iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4326

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Novel Approach to Investigate Network Content Event Records in Virtual Environment over Host System

Ms. Ritu Dahiya[1], Dr. J G Pandya[2]
[1, 2]*Kadi Sarva Vishwavidyalaya, Sector -15, Gandhinagar*

Abstract: ***With the technological advancements, new approaches are being adopted for the cyber crimes. There is a notion that, virtual environment does not leave traces of network attacks performed over it and secondly, the area of virtualization is presently less explored. Hence, networking in virtual environment is considered as the most secure means to escape conviction of cyber crimes. Cyber criminals are using this technology to maintain anonymity over World Wide Web and hence, misguide the process of digital investigations. Thus, the cyber criminals escape from the conviction. Network Packet Sniffing is done over the host system, while the attack is being performed from virtual environment. Further, the removal of virtual machine from the host system affects the direct evidences and artifacts of networks. However, traces of virtual machines can be obtained from the RAM Dump taken from the host machines. This paper is a step towards devising a novel technique to identify the attacks that are performed in a network through sniffing and analysis over the system.***

Keywords: Virtualization, Content Monitoring, Investigation, RAM Dump, Packet Sniffing, Cyber Crime, Network Attacks, Forensics

I. INTRODUCTION

The virtualization technology is being widely used across the world for optimum utilization of hardware and software resources, efficiency, security, economy, compactness, compatibility etc. This technology has redefined the networking over the World Wide Web (www). There is a notion that virtual environment does not leave traces of network attack footprints. Hence, cyber criminals are using virtual environment to attack networks, as it is considered most secure means to escape conviction. In this paper, the investigation of anonymous attacks in a virtual environment has been analyzed using the approach of network packet sniffing over the host system.

II. BACKGROUND STUDY

A. Virtualization Technology

In the virtualization technology, the virtualization solution is installed on the host operating system (OS) of the physical machine or it can be directly installed on the bare metal. Different or same OS can be installed on the virtual machine(s) and as per user requirement; various applications can be run on these VMs. For the virtualization to happen, a hypervisor is used. The hypervisor controls how access to a computer's processors and memory is shared. A hypervisor or virtual machine monitor (VMM) is a virtualization platform that provides more than one OS to run on a host computer at the same time.[1] The VMs are allocated virtual memory, disk space etc and they behave as virtually independent systems. This technology provides optimum utilization of physical resources on the base system and provides adequate resources to the applications on the VMs, hence provide economy and efficiency. The virtualization technology helps to overcome compatibility issues of the applications with the base system OS.

Solutions have a separate management application to manage the VMs on the host system. Hence, it is evident that lot of internal communication takes place for this system to work as per user requirement.
VMware, Citrix Xen, Microsoft HyperV etc are the virtualization solutions available in the market. Though the basic functionality of these virtualization solutions is the same as stated above, however, their installation, configuration, management, compatibility etc will vary.

B. Virtual Machine Networking

The VMs should be able to interface with i/p and o/p devices, provide responsive user interaction and simulate dynamic environment. A VM can have approximately four network adapters enabled, each of which can be configured to use different types of networking. VMs can communicate among themselves within the host system. VMs can communicate in the "bridged mode",

where it uses the physical network adapter to connect the VM to a physical TCP/IP based network as a separate computer. In bridged network, VM uses a device driver on the host system that filters data from the physical network adapter. The new network interface is created in software. In shared network, the first network adapter in the VM can use this option. Here, VM is not listed as a separate computer on the network.

A VM with Network Address Translation (NAT) enabled, acts like a real computer that connects to the internet through a router. The "router" is the virtual box networking engine, which maps traffic from and to the VM transparently. In virtual box, the router is placed between VM and the host. This separation enhances security, since by default the VM cannot talk to each other. The network frames sent out by the guest OS are received by the virtual box's NAT engine, which extracts TCP/ IP and resends it using the host OS. To an application on the host, it appears that the data was sent by the virtual box application on the host, using the IP address belonging to the host. Virtual box listens for replies to the packets sent and repacks and resends them to the guest machine. The VM receives its network address and configuration on the private network from DHCP server integrated into virtual box. The IP address assigned to the VM is usually a completely different network than the host [2].

C. Virtualization Platform for Cyber Crimes and the Network Artifacts

There is a notion that virtual environment does not leave traces of network attacks performed over it and this field is presently less explored. Hence, this emerging technology is being used by cyber criminals to evade the investigations and convictions.

Network Artifacts means the traces which can be found or gathered from the Electronic devices which sends and receives over the network data. This can be from the registries, packets captured network logs from event and log viewer. Network artifacts in the form of DNS details, IP and MAC address login, Net Protocols, network list details, NIC or virtual network cards, NIC configuration details and work station details are considered as necessary inputs for clarity on network traffic monitoring and analysis.

Cyber criminals can use various permutations of physical hardware, OS, virtualization solution etc, hence, it is necessary to find the traces and evidences for the activities.

D. Investigations in Virtualization Environment

There are some situations, where it would be useful to boot up a suspect computer, an action that is counter to all investigation best practices. One solution is to boot the suspect system into a VM from the suspect computer's image files. In this way, the examiner can see exactly what a user would see on the suspect computer without even actually touching (or possibly altering) the suspect computer. Live View is one such tool that can create a VMware virtual machine from raw (dd) image files [3].

E. Packet Sniffing and Analysis on Virtualization Platform

Packet sniffing allows individuals to capture data as it is transmitted over a network. Packet sniffer programs are commonly used by network professionals to help diagnose network issues and are also used by malicious users to capture unencrypted data like passwords and usernames in network traffic. Once this information is captured, the user can then gain access to the system or network [4] .Pcap (packet capture) consists of an application programming interface (API) for capturing network traffic over the networking protocols.

The first thing for packet capture is to determine the best location to set up the sniffer. In virtual environment, things get complicated since there is no physical spot from where the packets can be picked up from a single VM. The packets are sniffed from v Switch, which is set in promiscuous mode. Port groups are used to partition vSwitch. Packet sniffing allows individuals to capture data as it is transmitted over the network. This raw data can be used to gain information about the communication artifacts and pattern. With virtualization, the network functioning has been decoupled from the physical connectivity at the hardware substrate. [5]

In this paper, attack scenarios have been visualized for the lab set up. Data capture is done using packet sniffing tool.

III. METHODOLOGIES

A. Scenario Setup

Scenario 1: Obtained the credentials of the site which was opened in Virtual Machine on the base system through packet capturing tool.

Scenario 2: Obtained all the user details including credentials in packet capturing tool.

Scenario 3: Obtained the details of mail sent, to and subject with attachment details.

Scenario 4: Obtained credentials from the RAM Dump.

Scenario 5: Obtained Credentials from the .ad1 Image file of the virtual environment.
Scenario 6: The evidences have been obtained of the use of Virtual Environment.

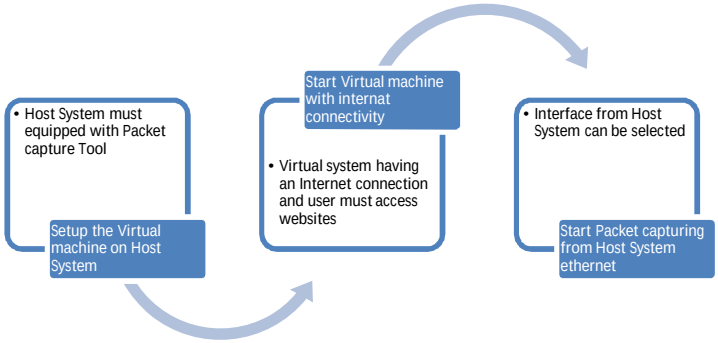


Fig 1. Checklist for Virtual Machine Packet Analysis

IV. TO SIMULATE THE REAL TIME SCENARIO FOLLOWING TOOLS CAN BE UTILIZED

A. Virtual Environment

Virtualization Environment allows multiple operating system instances to run concurrently on a single host system i.e. computer; that means it separates hardware from a single operating system. Each "guest" Operating System is managed by a hypervisor, also known as a Virtual Machine Monitor (VMM). Because the virtualization system sits between the guest and the hardware, it can control the guests' use of CPU, memory, and storage, even allowing a guest OS to migrate from one machine to another.[6] It supports almost every Operating system like Windows, Linux and UNIX flavors.

B. Concepts on Investigation in Virtual Environment

Virtual Environment is used by criminals to hide their tracks and records of network activities. There are mainly following two methods to investigate criminal tracks in Virtual Environment.

C. Investigations of Virtualization Environment

There are some situations in which virtual environment are used to do crime. So, it is necessary to find out the traces and evidences for the same. Obtaining the traces and evidences of virtual environment is a difficult task.

D. Investigations in Virtualization Environment

There are some situations where it would be useful to actually boot up a suspect computer, an action that is counter to all digital forensics best practices. One solution is to boot the suspect system into a VM from the suspect computer's image files.[10] In this way, the examiner can see exactly what a user would see on the suspect computer without even actually touching (or possibly altering) the suspect computer. Live View is one such tool that can create a VMware virtual machine from raw (dd) image files [7].

V. METHODOLOGIES ADOPTED TO IMPLEMENT SCENARIOS

A. Scenario 1: Obtained the credentials of the site which was opened in Virtual Machine on base system through packet capturing tool.

In this scenario, opening the email account in the virtual environment and capturing the packets on the base system with the help of packet sniffer tool. While analyzing the packets on base system, we get the details of the account or the user details in the browser of the virtual machine which was browsed.

B. Scenario 2: Obtained all the user details including credentials in packet capturing tool.

In this scenario, the detail of email account that was opened in browser in virtual environment on the base system running network packet capture was found.

C. Scenario 3: Obtained the details of mail sent, to and subject with attachment details.

In this scenario, we would be able to trace the mail that is sent from one email account to another email account with the contents like subject, mail recipient, body of the mail and attachments with the help of deeply analyzing network packets in network sniffing tools.

D. Scenario 4: Obtained Credentials from the forensic imaging of the virtual environment.

In this scenario, the forensic image is acquired from the virtual environment by using the imager tool. By analyzing the forensic image investigator, we can extract the credentials of the user of various social networks, email account and other network content related artifacts.

E. Scenario 5: The evidences have been obtained of the use of Virtual Environment.

In this scenario, all the possible places from where we can get the network events as well as the proof that the virtual machine was used on the system are obtained. Going through the analysis details of the IP addresses, MAC address and many more network related details are obtained.

VI. RESULTS OBTAINED FROM INVESTIGATION SCENARIO

To investigate the content accessed on the guest system, the host system Network Interface Card can be select to gather the details of activity performed over guest system.[11] Because the network packet flow will pass through the NIC card, so content monitoring can be done at host system level.

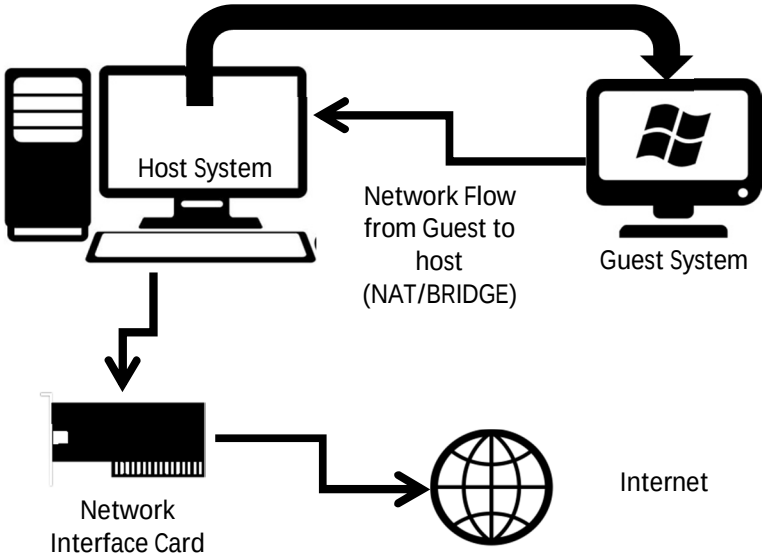


Fig 2. How Guest System Communicate over Internet [11]

The packet capture tool can be setup and capture the packets on host system, while activity happens over guest system.

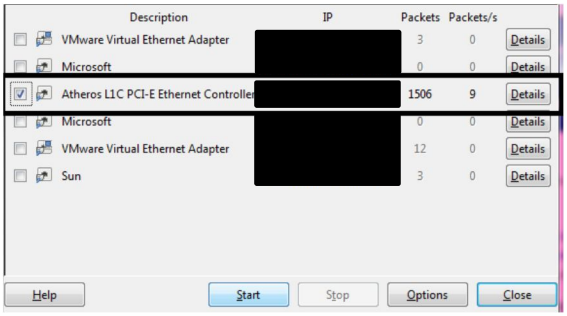


Fig 3. Selecting Interface in Packet Capture Tool

A. Email Account Accessed via Guest System

An email account is created on guest system and some activity is done over the guest system. During this activity, packet capture tool is activated on the host system and some activity is performed in the guest system.

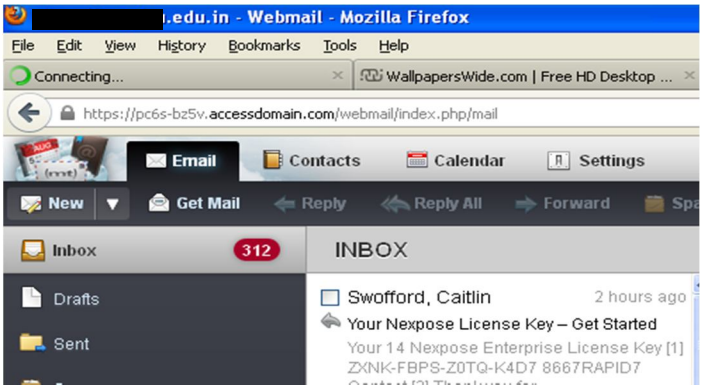


Fig 4. Email Activity from Guest System

Such packets are analyzed thereafter from packet capture file i.e. .pcap file. All network activity done over guest system is identified form the artifact collected in host system.

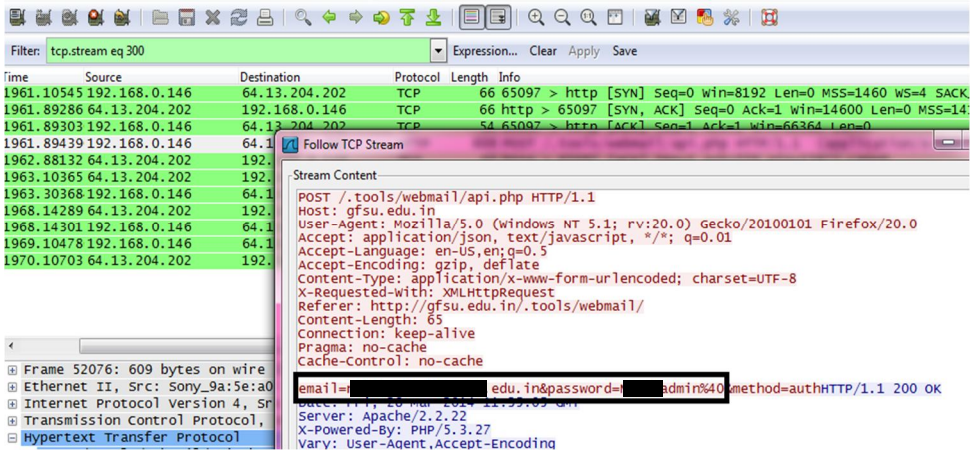


Fig 5. Credential Reveled by the Packet Capture Tool

B. Email Account setup on known Secure Socket Layer (SSL/HTTPS) Certified email Services:

On the virtual environment, two separate accounts are setup with different account details. The packets are captured from host system Network Interface Card.

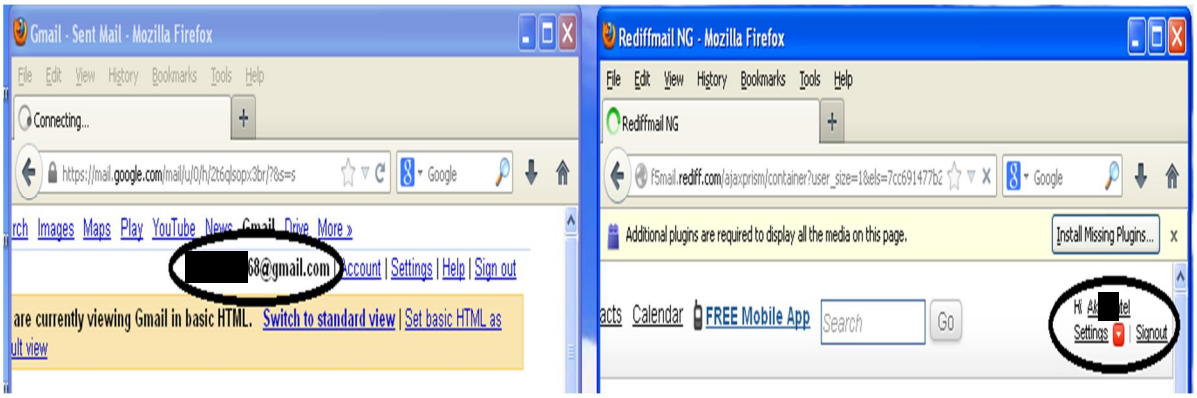


Fig 6. Email Account Registered on the Guest System

The artifacts of each activity are identified from the packet capture analysis tool using -follow the TCP stream. The network contents like login username, password, registered mobile number and city are obtained from packets capture file.

Fig 7. Registration Details Identified from the Host System using Content Analysis

C. Using Forensic Imaging of the Virtual Environment, Content can be Analyzed:

Above mentioned activities were performed on the Virtual Environment. Now to remain anonymous, suspect can remove the traces by cleaning the virtual system artifacts from the host system. Suspect also clears the entire packet capture files from the host system to maintain anonymity. Still the investigator can identify the suspect and activity performed over guest system using forensic imaging of the host system.

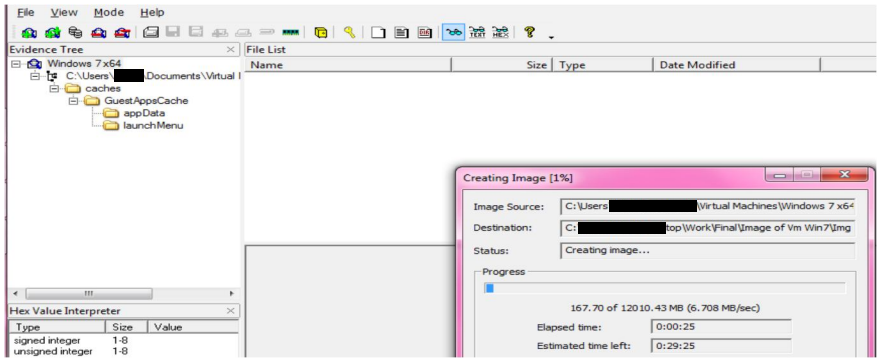


Fig 8. Forensic Imaging of the Host System

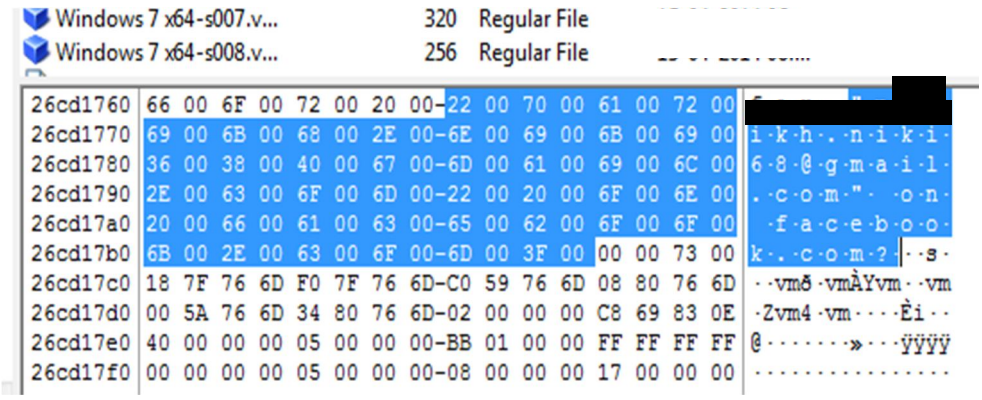


Fig 9. Email Account Artifacts Analyzed form Virtual Machine Disk File

VII. CONCLUSION

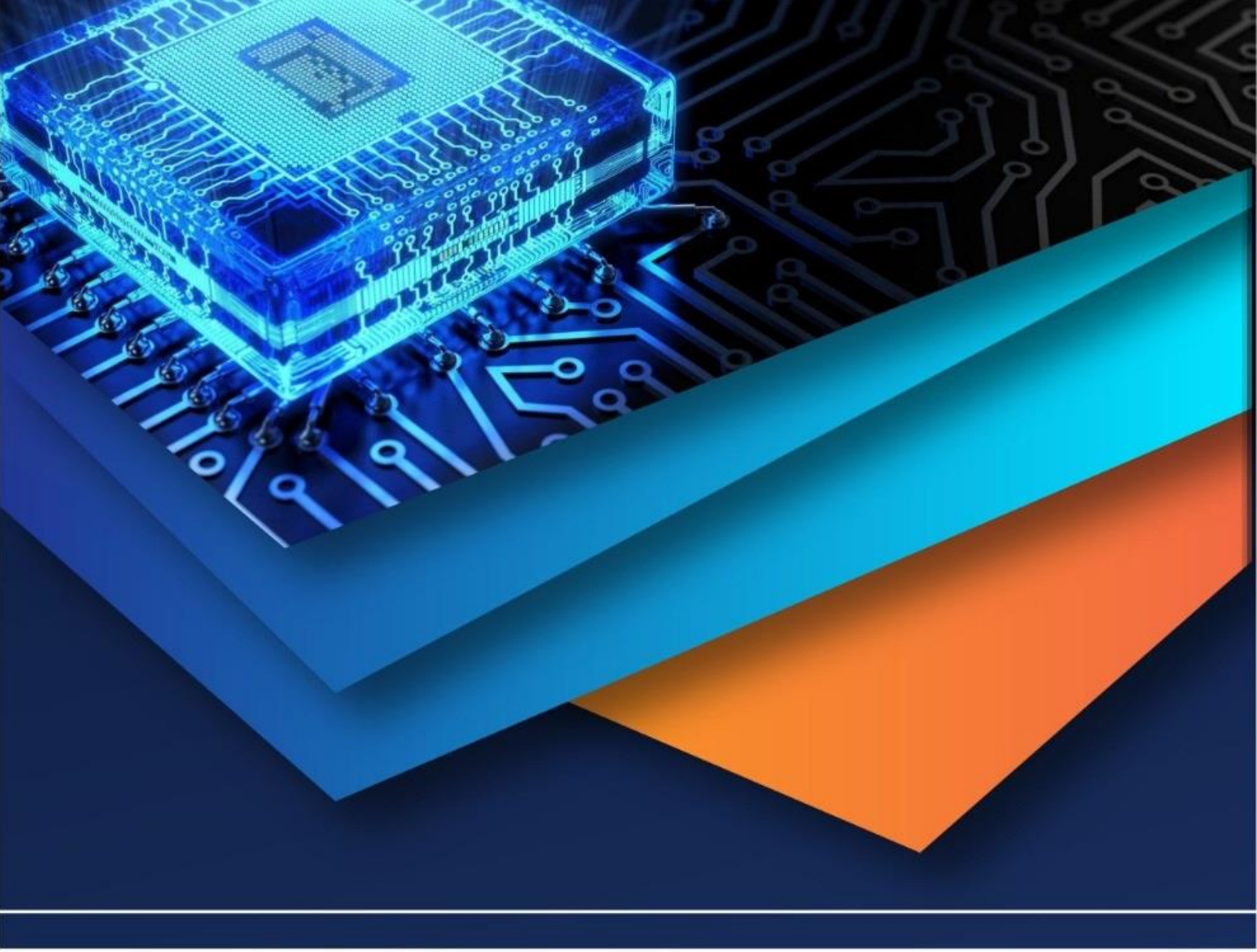
After executing all the scenarios over host system and guest system over network, it can be concluded that analysis of the packets captured on virtual operating system of the host machine can be done using network content analysis. Investigator can obtain details of user registration, email accessed, browsing details and sessions. The credentials of the user can be obtained by analyzing captured packet; RAM dump analysis and Image file analysis. Criminals often use virtual environment to remain anonymous over the internet or network, but using the above investigation methods, an investigator can identify the potential artifacts from the system.

VIII. FUTURE WORK

In future, the work can be extended to developing more scenarios with more number of virtual environments. Also, effort can be done to install virtual environment using multiple operating systems and try different attack scenarios. The anonymous browsers and third party applications like The Onion Router and Virtual Private Network related content analysis can be investigated.

REFERENCES

[1] Manjaiah, D.H. and Hemdan, E.E.D., 2012. Digital Forensics in Virtual Environments. Cover Story, p.12.
[2] Herpich, F., Nunes, F.B., Voss, G.B. and Medina, R.D., 2016. Three-Dimensional Virtual Environment and NPC: A Perspective about Intelligent Agents Ubiquitous. In Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning (pp. 510-536). IGI Global.
[3] Esendemirli, E., Turker, D. and Altuntas, C., 2015. An Analysis of Interdepartmental Relations in Enterprise Resource Planning Implementation: A Social Capital Perspective. International Journal of Enterprise Information Systems (IJEIS), 11(3), pp.27-51.
[4] Ko, A.C. and Zaw, W.T., 2015. Digital Forensic Investigation of Dropbox Cloud Storage Service. Network Security and Communication Engineering (Ed: Kennis Chan), CRC Press: İngiltere, pp.147-150.
[5] VMware. (2015, October 30). Configuring Hard Disk Sotrage in a Virtual Machine. Retrieved from VMWare: https://www.vmware.com/support/ws45/doc/disks_config_ws.html
[6] VMware. (2015, November 1). Defragmenting, shrinking, and cleaning up VMware Fusion virtual machine disks. Retrieved from VMware Knowledge Base: http://kb.vmware.com/ selfservice/microsites/search.do?language=en_US&cmd=displayK C&externalId=1001934
[7] Splunk Enterprise. (2015, November 1). Splunk documentation: Anonymizing data samples. Retrieved from Splunk.com: http://docs.splunk.com/Documentation/Splunk/6.2.0/Troubleshooting/ Anonymizedatasa mplestosendtoSupport
[8] The Sleuth Kit. Autopsy. Available online: http://www.sleuthkit.org/autopsy/ (accessed on 12 November 2015).
[9] Xiao, J., Lu, L., Wang, H. and Zhu, X., 2016, July. HyperLink: Virtual Machine Introspection and Memory Forensic Analysis without Kernel Source Code. In Autonomic Computing (ICAC), 2016 IEEE International Conference on (pp. 127-136). IEEE.
[10]Geddes, M. and Zadeh, P.B., 2016, June. Forensic analysis of private browsing. In Cyber Security And Protection Of Digital Services (Cyber Security), 2016 International Conference On (pp. 1-2). IEEE.
[11]Cochran, J., MICROSOFT TECHNOLOGY LICENSING, LLC, 2016. HYPERVISOR-HOSTED VIRTUAL MACHINE FORENSICS. U.S. Patent 20,160,034,295.
[12]Ren, J., Liu, L., Zhang, D., Zhou, H. and Zhang, Q., 2016, June. ESI-Cloud: Extending Virtual Machine Introspection for Integrating Multiple Security Services. In Services Computing (SCC), 2016 IEEE International Conference on (pp. 804-807). IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY