iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** XII **Month of publication:** December 2018

DOI:

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 XII, Dec 2018- Available at www.ijraset.com

Assailable Multiple-NIC Node Detection and Integrity Verification Solution (AMDIVS)

C Pradeep[1], K Mounika[2], ANSV Murali Krishna[3], SVSRK Kishore[4], C C Reddy[5]
[1, 2, 3, 4, 5]*NRSC/ISRO, Hyderabad.*

Abstract: ***The configuration of Multiple Network Interface cards on nodes can enhance Network operations such as load balancing, increased transmission capability and redundancy. On the other-hand such network configurations may bring potential cyber-attacks that can devastate your entire network. This attack is highly possible when two interfaces on the same node are connected to different network segments which are enabled at the same instance. This paper demonstrates a software tool that detects Nodes having the configuration of Multiple Network interface cards in a large Adhoc network using an agent which is a default feature available on Windows Operating System. For this demonstration, a batch file is instantiated to launch a trigger to the agent in each client node and get the Network information on from them. Then, the collected information will be used to create alerts in the Monitoring frame of the software tool. This work highlights the importance of system and network security and ensures the prevention of cyber-attacks over the organization's private network.***

I. INTRODUCTION

Every minute, there are new brands of cyber-attacks reported on the Internet consumers; these targeted attacks are carried out on computer nodes that violate the cyber security policies. All over the Global enterprise setup computers are considered as an important part of network systems, since they are used to process, store and widely to transmit data.

Therefore, the speed of data transmission directly relates to the system performance. With the advancement of digital technology, more and more improved features and advantages has been incorporated in the computer system to aid better performance. Analyzing, one such feature in networking which will be an advantage if configured properly and a biggest threat if not configured properly. Yes, it's the Ethernet Network adapter; nowadays it has become more common to have Multiple Ethernet adapters in a single workstation and embedded Ethernet controller in servers. It is the primary responsibility of an administrator to ensure that proper network configurations are implemented on such systems. This will avoid connectivity problems and reduce the space for security breaches in the network. But practically, it's high time for the administrators to manually monitor the true status of individual system every time. While preventing the network card from tampering with the operating system is possible using existing mechanisms, having a compromised network card remains a real problem, not only because the network card is a critical component from the security perspective, but also because a compromised device can be used to compromise surrounding computers and thereby will affect entire the network. Since, these attacks represent a real threat considering the privilege level an attacker might gain in successfully exploiting the underlying vulnerabilities of the Network interface card. Moreover, we believe that studying a detection approach (as opposed to a prevention one) is relevant, as the vulnerabilities can be caused by a component that reside in the system and can be completely under administrative control.

All possible countermeasures were considered, but none of them seemed really convincing. The best way to prevent a network from being compromised would probably a formal verification on the system information are true and correct. Systems that require external communication are susceptible to volatile security breaches. For instance, as early as the twentieth century, the most of the hackers intercept network information to operate their attacks over the network listening ports as they are more vulnerable.

This grade of cyber-attack was used to keep the Network administration & cyber-security team informed of possible danger to their network. The attacks performed in the mock drills shows how easy it is to infiltrate a network system that is not constantly monitored. It is very much possible for the attacker to take full control of a computer by exploiting vulnerability in the network adapter. The attacker gains full control of the adapter and can add a contaminant backdoor in the OS kernel using DMA accesses. The vulnerability becomes unconditionally exploitable when the ASF functionality was enabled on the network card to any attacker who would be able to send UDP packets to the victims in the network. The solution for this problem is based on the detection and aiming at instant blocking of attacks against the target network node, also maintaining good performance and virtually avoids false positives. In this paper, we propose a pragmatic design approach to detect workstations and servers with multiple Ethernet network adapters, where the monitoring agent is located as a default part of the windows operating system itself.

The agent that is being used here is the "WINDOWS RESOURCE TOOL KIT" that contains options that can support administrators in the categories of desktop management, performance management, server management, internet services and registry management. Depending on the Network interface configuration and the host operating system, building an efficient detection framework is possible. We explain the choices we made when designing such a framework that we called AMDIVS and give details on our proof of concept implementation. Our contribution in designing the framework is explained under twofold.

First, we actively scan the nodes devices with Multiple Network Interfaces and their network segment configuration by illustrating the effectiveness of an attack against a network device. Second, we provide a solution to this problem in the form of an anomaly identification system called AMDIVS (Assailable Multi-Network Node Detection and Integrity Verification Solution) by using an Agent that sits on the client windows operating system. The oncoming sections in this paper summarizes the above two points into detailed explanations, in section 1, Examples of possible attacks on a network card and its implications with respect to system and network security. Section 2, explains the Client Scanner Agent and their functionality. Then, we present the assumptions for our work in section 3; Section 4 illustrates the architecture and operations of our software tool and presents experimental results on the test setup.

II. ATTACK METHODS AND IMPLICATIONS ON SECURITY

While considering the system vulnerabilities, hardware certainly seems to be a target that can be exploited easily, new class of attacks have emerged that can specifically target network cards and compromise them.

The following are the possible attacks that an attacker can exploit by executing an arbitrary code on the available Network adapters

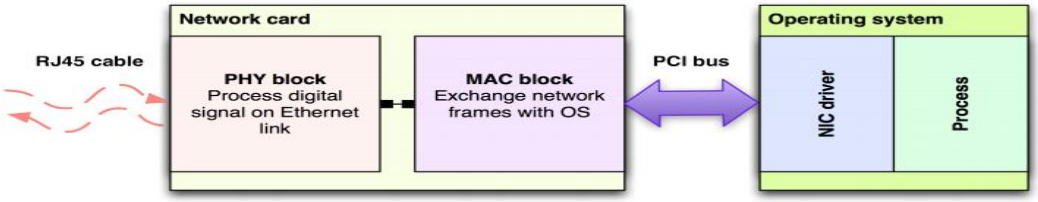


Fig.1. NIC card blocks shows flow of raw data to MAC block, also have access to registers, processes and volatile and EEPROM memory through PCI bus.

A. Firmware Corruption

A more insidious attack, attacker replaces the firmware code with new code, thereby reprogramming the device to do whatever he deserves. One scenario goes like this, writing a firewall bypass engine for the firewalls that works on PC-based environments: just overwrite the firmware in NICs of the participating PCs and then perform PCI-to-PCI transfers between the two NIC cards for suitably formulated IP packets.

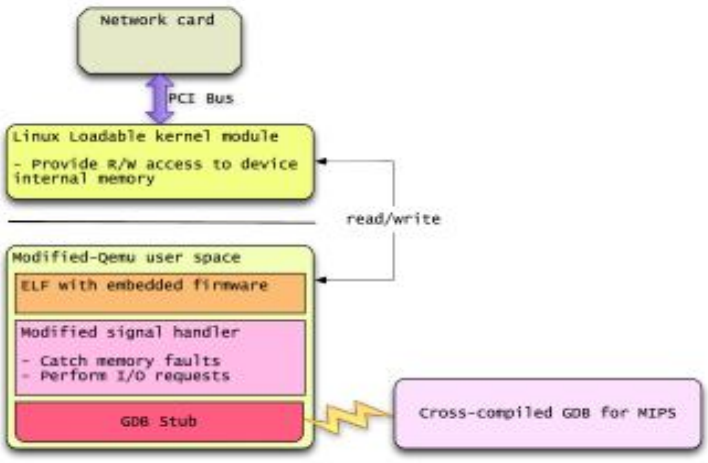


Fig.2. Network Interface card firmware corruption by cross compiled

Re-programming NIC card even read and write the main memory of the host system. This will allow sensitive information leak from the compromised node.

B. ARP/ DNS Cache Poisoning

ARP cache poisoning can be crafted with a single valid ARP reply in which any IP is mapped to any MAC address of the hacker's choice and can send this message to the complete network.

All the devices on network will accept this message and will update their ARP table with new information and this way the hacker can gain control of communication from any host in network.

DNS cache poisoning redirects the nameserver of another domain unrelated to the original request to an IP address specified by the attacker. These attacks are carried out at layer-4 of the OSI model; therefore the attack is possible on network switches, routers, hubs other than the computer nodes.

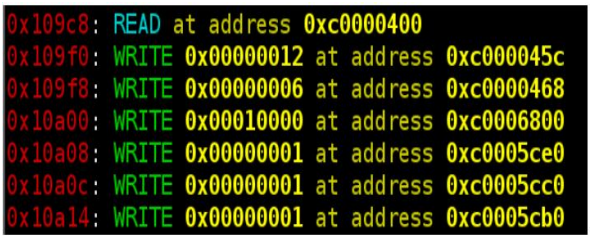


Fig.3. Show the hacker is able to get the internal memory access trace of a compromise host

C. Routing Attacks

Distance Vector routing that can announce 0 distances to all other nodes and creates Black-hole traffic & Eavesdrop messages.

Link State Routing that is capable of dropping links randomly and the can claim direct link to any other routers.

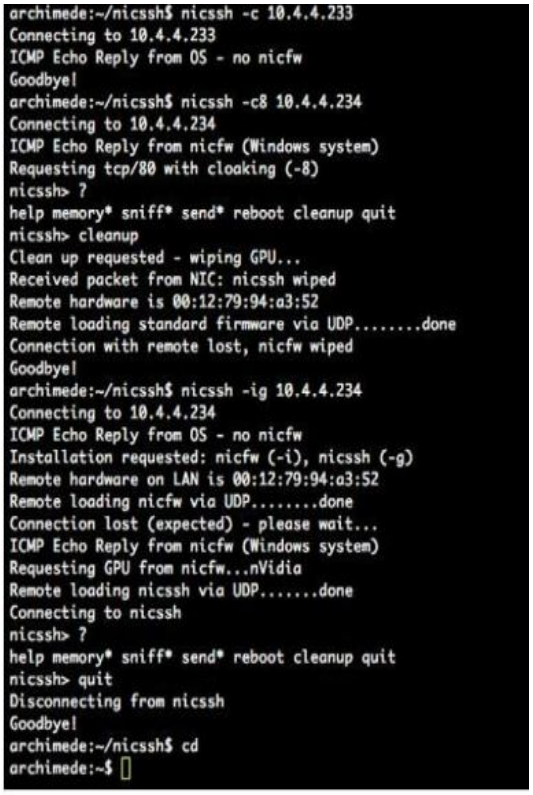


Fig.4. Rootkit attack on NIC and gained SSH to the host

III. AGENT COMMANDS - WINDOWS RESOURCE TOOL KIT

Generally, client agents are separate software packages installed on network computers to operate as per the instructions of the server instructions. In our project default features of Windows OS i.e., Windows Resource Tool Kits will work as a scanner to collect the required information.

The Resource tool kit is a group of supplementary resources that can offer technical guidance to administrators in management tasks, configuring networking and security features, and automating application deployment, maintenance and support in troubleshooting issues.

There are 126 services and commands available with this resource kit, since this paper focus on the network information, therefore the required features are explained here

1) *Chknic.Exe: (Information Collection agent)* Checks all network adapters on the local machine and makes sure they are compatible for network load balancing. The command will execute and collect all the available Network interface card information irrespective of their availability status i.e., enable / disable state. It works only with the minimum requirement that system should be powered on and connected to the monitoring network segment.
2) *Srvany.Exe:* (*Agent Installer*) allows Chknic.exe application to run as a service. To run this as a service proper configuration should be done in the registry path, so that the service may point to Srvany.exe. If the path is not set properly the service may stop shortly after it starts and returns an Event ID with "The service name failed to start". Always specify the full drive path to make the application executable including the extension.
3) *Fcopy.Exe:* (*File copy*) facilitates copying of files across LANs and WANs. Basically, it is a multi-server file copy tool that compresses files and folders and continues copying them using message queuing even if there are some network problems. It does not need a restart even after a network breakdown, since the message queuing handles the entire content delivery to destination.

You will have physically connected the two networks, and you cannot completely trust that PC to keep the security standard. If the PC is compromised over one network, it would then have access to the other. I would rather trust a security device, such as a router or firewall to do this role, as they are more designed for the case. They can still have their vulnerabilities, but are more designed for this role. You could create an appropriate security policy on that device and still only have one NIC in that computer. Then again, if that computer is directly compromised, the door is still open for access to both networks.

IV. ASSUMPTIONS FOR WORK

Generally, in the practical existence there is rarely a good reason to use multiple NICs on the same subnet. In our scenario, we are considering a case where the dual NIC ports are connected to two different networks, in this setup, we have a technical challenge while attempting to send packets over a communication channel; many-a-times operating systems can handle this kind of situation gracefully while most others may attempt to send packets mistakenly through the wrong interface.

The above said problem may be taken in little lighter sense when we consider that of Cyber security issue which a taunting problem when considered globally.

Let us get into the case with the below assumptions, though we assume, these are scenarios that are practically faced by network administrators in their day to day work environment.

A host computer is connected to both a corporate / private network (via NIC#1) which is connected to the company's secured i.e., business network and Internet is accessed (via NIC#2). This is a favorable condition for the hackers, malware, and virus to come into the business network and do whatever is their intension to do with the network, few examples of cybersecurity attacks are explained in section 2.

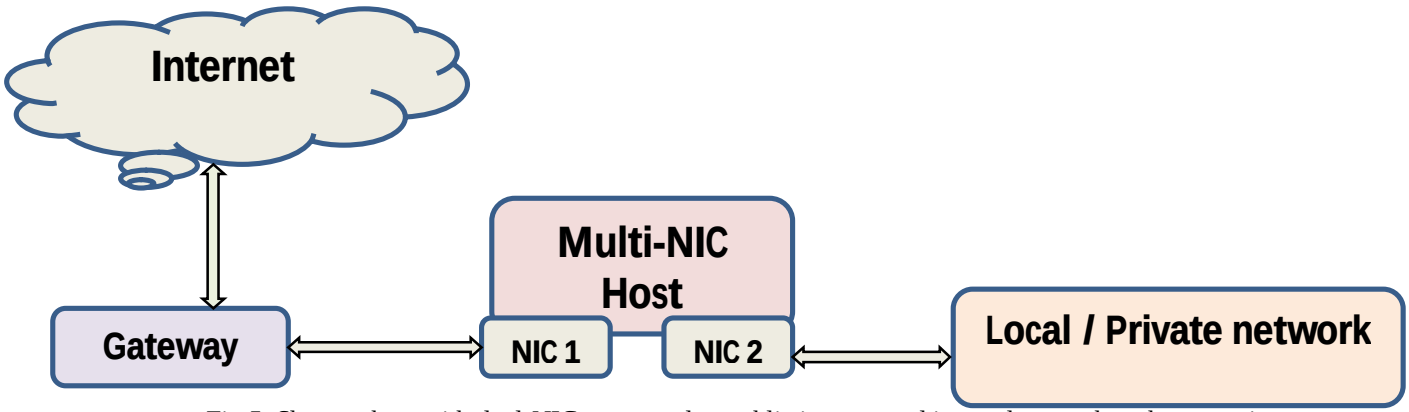


Fig.5. Shows a host with dual-NIC connected to public internet and internal network at the same time.

If consider a company with more business values and associated IT resources managing them are the biggest responsibility of the administrators to handle so many systems with data transferring network capabilities, it is even one step more for them to safeguard the resources along with the business data.At this juncture having a network host as explained in the above scenario is very much possible and finding each and every such system is really a tough task. Therefore, we have proposed a novel idea to find those probably vulnerable systems using a self-developed monitoring tool. This tool can give you scan reports on the entire network on your screen at a single shot.

V. AMDIVS – COMPONENTS AND OPERATIONAL MECHANISM

This software application designed to probe hosts in the LAN to find out for all available network hardware installed on the hosts. This is proposed as a designed to be used by administrators to verify security policies of their networks and to identify any attack services running on a host with the view to compromise it.

1) *Scanner:* The scanning agent or the scanning component is implemented using the broker pattern, which mediate and route information in between the executor agent on the server and the message collector which runs on the host client. The scanning component has a well-defined abstract; it knows about what information is being collected. Information is gathered and handed over to the executor about each selected host by the administrator.
2) *Executor:* The executor is a server side program that initiates a the scan to get the list of all known IP address in the network, after which it triggers the typical collector agent program to the list of hosts and to run the collector program locally in each hosts and waits for the entire list to complete the trip.
3) *Collector:* This agent which is a default command set of the Windows operating system which will be started by the executor program command to get the report on the host network details, port details and more associated information. The collector stores the information report on the local host which will be gathered by the copy program that is run by the orchestrator once the entire scan is done
4) *Orchestrator:* The orchestrator is a special program that checks for the messages from each host present in the scan list and sends a copy program to collect the information to the centralized server where the executor program is initiated. Then the orchestrator will insert the received information into the database. The information will be displayed with a query triggered on the database via sophisticated GUI module.
5) *GUI (Graphical User Interface):* The front-end of this application that helps us to query the required information from the database and display them in a graphically viewable mode. This GUI is also able to alert any mismatches or updates on information that is inserted or altered in the database. This will provide the general monitoring display window of all the clients and drill-down details of the selected host from the client list.

A. *Operational Mechanism*

The scanner sends a scan probe to the input IP address range in the LAN and gets the list client host in the network.
The Executor collects the IP list and sends trigger to all the collector agents in the input host list.
The collector agent runs locally to collects the information and writes it to the text file and send acknowledgement to the executor.
The executor receives acknowledgement from the input host list and the hands over the control to the orchestrator.
The orchestrator collects the information from the host list given by the executor which is available with the collector agent on each host. The orchestrator segregates the information and inserts them in the database which will be later formatted to be displayed in GUI The GUI displays the query of the administrator or application operation by fetching the data from the application database.
Deployment methods of AMDIVS do not require any complex installations and can be easily copied and run on any host anywhere in the network. The collector agent program can be copied through USB memory sticks and then just plug them in order to do a quick run and store the results on the same memory stick. AMDIVS does not employ third-party installers; it only uses commands which are common on Windows platforms.

VI. CONCLUSION AND RECOMMENDATIONS

When considering the possibilities of developing a simple application for this particular aspect of monitoring Multiple-NIC card host in the network, there are not many. Writing code in conceptual computer programming languages such as C++, java may not be very difficult. A combinational collection of many utilities such as IP scan, MAC scan, host ID, ports open and derivatives of all these can further help in analyzing the network, host security mechanisms and aid us in building a rigid cyber-secure model for the enterprise class organisations. Thus, AMDIVS provides a common monitoring solution to three major incidences like attack, defense and maintenance.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XII, Dec 2018- Available at www.ijraset.com

VII. DIRECTIONS OF FUTURE WORK

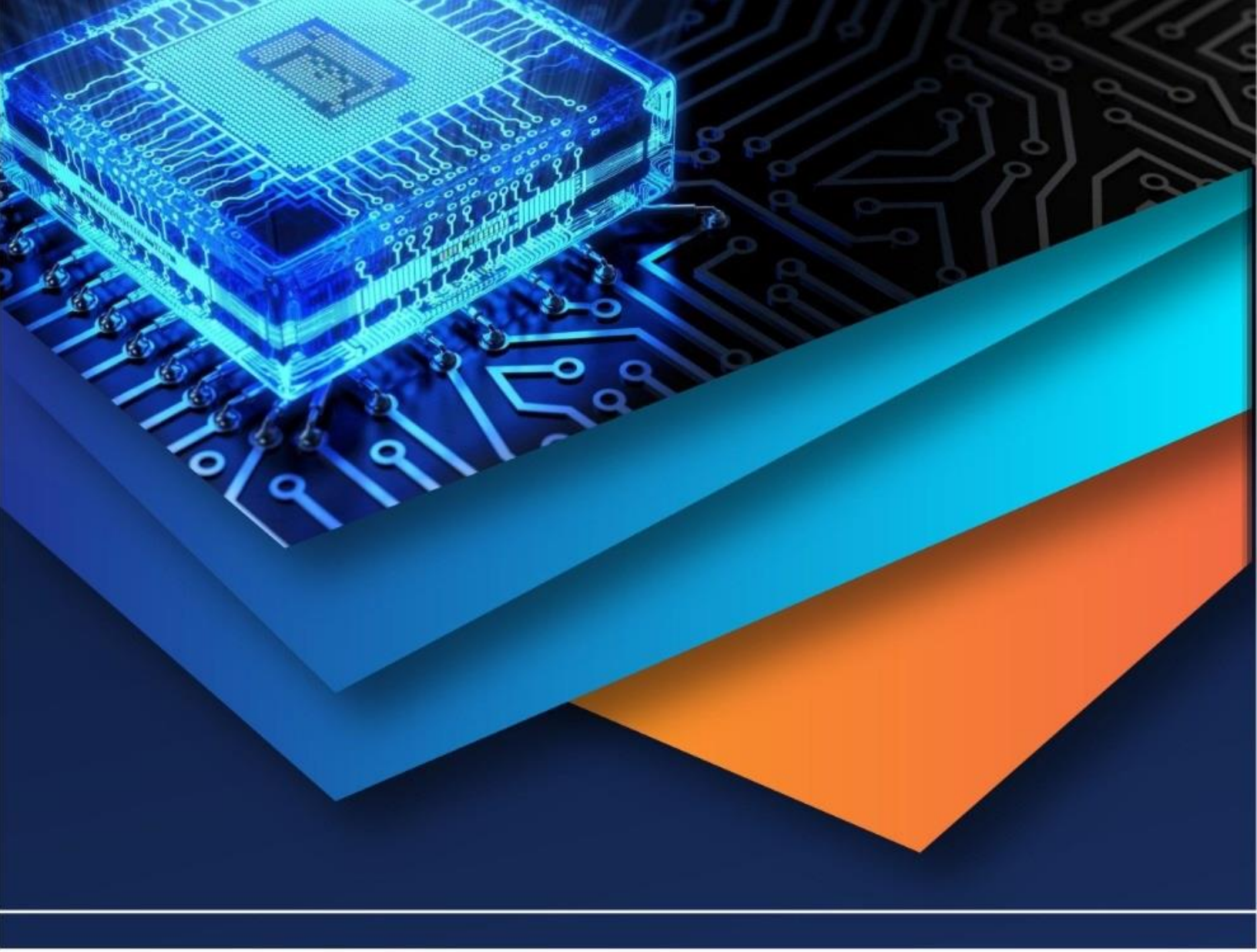
For future work, we can evaluate a plan to extend this application tool into WAN and mechanism to scan unix flour operating systems.

VIII. ACKNOWLEDGEMENT

The authors would like to thank the General Manager, CSNVF for giving us an opportunity to work on this application to bring out this idea. The authors would also like to acknowledge the internal users of networks services for their critical reviews to improve the cybersecurity mechanism to meet the purpose of secured assets and networks.

REFERENCES

[1] Cybersecurity issues; Data quest technical magazines.
[2] http://esec-lab.sogeti.com/static/publications/10-hack.lu-nicreverse_slides.pdf
[3] http://javacodex.com/
[4] https://en.wikipedia.org/wiki/Software_construction
[5] https://cryptome.org/2014/02/nic-ssh-rootkit.htm
[6] https://www.manageengine.com/products/desktop-central/desktop-management-challenges-education-vertical.html



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY