L00149506 Placement IEEE paper

by Gaurav Chittineni

Submission date: 09-Jul-2020 06:00PM (UTC+0100)
Submission ID: 1036456172
File name: L00149506_Placement_IEEE_paper.docx (691.37K)
Word count: 7443
Character count: 39581

LETTERKENNY INSTITUTE OF TECHNOLOGY

ASSIGNMENT COVER SHEET

Lecturer's Name: Ruth Lennon
Assessment Title: _____
Work to be submitted to: Ruth Lennon
Date for submission of work: _____
Place and time for submitting work: Blackboard as per submission link

To be completed by the Student

Student's Name: Gaurav Chittineni {L00149506}
Class: Msc Private Cloud Technologies
Subject/Module: Placement
Word Count (where applicable): 7227
I confirm that the work submitted has been produced solely through my own efforts.
Student's signature: Gaurav **Date:** _____

Notes

Penalties: The total marks available for an assessment is reduced by 15% for work submitted up to one week late. The total marks available are reduced by 30% for work up to two weeks late. Assessment work received more than two weeks late will receive a mark of zero. [Incidents of alleged plagiarism and cheating are dealt with in accordance with the Institute's Assessment Regulations.]

Plagiarism: Presenting the ideas etc. of someone else without proper acknowledgement (see section L1 paragraph 8).

Cheating: The use of unauthorised material in a test, exam etc., unauthorised access to test matter, unauthorised collusion, dishonest behaviour in respect of assessments, and deliberate plagiarism (see section L1 paragraph 8).

Continuous Assessment: For students repeating an examination, marks awarded for continuous assessment, shall normally be carried forward from the original examination to the repeat examination.

Network Monitoring and Management

Gaurav Chittineni
L00149506
Dept of Computing
chittinenigaurav@gmail.com
L00149506@student.lyit.ie

Abstract— **The main objective for the implementation of this project is the identification and classification of devices that are connected in a given network. The devices are identified using the subnet mask range. An automated script is created that is used to ensure that the timestamp and labels are automatically generated during scanning of the devices. The automation script is also used to capture and identify the network devices at given time intervals. Ping scan can be used to identify the network addresses that are live. Live hosts can be identified using the ICMP requests and responses. An ICMP response contains the details that show if the device is active or not.**

I. Introduction

The use of systems that can be able to monitor computer networks and components is important in maintaining the security and reducing the risk levels in an organization. Network monitoring involves the use of tools that can be able to scan and verify the connected devices. Network management is an aspect involving filtering and identifying the threats to a network in real-time. Intrusion detection systems can be able to monitor the threat levels from outside the network infrastructure. Network problems can be caused by overloading and increased number of connected devices within the network. The response and the turn around time for a given server can be measures in terms of the responsiveness of the server to respond with resources to a client program. Different routing methods and algorithms can be used to perform network configuration and management to ensure that data is analyzed on the fly. The aspect of monitoring the performance of network devices and servers is to give alerts during systems downtime and failures. The metrics that are used to measure the performance and enhance the alert capabilities of the monitoring software include, CPU usage, memory capacity and the disk space. Monitoring the devices using external software and network management tools is more effective on measuring the effectiveness and the performance of the network enabled devices. Network monitoring requires the running of parallel servers concurrently accessing the same resources. This aspect of distributed computing is used to enhance of the capacity and increase in the bandwidth while enhancing other operations such as backup. This project is concerned with the aspects of monitoring a network environment to determine the number of network devices in the network. The list of the devices connected are appended into a file.

Managing all devices on a network via snapshots can be done using automation script. This automation script can log IP addresses of all the network devices connected, can generate the date and time details of snapshots and it can rollback the devices to previous snapshot without effecting the performance and security. In this method a virtual network is setup and virtual admin is used to control the process. Several Virtual machines of ESXI server or Centos or Windows server are installed as devices of the network. A FortiGate firewall virtual machine is used as router/firewall of network. This forms a simple network. Using scripting for eg:- 'arp -a' IP addresses scanning is done. Snap shots are created for each VM, date and time of each snapshot is generated using commands. All the Virtual machines except admin VM are roll backed to previous snapshot. At last the admin VM is roll backed to previous snapshot state. Thus the end result is achieved without effecting the performance and security.

II. Importance of Network Monitoring

Scanning for the entire network infrastructure is important to the operations and the management of an organization. Information about the devices connecting to the network architecture can usually be logged for identification of the time and the date of establishing the connection[1].

Network monitoring is important due to the following reasons:

A. Security

The most important aspect of maintaining the network security is to maintain the integrity and prevent the alteration of data. Scanning enables the network administrators to keep and maintain track of all the operations that may affect the operations and the performance of the organization. For instance, checking if the maximum number of users connected to the network is exceeded is a proactive measure to ensure that the server and applications are up and running.

B. Troubleshooting

This involves finding the generic problems and the threats that may be affecting performance of the devices and the applications. Automation tools can be used to check and monitor the network in real-time ensuring that problems are easily detected. Early detection of network threats ensure provision of mitigation techniques that can be used to cub the threats and risks. Penetration testing of the network infrastructure should be done frequently using automated tools that are configured to operate at time intervals. After the identification of threats, exploits can be executed against the target environment to determine the risk level of the threat to the organization[2].

C. automation scripting:

shell scripting is a scripting which executes various commands step by step. It is nothing less or nothing more than a program. It is used in providing interface layer between end user and linux kernel. In RHEL 7 bash is generally used as default for user accounts. Varying from case to case the tasks for automating might be different. The main advantage of scripting is the user need not do the programming again and again if needed. The user can just run the script and it will be done.

D. snapshot

The duplicate of virtual machine at a point of time is called snapshot. For the virtual disk a change log is provided by the snapshots. These change logs are used to restore the disk files to a particular point when there is any failure in the system. Backups are not provided by the snapshots alone. When the snapshot is taken then it can be only readable not writable. Administrators can take a multiple snapshots so that can restore it to a particular point of time. Current disks and memory states will be deleted if virtual machine is reverted to snapshot. The size of the original disk file should not be less than the snapshot file.

With high disk write activity the snapshots will grow rapidly. With in an hour most of the screenshots will be deleted. It is recommended to delete the snapshots with in 24 hours. There are different formats in snapshots like .vmsd, .vmsn and .vmdk files. In vmware snapshot manager administrators will create snapshots. All of the delta files into the vmdk are merged with snapshots by deleting or committing. The snapshot will not be deleted properly if delta files remain in the vm's directory after deletion.

There are few best practices to follow regarding snapshots. They are

1. Any snapshot should not be more than 72 hours. 32 snapshots in chain are supported by the vmware. Try to maintain only three snapshots in any chain,
2. For input or output intensive virtual machines with rapid data changes do not rely upon snapshots because when virtual machine is restored data inconsistencies will be occurred.

E. Tools and Architecture

Scanning of a network infrastructure begins with the classification of the architectural design and identification of the hardware requirements. Organizations build up on the network design to increase more coverage on the number of devices that can be connected for a give period of time. This therefore shows that the right tools must be used to monitor and manage the operations performed on the network. Open-source tools used for monitoring are important in saving of the time and resources investment. Depending on the tool of choice, certain principles and guidelines must be used to secure the integrity of data and information exchanged by the organization.

Tools that can be used for network monitoring include:

i. Cacti

This is a network monitoring tool that involves the collection of data from the network devices. The network enabled devices include : routers, switches, firewall. Once the data packets are captured, cacti is then used to display robust graphs from the data collected[3]. SNMP protocol is used for communications and sharing of the data packets for the devices that are connected within the network. The effectiveness of cacti in data collection is the use of commands and queries. Exploiting the use of commands extends the capabilities that are found in cacti that includes a graphing system. Graphing system is used to create and visualize the graphs from the data-set of the data packets tored. Multiple users can be able operate and access the tool concurrently using the necessary permissions.

Figure 1:Cacti graphing utility program.

ii. N top

This is a Linux command line tool that leverages the probe of network traffic using libpcap for packet capture. An extension of ntop is ntopng a tool that uses multiple instances of the same interface with capabilities of using port mirroring that acts as a tap to filter the data packets flowing on the network. Figure[2] :N top network management tool.

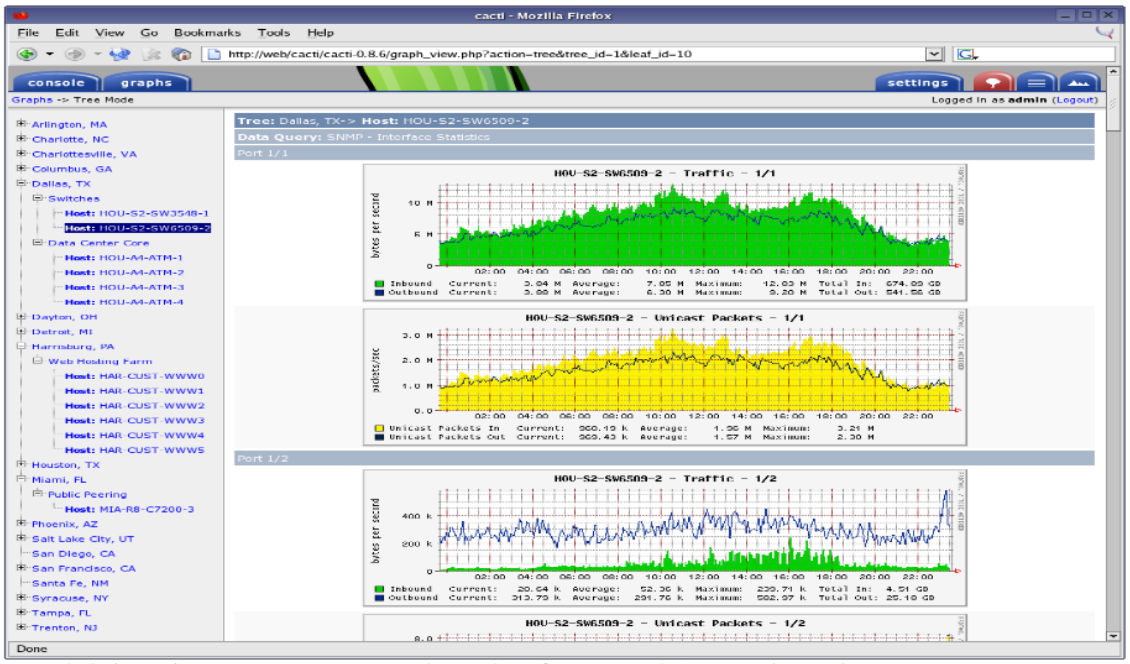


Figure 1:Cacti graphing utility program

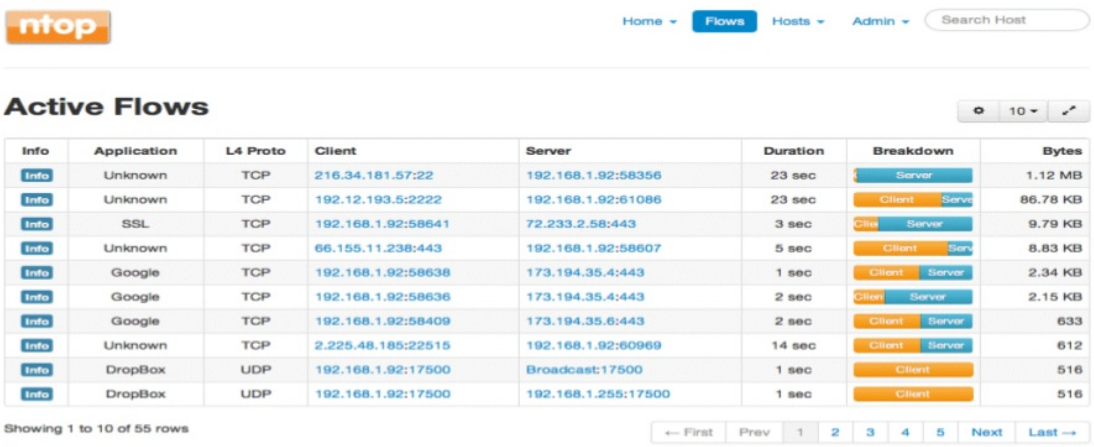


Figure 2 :Ntop network management tool.

The open source version is fast enough to give a quick insight on the network traffic with additional features such as :

- Generation of reports on timely basis.
- Determining the number of packets exchanged.
- Determining the IP ranges for the devices connected.

The application is able to cluster on the level of performance of the device, for instance the up-time and down-time of a server depending on the data packets that are transmitted from the client to the server-based applications[4]. The importance of using the tool for network capture is the intuitive features packaged with the commercial version. Advanced scanning techniques are adopted to identify the network threats and the risk in real-time. Identifying the threats in real-time is features that ensures the mitigation techniques can be put in place to cub the increased threats to the enterprise.

Network management is charged with the responsibility of maintaining the integrity of the network architecture. Security along with integrity of the applications and data is important in the management and the operations of an organization[5]. Therefore network scanning is a field that actively involves identification of the devices within the network that are a threat to the operations of the organization. Different tools are used depending on the nature and the complexity of the network infrastructure. Advanced tools such as wireshark can be used to capture and analyze the network traffic in real-time. The data traffic can then be analyzed to identify the threats and vulnerabilities that can be exploited by attackers to gain access to the system. Privilege escalation are techniques that can be used to ensure that the attackers are able to perform their operations with administrative features[6].

III. Virtual Machine Configuration

Virtual machines are used within the Linux environment to manage scanning and reporting on the network devices. The virtual machines can be used with sandbox features that act as stealth environments to detect and identify the threats affecting the network devices in real-time. A virtual machine is an emulation of a computer based architecture that is used to leverage the power and the functionalities of a physical system. The implementation of a virtual machine may involve a combination of the hardware and the software devices. There are different type of virtual machines depending on the use and the environment. This project is concerned with the generation of an automation tool that can be used to scan a network environment producing a list of interconnected network devices [7].Virtual machine is used to leverage the importance of a multiple system with time-sharing capabilities able to perform multiple tasks. Generalization is the concept that is used to share virtual memory with privileged access to the input / output devices. The main purpose for using the virtualization technology is management of a virtual environment that can be used in the place of a physical system.

Figure 3:Virtual machine architecture.

Figure 4: Virtual Box

Virtual Box is an application that creates a virtualized environment that behaves as a separate system interconnected to the hardware enabled devices. The Virtual machines executes on a single window in the processes managed by the

Figure 3:Virtual machine architecture.

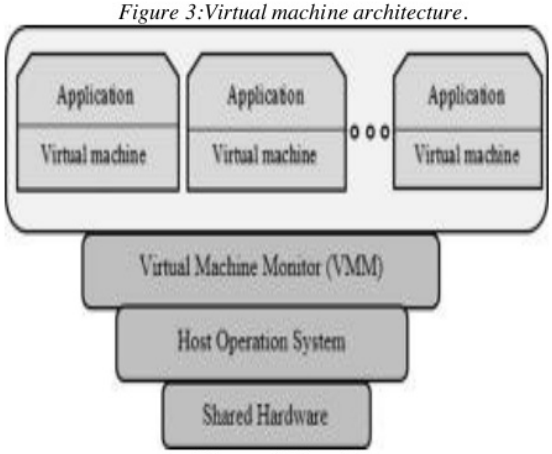
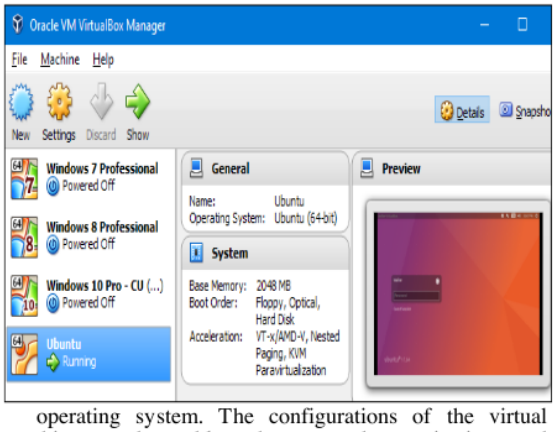


Figure 4: Virtual Box



operating system. The configurations of the virtual machine used enables the network monitoring and management tools to operate with increased latency. The monitoring tools are used to scan the internal network externally using the virtual environment as a sandbox system[8].

Figure 5:Creating a virtual machine.

The virtual machine is allocated memory from the physical system during the initial setup and configuration. Dynamic memory allocation to the virtual device is important to ensure that the network monitoring event do not overload the operations of the physical device. In this case, a fixed memory size is created to ensure that the virtual machine only uses the available size limit. Allocation of fixed size memory maintains the performance and the efficiency of the virtual machine in terms of the execution and the response time speeds. After successful installation and configuration of the system, the virtual machine can hence be started.

Figure 6:Virtual machine execution.

The script can be executed using different versions of the virtual machines to increase on the performance. The

Figure 5:Creating a virtual machine.

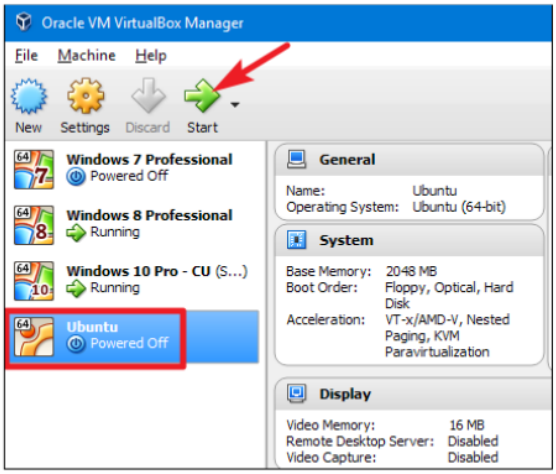


Figure 6:Virtual machine execution.

scanning device must be connected to the local network. This ensures that the virtual machine used is able to get the range of the subnet mask that is used to scan for the devices[9].Domain name configuration ensures that the devices accessing the internet resources are resolved into the respective addresses that are added to the network list.

IV.Network Scanning

This can be explained as a procedure that is used for identification of devices that are actively connected to a network using the application of network protocols. Scanning can also be termed as the process that is used to identify the elements that can be used to perform attacks on a network.

Scanning techniques used depend on the nature and the features of the protocol that the devices use to connect to the network[10].For instance, ICMP can be used while using ping to send packets to a remote devices and checking for remote hosts. The process of network scanning involves sending a well crafted message to the ranges of the IP addresses and listening for a response for each of the IP in the range. If a response is received for a certain IP In the range, then the IP address can be added to the list of live hosts[11].

Importance of network scanning

Management and the monitoring of networks and systems is important due to the following reasons:

- Identifying the network users currently connected to the network.
- Determining the state of the devices.
- Checking on the elements of the networks.
- Detection of network threats in real-time.

Logging can be used as a management technique that ensures users connected to the network are appended to a file. Attackers are able to gain access to the information of the IP address by obtaining the ranges using DNS system. This is protocol can be used to determine the range of the IP address that is assigned to a given organization. The process involved

using the automation tool to scan the network can be described as :

Scanning of IP networks is generally done by sending ping requests to an IP address and receiving a response[12]. The response sent is used to determine the state of the IP address. Address Resolution Protocol can be used to ping the whole subnet mask that is covered by the range of the IP addresses using automatic scans and device discoveries.

Figure 7:Network scanning process.

Although ICMP protocol is more complicated timestamp and echo requests can be used in mapping of network topology. The purpose of performing this experiment of network scanning include :

- To determine all the devices that are connected to the network topology.
- Checking the operating systems that are in use.
- Determining the health of the network infrastructure.
- Filtering malicious data traffic.
- Protecting the networks from any form of attack.

Figure 8:Passive network scanning.

Vulnerability assessment and scanning can be described as a method that is used to determine the vulnerabilities found in a computer system. This method is used to identify the weaknesses in the operating system that can be exploited by attackers to compromise the operations of the systems and the networks. The processes such as port scanning, ping sweeps are used to generate specific information about live hosts and mapping the entire infrastructure of the live hosts[13].DNS is an address resolution system that is used to translate known domain names to specific address. This information of IP addresses is contained in the cache system. Attackers can be able to access the cache using spoofing techniques to gain access to critical information contained in the DNS system about known IP ranges. Enumeration is the stage that is concerned with the collection of useful information such as :

- Routing information.
- Usernames.
- Group names.

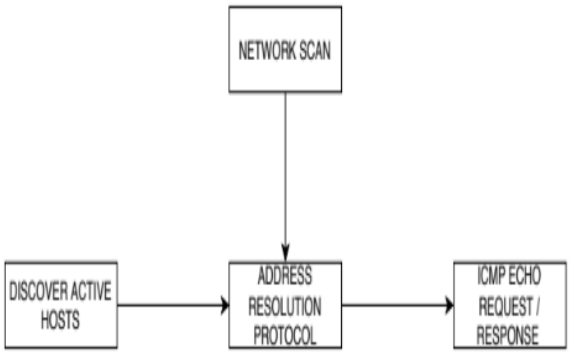


Figure 7:Network scanning process.

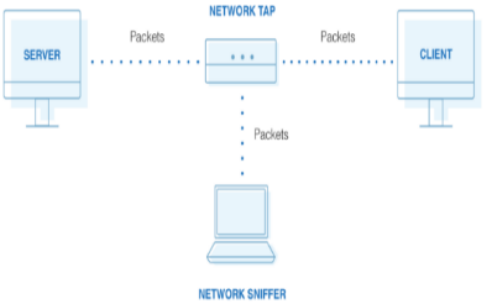


Figure 8:Passive network scanning.

This information is used to stage attacks to the target environment using the vulnerabilities discovered. This project is aimed at collecting all the important information about the IP address, log the information to a file and discover the threats that can affect the performance of the network.

V.METHODOLOGY

This project follows certain paradigms used in the process of scanning and verifying the IP addresses connected to the network. The process involves identification of the gateway used and the subnet of the network devices. The gateway is important due to the identification of the routing information from the network enable device[14]. All the devices that are alive can be found within the range of the subnet mask. The subnet is provided with the range of the addresses and seq a command-line Linux utility tool is used to validate the mask. The automation script created in bash is used to scan the network at intervals, the snapshots of the timestamp are also recorded. The reason for using automation is to improve on the performance and interoperability in scanning for the available devices. The results from the network monitoring and management tool indicates the range of the addresses that are live.

VI.IMPLEMENTATION

A bash script is implement that is able to scan for the entire network for a list of available devices. Scanning the network requires the use of sudo privileges or performing the operations as root. This therefore means that sudo rights must be given to the script to enable scanning of the devices that are connected to the network[15].Ping requests are used to scan the entire subnet using a given range for the IP addresses. The subnet mask is composed of the network address information. The range of the subnet begins from 1 and ends at 255 , for instance if the IP range starts at 172.1.1. then the end is 172.255.255. This is the mask that is used for the management and scanning of the IP ranges. Logging is a feature that is used in the developed in the scanner application to maintain track of all the devices that are connected to the network. Once a live device is detected in the network , the address is then added to the log file.

Using the Unix volume managers the copy-on-write operations are usually enabled to enhance creating copies of the changed blocks of data. An image can be used to preserve the integrity of the device that contains the snapshots. The snapshots can be mounted into the file system using read-only permissions for the medium. Some of the volume managers also contain implementation of write operations that extends the copy-on-write privileges to associate the entire blocks of

memory using the original block contained in the original volume of the filesystem. Logical volume managers are used during the implementations of the read and the write operations.

The operations for managing and creating the snapshots of the backup copies depends on the availability of the writable snapshots for a particular device. Parent blocks of data contained in the original volume of memory are usually referenced by the volume managers using the read and write permissions. File systems such as ODS-5 and UFS2 contain an implementation of a namespace that provides an API used to access the file histories in the operating system. Using the NTFS system , the API provides access to the snapshots using a shadow-copy services. Clustered storage platforms contain an implementation of a scalable system that can be able to access the snapshots directly using read-only permissions at the directory level. Dynamic memory access is used to manage the implementation of the copy-on-write operations performed on the system[16].

Cloning of the snapshots involve the creation of copies of individual files using Btrfs file system. This system supports the creation of multiple instances of the snapshots using the same volume. A hybrid implementation of the read-write operations requires the branch files from the sub-volume to be mounted into the specific applications in the form of clones. At the block level , the operating system saves all the copies of the snapshots by maintaining the state of the applications.File and directory access using the kernel devices requires the use of special permissions that are used for read and write access into the devices. Special driver programs are used to control the particular permissions that are required for the management of the hardware programs. Once data is written into the services managing the applications, the main function of the kernel is to write the data into the device. Floppy disks are used to hold the data written temporarily before transfer to a secondary device for permanent storage.

The main function of the floppy device is the transfer of the data into a physical medium using a port connected to the device. The port can also be used to transfer or send the data to another parallel port that is connected to the same device. The device drivers are able to implement an isolation device that contains the specific code of the kernel. An application is able to access the kernel and the device using a platform specific file that contains the configuration information.

The main reason for capturing and maintaining copies of the filesystem at given time intervals is to maintain a backup of the data that is stored in the applications. Some of the data is usually stored temporarily in the primary storage and as a cache and deleted once the operations and the processes accessing the data are depleted.

Therefore to maintain the integrity and the copy of the data , the snapshots are usually generated automatically using generic time intervals. The determination on the device driver that is used by the kernel to access the applications is dependent on the processes and the services that are executing for the current instance of the file system. The devices are usually mapped into platform specific files using the drivers.

The process involved in scanning of the devices for those are connected within the network requires the use of Network and Dial-up protocols. The connections are managed by the kernel for the platform specific device and the Ethernet devices[17]. The point-to-point protocols are used to connected one platform specific device to another to enhance the sharing and access to the files.

A tree based hierarchy is contained in the main configuration of the root filesystem with the files being contained in the device drives and the hard drives.

Multiple implementations of the file system is used to manage the user access to the programs and the files contained in the operating system. Mounting the partitions and the devices is an operation that should be undertaken before accessing the partitions. File systems are important due the nature of the operations that they perform including managing IO operations and access to data loss. Backup copies of the data contained in the filesystem is usually managed by the file system.

A swap partition is used to create an additional extension space that can be used to hold the programs that are available in memory. The partitions that are created in the instance of the operating system can be clustered into primary , extended , logical and the swap partition. The partitions are usually allocated address space depending on the complexity and the nature of the files that are stored in that instance.

Formatting the filesystem therefore means that, write and read permissions are required to access the files and the directories that are contained in the filesystem. Creation of the snapshots for the partitions require the read-only access. These permissions are usually issued by the root and the manager of the device. The permissions vary depending on the capabilities and the utility programs that are used to access the root programs.

The structure and the logic of a given filesystem can be defined as :

- Flexibility to other utility programs.
- Security of the operations managed by the filesystem.
- Integrity of the data stored.

Some of the file systems are usually accessed as local devices while others are managed and controlled using a network protocol such as the SMB. The SMB is used to provide access to the files belonging to a certain computer system on port 445 via network access.

Virtual files can be mapped using the virtualization technique for access from the physical devices. Virtualization enables the physical devices to be accessed using a Network layer. Access to both the files and the metadata is a function that is managed by the file system. The file system is also responsible for storage capabilities that involve allocating address space to the storage devices. Factors such as reliability and efficiency to the speed of data access are considered during the implementation of the physical storage medium. The design operations considers both the storage capacities for the physical medium and access to the virtual files[18].A file system contains layers that are separated using an application programming interface that manages the ways in which the files and the storage media is access from different interfaces. The virtual file system is also able to support multiple instances of the same physical system that is contained in the implementation and the design of the file

system. The physical layer is mapped into operations that involve storage of physical blocks of memory and data into distinct locations. Memory management is the function of physical layer that involve translating the physical blocks of memory into the relative locations in the physical storage medium. The physical file system is hence charged with the responsibility of mapping the device drivers into the channels that can be managed by the device drivers.File system fragmentation is an operation that occurs when the unused space in memory is not contiguous such that the spaces allocated for the data does not grow with time. Once the files and the programs are deleted from the file system, the memory that was initially allocated for that program is considered for allocation to another instance of the same program or process.

Figure 9:Script implementation.

Figure 10:Implementation 2.

Figure 11:Implementation 3.

Figure 12:Result 1.

Figure 13:Result 2.

Screen capture is a command line tool that is used to capture the snapshots of the devices for given time intervals. The tool can be installed on the command-line using apt-get install screencapture using sudo privileges. The timestamp is recorded and generated together with the captured snapshots. The snapshots are then saved to a directory.

Figure 14:Screen capture.

VII. Device Management

The main function of a filesystem is the control and the retrieval of data from a computer system. The data in a filesystem is usually stored in a huge volume of data in the form of bits. The rules and the management structure used to manage the groups of data in the computer system can be termed as the file system. Different types of filesystem vary depending on the design and the applications that use and manage the data. Some of the filesystem can be used for local storage into the devices while others have access through the use of network protocols. The contents and the metadata of the files stored in the devices can be restored from a backup system. The main functions of a filesystem include ; data optimization using the storage mediums , data synchronization and management of the files[19].

The filesystem is important in the management of the devices and snapshots of the devices that are connected to the network. Once the snapshots have been captured, they are stored in the filesystem for retrieval. Rolling back the device into the original state requires access into the filesystem. A backup copy of the snapshots is usually created and stored in the filesystem. This therefore means that to access the filesystem, the user needs the necessary read and write permissions. A virtual filesystem can be used to operate on multiple and concurrent instances of the same file system.

The implementation of multiple file systems require the a parallel interface that contains the functionalities of the system in use. Physical blocks are used for the management of the read and write capabilities , they are also able to handle memory and buffer blocks by placing the blocks into the specific locations in the context of the storage medium. The interactions with the physical medium using the device drivers enhances the retrieval of the snapshots from the storage devices .Snapshots are used to manage the particular state of a computer system in a given instance. The state of the system and the capabilities of the system using the defined device drivers is the feature for the management of the snapshots.

A. *Rationale*

Cloning and the creation of backup copies for the filesystem is a process that can take lots of time to complete. A multi-threaded system can usually contain the write and the read permissions to the data that is stored for backup in the devices. Accessing the data from the file system may result to data corruption due to write access by parallel programs at the same time. This hinders the process that is used in the creation and development of a backup copy of the filesystem. For instance, moving a directory or a file from the computer system before a backup copy of the file has been created. The problem of data corruption in memory of the computer system can be prevented through the use of file synchronization and disabling the write permissions for concurrent programs. Preventing the applications from accessing the write operations of the file system is an approach that can be used for the management of backup copy of the snapshots.

High-end system contains a back copy in the form of a snapshot with the applications having write access into the filesystem. The backup contains only a read-only copy using the data frozen from a specific point in time. O(1) notation is used during the process of implementation and creation of the snapshots. The time taken to create a clear snapshot the device depends on the data that is contained in the file system.

```
#!/bin/sh

: ${1?"Usage: $0 ip subnet to scan. eg '192.168.1.'"}

LOG=Log.log

X=$1

echo "Scanning IP range ..."

for addr in `seq 0 1 255 `; do
echo ${X}${addr} >> ${LOG}
( echo ${X}${addr})
( ping -c 3 -t 5 ${X}${addr} > /dev/null && echo ${X}${addr} is Alive ) &
```

Figure 9:Script implementation.

```
DNS="8.8.8.8"
INTERFACE=$(ip route get "${DNS}" | awk -F 'dev ' 'NR == 1 {split($2, a, " "); print a[1]}')
NETWORK_IP=$(ip route | awk "/${INTERFACE}/ && /src/ {print \$1}" | cut --fields=1 --delimiter="/")
CIDR=$(ip route | awk "/${INTERFACE}/ && /src/ {print \$1}" >> ${LOG})
FILTERED=$(echo "${NETWORK_IP}" | awk 'BEGIN{FS=OFS="."} NF--' >> ${LOG})

ip -statistics neighbour flush all &>/dev/null

echo -ne "Pinging ${CIDR}, please wait ...\n"
for HOST in {1..254}; do
  ping "${FILTERED}.${HOST}" -c 1 -w 10 &>/dev/null &
done
```

Figure 10:Implementation 2.

```
FILTERED=$(echo "${NETWORK_IP}" | awk 'BEGIN{FS=OFS="."} NF--' >> ${LOG})

ip -statistics neighbour flush all &>/dev/null

echo -ne "Pinging ${CIDR}, please wait ...\n"
for HOST in {1..254}; do
  ping "${FILTERED}.${HOST}" -c 1 -w 10 &>/dev/null &
done

for JOB in $(jobs -p); do wait "${JOB}"; done

ip neighbour | \
    awk 'tolower($0) ~ /reachable|stale|delay|probe/{printf ("%5s\t%s\n", $1, $5)}' | \
      sort --version-sort --unique
```

Figure 11:Implementation 3.

```
192.168.1.27
192.168.1.28
192.168.1.29
192.168.1.30
192.168.1.31
192.168.1.32
192.168.1.33
192.168.1.34
192.168.1.35
192.168.1.36
192.168.1.37
192.168.1.38
192.168.1.39
192.168.1.40
192.168.1.41
```

Figure 12:Result 1.

```
192.168.1.244
192.168.1.245
192.168.1.246
192.168.1.247
192.168.1.248
192.168.1.249
192.168.1.250
192.168.1.251
192.168.1.252
192.168.1.253
192.168.1.254
192.168.1.255
Pinging , please wait ...
2c0f:fe38:2100:8377::34 76:c1:7d:5b:2a:89
192.168.43.38    76:c1:7d:5b:2a:89
fe80::74c1:7dff:fe5b:2a89        76:c1:7d:5b:2a:89
```

Figure 13:Result 1.

Figure 13:Result 2.

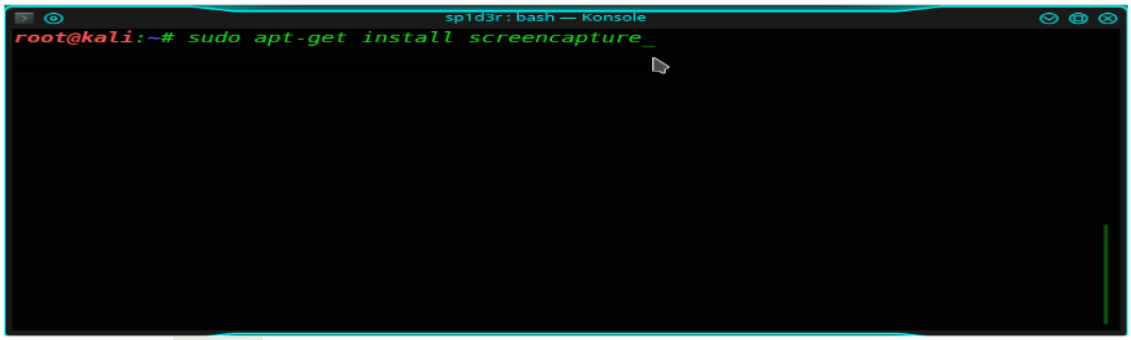


Figure 14:Screen capture.

Pointers are used as references to address the memory capacity that is occupied by the snapshots. This method of using pointer based attributes to reference the data in the backup consumes less disk capacity as compared to direct access method of creating a clone. Different file system can be used to provide different implementations of the snapshots due to the size and the availability of the memory capacity for each of the operating system using a platform specific device.

B. *Rolling back*

The action of rollback of the devices to the original snapshot requires the use of snapper. Snapper is a command-line linux utility tool that is used in the context of this project to rollback to the original snapshot of the devices created.napper checks for previous logs to determine and check the original versions of the snapshots that were created using the timestamp.

Figure 15:Roll back 1.

Figure 16:Device rollback.

VIII. Performance and Security

The programs that are used to access and perform network scans are required to be fast to ensure that the results are generated in real-time. Time complexity is considered for the utility programs. The time length for the generation of the results depends on the complexity of the network. Different tools can be used depending on the nature and the protocols that are used to manage the network operations. For instance in TCP , SMTP , FTP protocols , different network scanning and utility programs can be used for analyzing the data packets. Malicious data packets can be identified in real- capturing and .time and the threat intelligence tools can then be used to identify the nature of the threats and the risk levels.The risk levels are used to indicate the impact of the network threat on the network infrastructure and architecture. Scanning and Enumeration tools are used to identify the devices that are connected to the same network. These devices are allocated certain addresses using the DNS and the Address Resolution protocols. Once a device connects to the internet, Physical and remote addresses are allocated to that device which are used to access the internet.

The integrity of the data packets should be maintained by the organization performing the network analysis. This is to prevent the packets from being manipulated for later access into the systems. Network scanning is an approach that usually depends on the number of the IP that originate from a destination to some source IP using a known port. The port is used for sending the data packets between the client and the server programs. Detecting of IP addresses that exceeds a defined approach is a method that consumes system resources including memory and the CPU. This method can be used to generate huge volumes of data traffic and therefore is not valid for in network scanning[20].

Network scanning tools such as NMAP are used to leverage the power of low-level scanning to identify the malformed packets from one distinct port to another. The anomalies that originate from network scanning methodologies emanate from poor accuracy in the detection techniques. The abnormal and the malicious patterns that prevail in a network can be detected from the host connected devices that generate the traffic. Anomaly detection systems can be able to identify the normal and legitimate user activities.

```
#!/usr/bin/env bash

# the path containing the logs of the snapshots

PATH="/var/local/log/snp"
# the date of the snapshots
date=$(date "+%Y-%m-%d-%H%M%S")
# log file used
LOG="${PATH}/snp_${date}.log"

! [[ -d ${PATH} ]] && mkdir -p ${PATH}

# execute
exec >  >(tee -a "$LOG")
exec 2> >(tee -a "$LOG" >&2)
```

Figure 15:Roll back 1.

```
# log to a file

echo "> Logging to: ${LOG}"

snapshot_=$(snapper create --type=pre --cleanup-algorithm=number --print-number --description="${cmd}")
echo "> New pre snapshot with number ${snapshot_}."
echo -e "> Running command \"${cmd}\".\n"

eval "${cmd}"

snapshot_=$(snapper create --type=post --cleanup-algorithm=number --print-number --pre-number="$snapshot_")
echo -e "\n> New post snapshot with number ${snapshot_}."
```

Figure 16:Device rollback.

The methods and the tools that are used in the process of identifying the malicious activities aid an organization on improving the security measures and mechanisms that can be used to guarantee data safety. The administrators and the managers of the applications need improvise routine and timely based scanning to uncover the threats that can compromise the operations of the organization in real-time. Different tools have distinctive levels of proficiency that can be used to generate outputs and results based on the features of the scanner. Network security is a mechanism that can therefore be used to fulfill and manage the operations.

The importance of network security in an organization include :

- Protecting the network connected devices.
- Maintaining data and information security.
- Reducing the vulnerabilities emanating from applications and high-end systems.

Vulnerability assessment can be identified as the procedure and the process that can be used to identify the threats and the potential security risk to the operations of the company. The scanners that are often used to scan for the network threats prioritize on the weaknesses and the vulnerabilities with each of the security risk assigned a value to indicate on the level of threat that the attackers to the potential damage of the network enterprise.

The information and the reports that are generated by the network scanners enhance the operations and the performance of an organizations network.

A. Access Control

The procedure and the process that is used to identify and recognize the threats and the risk levels to the information systems in an organization. The control used to manage access to these resources involves elevating the privileges that can be used to access the systems. Confidential information should only be accessed by authorized users with timestamp indicating the time of access and the transactions undertaken. Data protection is an interdisciplinary field that is concerned with the security measures and the need to use complex systems to manage the integrity of the data. Vulnerabilities in the information systems used by an organization may expose it to data loss and manipulation.

Encryption is a process that can be used to control access to the data and information using cryptographic keys that encrypt the data and are only shared with the involved parties. The project was involved with the identification of the devices that are connected to a network using routine programs that ping through the network. The ping scans are transmitted between the clients applications and devices accessing the network to identify the live hosts. The factors and the measures that can be used to secure the network from the connected devices is identified and the necessary measures and procedures outlined[21].

Vulnerabilities are usually mapped into domain specific categories depending on the threat level and the impact to the systems. Different methodologies can be used to identify and classify the vulnerabilities that are present in a network enterprise. The mitigation techniques and procedures are usually derived from the vulnerabilities identified. The process that is used in the process of identifying the threats and the risk level depends on the complexity of the networks and the data traffic. Data traffic usually emanates from the connected devices in the network. This therefore means that the identification of the network based threats and vulnerabilities requires complex network based scanners to perform an in-depth analysis of the data traffic.Network mapping is a process that involves clustering the network resources and the devices into their respective domains. The ports used for establishing connections to the network depends on the protocols that are used. For instance, port 22 is used for SSL protocol and for devices that require to gain access to other systems.

IX.CONCLUSION

The security of a network enterprise is important in securing the applications and the data exchanged. Other procedures such as the use of encryption can be used to secure the data from external threats and manipulation. The main reason why attackers gain access to a system is to gain access to the data to perform manipulation operations.

A key is used to encrypt the data stored by the applications, both private and public keys are generated. The public key is exchanged with all the parties that are involved in the connection while the private key is used to maintain the integrity of the applications and the data.The list of IP addresses displayed are determined from the subnet of the local network. Both live and down hosts can be identified using a ping request , the method simply works by sending an ICMP request to the device and analyzing the ICMP echo response sent. The response is used to indicate if the device is live or not.

The main objective of this project has been met whose aim was the identification of the devices that are connected with a network. Domain host control is a procedure that can be used to ensure that all domains translated into specific IP addresses are secure. Attackers can be able to configure and use certain Domain names to perform malicious operations. These operations may include carrying out denial of service attacks, spoofing and data theft. These operations can be blocked if the domain names are verified and authorized before they can be translated to domain specific addresses.

Virtual machines are used in the operations of this project to leverage the speed of using distributed systems concurrently to perform the same procedures. In this case different virtual machines can be used to perform the same procedure of scanning through the entire network infrastructure.

Git hub link for the practical *: - https://github.com/GauravChittineni/Network-Monitoring.git*

X. References

[1] F. Tang, Y. Kawamoto, N. Kato, K. Yano and Y. Suzuki, "Probe Delay Based Adaptive Port Scanning for IoT Devices with Private IP Address Behind NAT",*IEEE Network*, vol. 34, no. 2, pp. 195-201, 2020. Available: 10.1109/mnet.001.1900264.

[2] A. Al-Fandi, "Symmetric Volatile Shared Key Encryption: A Two-way Communication Shared Key Encryption",*Mathematics and Computer Science*, vol. 2, no. 3, p. 27, 2017. Available: 10.11648/j.mcs.20170203.11.

[3] I. Prasetyo, "Analisa Sniffing Paket ICMP menggunakan Wireshark",*SISTEMASI*, vol. 8, no. 1, p. 221, 2019. Available: 10.32520/stmsi.v8i1.339.

[4] "INTEGRATION OF ICMP WITH IP TRACEBACK FOR DETECTING MALICIOUS NODE.",*International Journal of Advance Engineering and Research Development*, vol. 3, no. 10, 2016. Available: 10.21090/ijaerd.031034.

[5] М. Бойченко, И. Иванов, А. Кондратьев and В. Лохтуров, "Regulating Loads of Network Interfaces using Ping Utility of ICMP Protocol",*Herald of the Bauman Moscow State Technical University. Series Instrument Engineering*, no. 89, 2016. Available: 10.18698/0236-3933-2016-4-74-84.

[6] K. Coffey, R. Smith, L. Maglaras and H. Janicke, "Vulnerability Analysis of Network Scanning on SCADA Systems",*Security and Communication Networks*, vol. 2018, pp. 1-21, 2018. Available: 10.1155/2018/3794603.

[7] K. T, "Intrusion Detection and Vulnerability Analysis with Temporal Relationalship",*International Journal of Psychosocial Rehabilitation*, vol. 23, no. 4, pp. 1205-1216, 2019. Available: 10.37200/ijpr/v23i4/pr190447.

[8] K. Rieck, "Vulnerability analysis",*it - Information Technology*, vol. 59, no. 2, 2017. Available: 10.1515/itit-2016-0059.

[9] "VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT)",*International Journal of Recent Trends in Engineering and Research*, vol. 4, no. 3, pp. 326-330, 2018. Available: 10.23883/ijrter.2018.4135.tru9k.

[10] "Vulnerability Assessment and Penetration Testing through Artificial Intelligence",*International Journal of Recent Trends in Engineering and Research*, vol. 4, no. 1, pp. 217-224, 2018. Available: 10.23883/ijrter.2018.4028.rdd10.

[11] A. Bialas, "Vulnerability Assessment of Sensor Systems",*Sensors*, vol. 19, no. 11, p. 2518, 2019. Available: 10.3390/s19112518.

[12] T. Isogai, "Dynamic correlation network analysis of financial asset returns with network clustering",*Applied Network Science*, vol. 2, no. 1, 2017. Available: 10.1007/s41109-017-0031-6.

[13] "Linux servers exploited for a decade",*Network Security*, vol. 2020, no. 4, p. 3, 2020. Available: 10.1016/s1353-4858(20)30038-6.

[14] L. Galante, P. Geus and M. Botacin, "Monitoração de aplicações em ambientes Linux - Linux applications monitoring",*Revista dos Trabalhos de Iniciação Científica da UNICAMP*, no. 26, 2019. Available: 10.20396/revpibic262018870.

[15] N. Trivedi, H. Patel and D. Chauhan, "Fundamental Structure of Linux Kernel based Device Driver and Implementation on Linux Host Machine",*International Journal of Applied Information Systems*, vol. 10, no. 4, pp. 40-45, 2016. Available: 10.5120/ijais2016451495.

[16] "LINUX DEVICE DRIVER DEVELOPMENT ON ARM CORTEX A9 BASED EMBEDDED SYSTEM",*International Journal of Advance Engineering and Research Development*, vol. 3, no. 10, 2016. Available: 10.21090/ijaerd.031019.

[17] A. Khoroshilov, "Software Model Checking of Linux Device Drivers",*Electronic Proceedings in Theoretical Computer Science*, vol. 253, pp. 7-8, 2017. Available: 10.4204/eptcs.253.3.

[18] А. Сальный and А. Остроух, "Research of File System Capacity for Linux Kernel",*Automation and Control in Technical Systems*, vol. 0, no. 4, p. 158, 2016. Available: 10.12731/2306-1561-2014-4-16.

[19] "DETECTION OF MOVING OBJECTS BY A PASSIVE SCANNING SYSTEM",*Автометрия*, no. 1, 2019. Available: 10.15372/aut20190110.

[20] O. Kaller, L. Bolecek, L. Polak and T. Kratochvil, "Depth Map Improvement by Combining Passive and Active Scanning Methods",*Radioengineering*, vol. 25, no. 3, pp. 536-547, 2016. Available: 10.13164/re.2016.0536.

[21] A. Gupta, D. Kumar and A. Barve, "Hidden Markov Model based Credit Card Fraud Detection System with Time Stamp and IP Address",*International Journal of Computer Applications*, vol. 166, no. 5, pp. 33-37, 2017. Available: 10.5120/ijca2017914060.

L00149506 Placement IEEE paper

ORIGINALITY REPORT

6%	4%	1%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.lyit.ie Internet Source	2%
2	Submitted to Melbourne Institute of Technology Student Paper	1%
3	Submitted to Letterkenny Institute of Technology Student Paper	<1%
4	Submitted to University of Maryland, University College Student Paper	<1%
5	Submitted to Victorian Institute of Technology Student Paper	<1%
6	www.ijert.org Internet Source	<1%
7	myassignmenthelp.com Internet Source	<1%
8	Submitted to University of Newcastle upon Tyne Student Paper	<1%
9	article.sciencepublishinggroup.com	

	Internet Source	<1%
10	Submitted to Asia Pacific Instutute of Information Technology Student Paper	<1%
11	Submitted to Fullerton College Student Paper	<1%
12	Vladimir V. Razevig, Margarita A. Chizh, Valery V. Chapursky, Sergey I. Ivashov, Andrey V. Zhuravlev. "Numerical comparison of mono-static and multi-static array performance in personnel screening systems", 2016 Progress in Electromagnetic Research Symposium (PIERS), 2016 Publication	<1%
13	Submitted to Australian Catholic University Student Paper	<1%
14	Submitted to University of Northumbria at Newcastle Student Paper	<1%
15	Syed Rizvi, RJ Orr, Austin Cox, Prithvee Ashokkumar, Mohammad R. Rizvi. "Identifying the attack surface for IoT network", Internet of Things, 2020 Publication	<1%

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		