aspects of the data that change over time, such as SNIs (which are prone to drift in production settings), the Snorkel Flow model was comparedwith a static rules-based solution and the baseline model described above. Incredibly, the Snorkel Flow model was 77.3% more accurate than the rules-based approach and also outperformed the



baseline model by nearly 10%. An additional experiment was performed to test Snorkel Flow's ability to adapt to changing distributions in the data, like the proportions between application types in the network traffic. Here, the Snorkel Flow model beat the baseline model by over 20% and managed to slightly outperform a fully-supervised model as well.

Snorkel Flow has no-code UI support for rapidly creating labeling functions with network data

Ultimately, using Snorkel Flow enabled this customer to:

- Deliver high-accuracy ML models for a network data application quickly, without being slowed down by an extensive hand-labeling process.
- Develop adaptable solutions that provide a marked improvement over brittle, rules-based approaches.
- Build applications that are robust to network data drift, by maintaining consistently-high performance scores even when data distributions change.
- Help network data experts and data scientists to work together, using first-class network visualization and data processing utilities in a unified platform.

Encouraged by these impressive results on their first Snorkel Flow project, this customer is now developing a new application focused on anomaly detection for IMS network equipment metrics. This effort will identify real-time anomalies over time-series data, starting with the number of call attempts per second.