I.J. Information Technology and Computer Science, **2020, 5, 38-51**
Published Online October 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2020.05.03

A Remote Access Security Model based on Vulnerability Management

Samuel Ndichu
School of Computing and Informatics, Maseno University, Private Bag, Maseno, Kenya
E-mail: ndichu.ranji@ gmail.com

Sylvester McOyowo, and Henry Okoyo
School of Computing and Informatics, Maseno University, Private Bag, Maseno, Kenya
E-mail: oyowosilver@ gmail.com; okoyo.ho@ gmail.com

Cyrus Wekesa
School of Engineering, University of Eldoret, Eldoret, Kenya
E-mail: cyrus.wekesa@ gmail.com

Received: 05 March 2020; Accepted: 16 March 2020; Published: 08 October 2020

Abstract: Information security threats exploit vulnerabilities in communication networks. Remote access vulnerabilities are evident from the point of communication initialization following the communication channel to data or resources being accessed. These threats differ depending on the type of device used to procure remote access. One kind of these remote access devices can be considered as safe as the organization probably issues it to provide for remote access. The other type is risky and unsafe, as they are beyond the organization's control and monitoring. The myriad of devices is, however, a necessary evil, be it employees on public networks like cyber cafes, wireless networks, vendors support, or telecommuting. Virtual Private Network (VPN) securely connects a remote user or device to an internal or private network using the internet and other public networks. However, this conventional remote access security approach has several vulnerabilities, which can take advantage of encryption. The significant threats are malware, botnets, and Distributed Denial of Service (DDoS). Because of the nature of a VPN, encryption will prevent traditional security devices such as a firewall, Intrusion Detection System (IDS), and antivirus software from detecting compromised traffic. These vulnerabilities have been exploited over time by attackers using evasive techniques to avoid detection leading to costly security breaches and compromises. We highlight numerous shortcomings for several conventional approaches to remote access security. We then adopt network tiers to facilitate vulnerability management (VM) in remote access domains. We perform regular traffic simulation using Network Security Simulator (NeSSi2) to set bandwidth baseline and use this as a benchmark to investigate malware spreading capabilities and DDoS attacks by continuous flooding in remote access. Finally, we propose a novel approach to remote access security by passive learning of packet capture file features using machine learning and classification using a classifier model.

Index Terms: VPN, DMZ, malware, DDoS attack, encrypted traffic, vulnerability management, machine learning.

1. Introduction

Data and information transmitted through the internet are fast, easy, and cheap. However, this mode of communication and access through public networks is prone to all kinds of security threats, which exploit vulnerabilities in communication networks. In remote access, vulnerabilities are evident from the point of communication initialization following the communication channel to the resources being accessed. The threats differ depending on the type of device being used to procure remote access. One kind of remote access devices can be considered as safe as the organization provisioning probably issues it for remote access. Hence, the organization ensures the installation of updates and patches that secures the device, and other security software's and other controls deemed necessary as per the issuing organization's security policy. The remote access devices are referred to as managed remote access devices. The other type of device is considered risky and unsafe, as they are beyond the organization's control and monitoring. The devices are risky because they lack measures for enforcing or maintaining security baselines as set out in the organization's security policy. The myriad of devices is, however, a necessary evil. One example would be employees who require access to the organization's local resources when they are on business trips, using client's machines. In other instances, employees will use devices from public avenues like cyber cafes or wireless networks. Other examples of unmanaged devices include remote support by vendors and telecommuting, where an employee working from home would be using a personal device that is more prone to compromises compared to organization issued ones. Remote access vulnerabilities rating using Common Vulnerability Scoring System (CVSS) [1] reveals vulnerabilities in three domains; remote device and user, access method, and data or resources being accessed. Organizations implement controls such as Network Access Control (NAC), Virtual Private Network (VPN), Demilitarized Zone (DMZ), and Network sheep-dip to ensure security during remote access.

Vulnerability management (VM) is the process of identification, classification, remediation, and mitigation of vulnerabilities [2]. There are various remote access methods, including tunneling, portals, remote desktop access, and direct application access. The remote access methods are implemented in remote access technologies, among them telnet, Secure Shell (SSH), and VPN, to name but a few common ones. To secure communication networks during remote access, organizations have for long implemented tunneling methods by deploying VPN technologies for remote access. The method securely connects a remote user or device to an internal or private network [3] using the internet and other public networks. However, the VPN is a conventional remote access security approach and has several vulnerabilities, which can take advantage of encryption, the significant threats being malware, botnets, and Distributed Denial of Service (DDoS). Because of the nature of VPN, encryption will prevent the traditional security controls such as firewalls, Intrusion Detection System (IDS), and antivirus software from detecting compromised traffic. The VPN vulnerabilities have been exploited over time by attackers by the use of evasive techniques. The exploitation has enabled unauthorized access to data and resources, leading to costly security breaches and compromises. To remediate logical vulnerabilities in remote access, it is therefore vital to address all vulnerabilities in remote access. The objectives of this study are to analyze conventional remote access security controls and approaches, highlight their weakness, and develop a remote access security model. To achieve the research objectives, we propose the integration of remote access domains, tiered networks, and vulnerability management.

The rest of this paper is organized as follows; in Section 2, we present the conventional approaches to remote access security and their limitations. We present our methodology for managing remote access vulnerabilities in section 3. In section 4, we present the simulation and evaluation results for regular and compromised traffic and propose a novel approach for malware detection in encrypted traffic. The outcomes of our research are fourfold:

a. We highlight the limitations of current approaches to remote access security.
b. We carry out experiments to show malware spreading capabilities and DDoS continuous flooding attacks in remote access.
c. We propose a novel approach to remote access security by VM passive feature learning.

2. Literature Review

Several security controls exist to address vulnerabilities in remote access. The security controls, for example, the antivirus is signature-based, where the knowledge of malware variant is necessary for effective detection. When it comes to heuristic-based approaches, they are prone to a high rate of false positives and take long to analyze traffic for malware and other compromises. Over the years, several approaches have been developed and implemented to ensure security in networks, a good number concentrating on remote access security. The following are traditional approaches to remote access security.

2.1. Network Access Control (NAC)

Network Access Control (NAC) is an implementation for determining the health and status of devices requesting access to network resources. It enforces security baseline, prevents access by unauthorized devices [4] by checking various pre-specified statuses such as installation and updates for antivirus programs, patches, IP address, Media Access Control (MAC) address or even password policy. Any device failing to meet network security requirements status is quarantined. As such, remote devices that might potentially be compromised are prevented from connecting. Device examination classifies devices as safe or not, allowing only safe one's access to the network. Information security policies are used to determine whether a device meets the pre-set requirements. NAC ensures compliance with the organization's security policies for each remote device. It allows or denies network access by:

a. Identification and authentication.
b. Network security policy enforcement.
c. Triage, where safe remote device accesses data or quarantined if not safe.
d. The remote device accesses data and resources after compliance with security policies.
e. The remote device is disconnected if it does not comply.
f. Continuous check for the first network and each subsequent connection attempt.

However, a NAC server may lock out any device that is not considered safe by the organization, such as the unmanaged devices. The lockout means that availability is restricted, for example, if an employee happens to travel without an organizational issued device, there will be no means of access to the data and resources they might need, which may end up hindering the business or core operations. Furthermore, even for a device that would be considered safe, once a session is established, there would be no means of evaluating the legitimacy of encrypted traffic in the tunnel.

2.2. *Virtual Private Network (VPN)*

A VPN securely connects a remote user or device to an internal or private network [3]. It uses the internet or any other unsecured network to transmit data employing a tunneling method and other security mechanisms to prevent data access and interception by unauthorized users. Tunneling provides encryption and data integrity. The remote user or device connected to a virtual private network acts as a local user connected to the local network. A VPN facilitates secure data access from different geographical locations and the use of local internet and access to websites or applications blocked at the remote user's location. VPN's can be classified according to their application environments; the environments include Local Area Network (LAN), remote access, and extranet use. The study concentrates on remote access VPN that is used to secure communication between remote devices and the internal network. Fig.1., below shows a conventional remote access VPN that connects remote devices to the internal network.

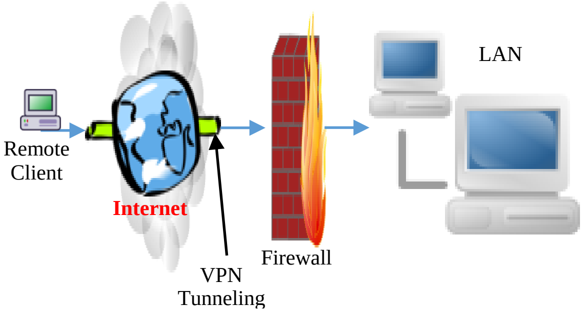

Fig.1. A remote access VPN.

Tunneling can be voluntary or compulsory. Voluntary is when a connection is established on demand by the remote device or user. A service provider sets up and manages compulsory tunneling configuration and VPN server connectivity. VPN protocols include point-to-point tunneling protocol (PPTP), layer two tunneling protocol (L2TP), and internet protocol security (IPsec). IPsec operates in either tunnel mode where the complete IP packet is encrypted or transport mode where data and IP packet are encrypted, and the packet header is left unencrypted. A VPN concentrator is a server mechanism for validating and authorizing VPN connection requests. Remote devices connect to the VPN concentrator. However, a VPN introduces several unforeseen challenges to the security of the internal network, the major ones being malware, botnets, and DDoS. If a remote device is infected, the compromised traffic will be transmitted without the perimeter security controls such as the firewall or IDS raising the alarm, as they are not capable of analyzing the encrypted traffic. Therefore, the core advantage and strength of a VPN is used to evade detection mechanisms.

2.3. *A Demilitarized Zone (DMZ)*

DMZ is a means of enhancing network security that separates an organization's internal network from its access network [5]. It is a component in remote access that, if properly configured, can detect and prevent malicious activities perpetrated toward the internal network. Proxy servers in a DMZ further restrict access to organizational resources by remote users and devices. Fig.2., below shows a Simple Mail Transfer Protocol (SMTP) proxy server in a DMZ. The layout is just one of the many ways of setting up a DMZ. Firewall(s) in a DMZ provides essential security functionalities such as screening and authentication. In a DMZ, traffic is terminated at an isolated area of the network, thereby preventing malware and other compromised traffic from getting to the internal network. However, the resources in a DMZ, for example, the proxy servers, will be exposed to compromised traffic, as the firewall is not capable of screening the encrypted traffic.

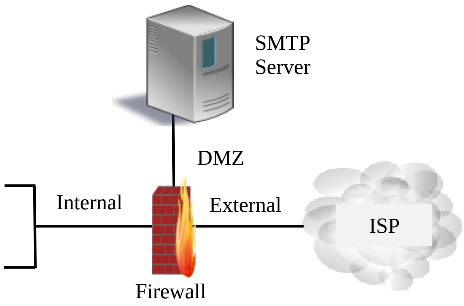

Fig.2. An example of a DMZ.

2.4. *Network sheep-dip*

Network sheep-dip in information and network security, also referred to as a footbath, is the process of checking media and traffic for malware before they are allowed into the internal network [6, 7]. Data and messages entering the network from a remote device need to be analyzed for malware. A network sheep-dip has the capabilities of running monitors for the port, network, user, group permission, process, device, file, registry, and kernel [8]. A network sheep-dip will have monitors for file, network, and antivirus software. The network sheep-dip monitors will detect and analyze malicious data and code for viruses, worms, and Trojans. Fig.3., below shows an implementation of a network sheep-dip, which includes antivirus, anti-spyware, anti-Trojan, anti-spam ware, anti-phishing, and an e-mail scanner. A network sheep-dip scans decrypted traffic from the access or public network before the traffic is allowed into the internal network, which is vital to ward off malicious traffic. However, a network sheep-dip is a traditional signature and heuristic-based approach and, therefore, prone to the challenges of zero-day attacks, false positives coupled with lengthy analysis and scanning time.

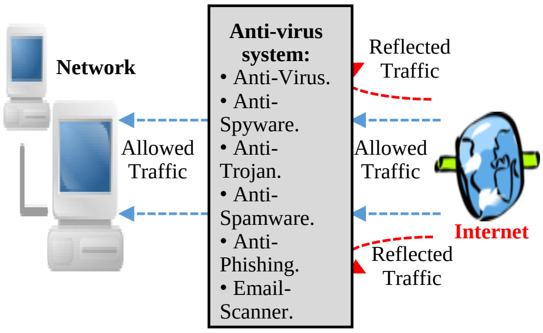

Fig.3. A network sheep-dip.

These conventional approaches to remote access security have been breached repeatedly by attackers to perpetrate attacks and, in some instances employing their very core technologies and advantages to circumvent detection, for example, failure by perimeter controls to detect malware in encrypted traffic. The threat landscape is ever-changing, with attackers quickly adopting new approaches and evasion techniques to beat the available detection mechanisms. As such, proactive and dynamic approaches are necessary to counter the ever-changing remote access threat landscape. We, therefore, propose a VM approach to threats in remote access by adopting tiered networks and a novel approach for malware detection in encrypted traffic. This approach will ensure the confidentiality and integrity of encrypted data in remote access is preserved while at the same time, ensuring only legitimate traffic is allowed through to the internal network.

3. Methodology

In this section, we present a tired network approach for VM in remote access. We then present a conceptual security model for remote access security, followed by simulations and evaluation.

3.1. *Tiered network approach*

A tiered network approach to VM in remote access is presented in this section, which includes the internet, extranet, and intranet tiers. The tiered network approach is a way of dividing a communication network into partitions or segments [9]. The segmentation is done in order to facilitate the placing of security controls between the tiers to control and manage access to data and information during the transfer from one tier to the other to deter unauthorized access. Adopting the tiered network approach would facilitate effective and efficient implementation of security controls to each of the domains in remote access (remote device and user, access method, and local data or resources [1]), thereby enhancing the remediation process. The basic communication network tiers are internet, extranet, and intranet, adopting the network tiers for remote access security would facilitate VM and implementation of security controls. During remote access, a user or device in the first domain initiates communication through the second domain of access method to the third domain of local data or resources. The control between remote access network tiers is a critical aspect to ensure security during remote access. Therefore, there is a need to implement control measures between the network tiers. The controls can be implemented in terms of authentication and authorization mechanisms. Fig.4., below shows the various network tiers in remote access and implementation of controls between the network tiers. Starting from the internet tier where the remote device or user is located, authentication and authorization are required to allow the remote user or device access to the extranet tier. Access from the extranet tier to the intranet tier requires a high level of security. Therefore, it is necessary to have advanced measures such as tokens, personal identification, and digital certificates. Access from the intranet tier to the internet tier does not necessarily require any security control, but it is essential to restrict any access from the internet tier to the intranet tier.

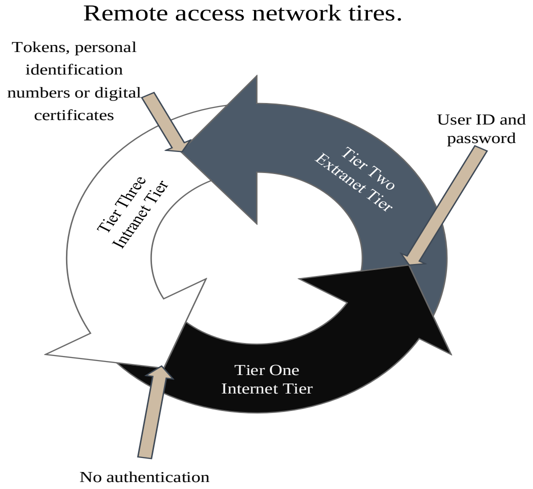

Fig.4. Remote access network tiers.

3.2. Vulnerability Management (VM) in Remote Access

Fig.5., below shows the VM process for remote access based on domains and network tiers. As a starting point, it is crucial to identify vulnerabilities in remote access. The identification should be made for all domains of remote access, starting from communication initialization, access method, to local data or resources. The identified vulnerabilities should then be categorized as per the three domains in remote access. Scoring involves evaluating the impact of a vulnerability, for example, if the vulnerability is successfully exploited. The scoring is essential for vulnerability prioritization, which determines the number of resources to allocate for vulnerability remediation. Remote access classification into distinct domains enables identification of vulnerabilities in remote users and devices, access methods, and local data or resources. Necessary and unique security controls are then applied to each of the remote access domains in a unique way to remediate the scored vulnerabilities. For remediation of the identified vulnerabilities, network tiers facilitate the implementation of security controls to safeguard data during remote access. If by the end of the cycle, a vulnerability has not been remediated, it is vital to confirm whether it is correctly categorized at the beginning of the process. Documentation of the VM process for remote access facilitates the future review of activities, knowledge transfer, and, more importantly, enhances continuous vulnerability management.

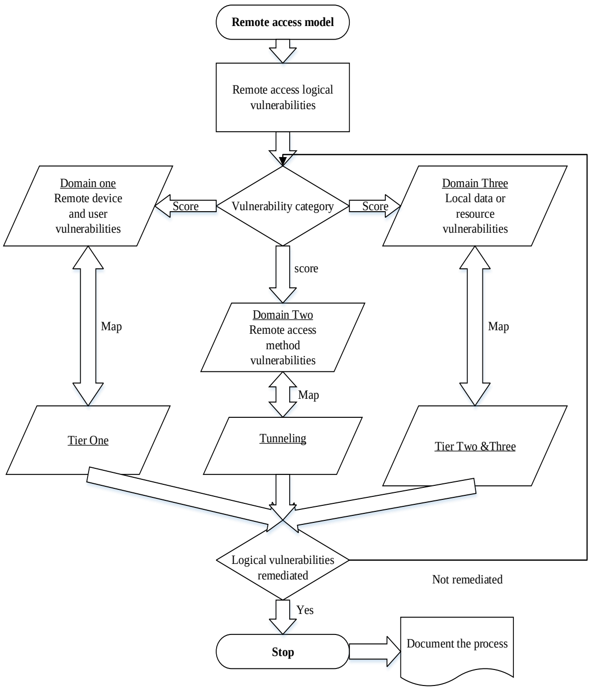
Remote access model
Remote access logical vulnerabilities
Domain one
Remote device and user vulnerabilities
Score
Vulnerability category
Score
Domain Three
Local data or resource vulnerabilities
score
Map
Domain Two
Remote access method vulnerabilities
Map
Map
Tier One
Tunneling
Tier Two &Three
Logical vulnerabilities remediated
Not remediated
Yes
Stop
Document the process

Fig.5. Vulnerability Management (VM) in remote access.

3.3. Simulation and Evaluation

Simulations and evaluation for remote access attacks are presented, which includes network topology and configuration. Simulation and laboratory setup research for network security has been and continues to be an area of concern for many years. The research has yielded several results, which are all very useful today for their uncountable applications, among them network behavior analysis, vulnerability analysis, models, and framework evaluation. Some of the simulation software and applications include CyberOps [10], RCEL [11], MAADNET [12], CyberCIEGE [13], RINSE [14] and DETERLab [15]. Remote access integrates several domains and tiers, which in actual implementation span across different geographical regions. Achieving the setup in an actual network environment would require a significant number of resources in time, applications, software, and hardware.

On the other hand, experimenting in a production environment would be riskier, as it would impede business operations. As such, the simulation would provide a better alternative for the abstraction of the workings of remote access modules across different networks and locations. The simulation will provide the same level of detail and accuracy as with an actual implementation with an advantage of lower cost and time. Besides, it enables the repetition and evaluation of different attack scenarios without harming the host devices. Pastor *et al.* [16] have done an extensive analysis of thirteen (13) tools and systems used for information and network security simulation, grouped into either simulators or laboratory setups. Availability, speed of learning, and level of detail will govern the choice of a simulation system. After keenly reviewing the range of simulation systems available for network security, the study narrowed down to Network Security Simulator (NeSSi2) [17]. The reason is that it is most suited for detailed evaluation and detection for security-related frameworks and models. NeSSi2 is an open-source and provides profile-based automated attack generation, analysis, and detection. NeSSi2 installation requires java runtime engine and MySQL database installation. NeSSi2 has three components, simulation back end, user interface, and a database. The NeSSi2 user interface is used to implement the model profiles and scenarios, and back end to run simulations for attack scenarios. Simulation results were saved in a MySQL database. The model implementation would involve the creation of a remote access network topology and configuration of profiles. The performance evaluation would involve the creation of scenarios and run of simulations.

3.4. Network Topology

A remote access network topology would primarily have internet, extranet, and intranet tiers. The remote access tiers are implemented as subnets, as shown in Fig.7., below, which is a screenshot from NeSSi2, network security simulator. The subnets are connected using links, each subnet implementing different aspects of remote access. Internet tier comprises nodes (remote devices) and remote access router. Extranet tier comprises of firewalls and proxy servers. The intranet tier consists of LAN devices, servers, and a core router.

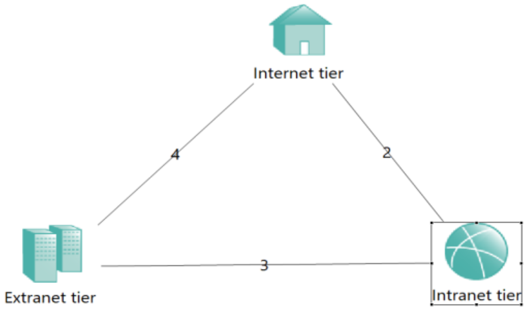

Fig.6. Model subnets.

3.5. *Configuration*

a. Profile configuration – Profiles define the functionality of each component of a subnet. A profile is set by adding applications to nodes and are essential for scenario creation.
b. Scenarios – Scenarios enable the allocation of profiles to nodes. Three scenarios were implemented; regular traffic, malware, and DDoS attack scenarios using TCP, worm, and DDoS application profiles.
c. Simulation: Simulations were created from each scenario by executing the scenarios - running the simulations. It is initiated from the front end, executed in the back end, and saved in the database. The length of each simulation is measured in tick units, which is a unit for time measurement in NeSSi2. Each simulation is set to run for 5000 ticks.

For successful simulation and evaluation of the above three scenarios, two different networks were set, one with healthy and uncompromised remote devices and another one with compromised remote devices, as shown in Fig.8., below. The uncompromised set is installed with TCP client application profiles and used for simulation of regular traffic scenario, which is essential for setting the bandwidth baseline. The set with compromised remote devices (botnets) is installed with malware and DDoS application profiles. The set is to enable us to investigate malware spreading capabilities and DDoS attacks by continuous flooding in remote access. Also included in the figure is a conventional network setup where the link is terminating inside a firewall.

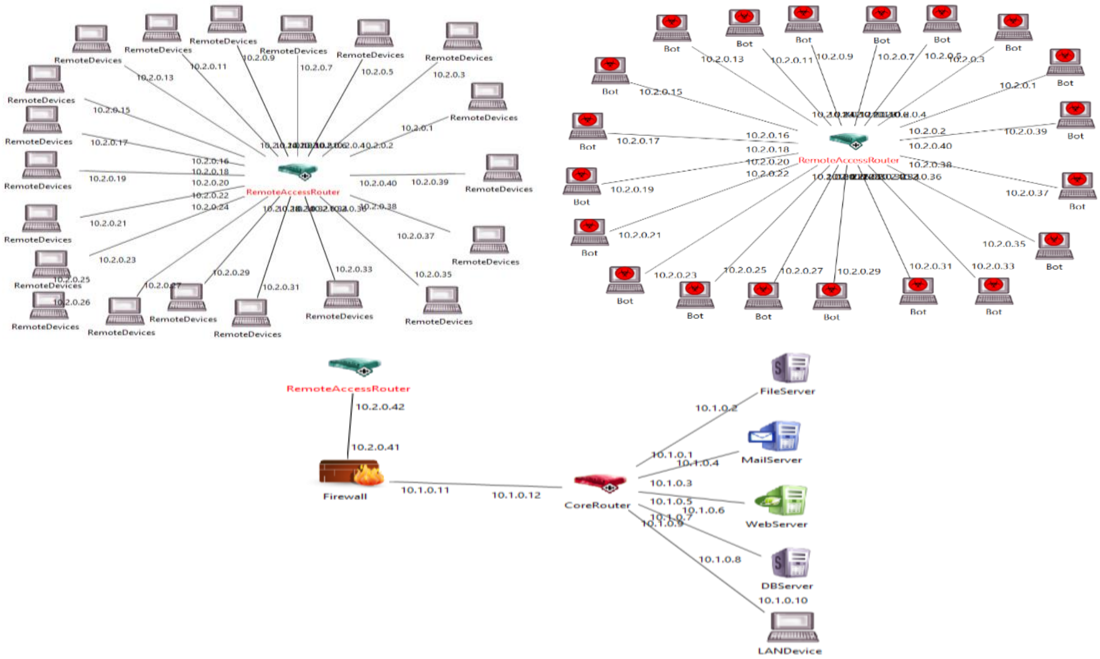

Fig.7. Remote devices, botnets, and network setup.

3.6. *A Conceptual Remote Access Security Model*

A security model for remote access security by the integration of vulnerability management, domains, and network tiers in remote access is presented. Integrating vulnerability management, remote access domains, and tiered networks approach would facilitate remediation of logical vulnerabilities in remote access. The integration process entails placing a remote access domain into a relevant network tier. Any stand-alone security control, for example, host-based firewall, antivirus software, or anti-malware, is not enough security control against the evasive remote access attacks. The protection of data and resources would require the implementation of various security controls and, more importantly, a mechanism to ensure that the security controls work in harmony with each other. Such a mechanism would be a framework or a model to address logical vulnerabilities in remote access. A remote access security model is developed by integrating vulnerability management, remote access domains, and tiered networks, as shown in Fig.6., below. The remote access security model builds on the weaknesses of the traditional security approaches to network and remote access security. Tunneling has stood the test of time in terms of ensuring confidentiality and integrity through encryption, but its sole advantage is used to circumvent detection by attackers. To bridge the gap, which is a significant loophole in remote access security, an equally dynamic approach for VM and detection of compromised encrypted remote access traffic by passive feature learning (PFL) using Machine Learning (ML) is developed. PFL using ML would ensure a high degree of accuracy and faster speeds in the detection of malware and illegitimate traffic that piggybacks on legitimate traffic during remote access. Besides, passive detection of malware and illegitimate traffic in encrypted traffic preserves the essence of privacy and security of data in tunneling.

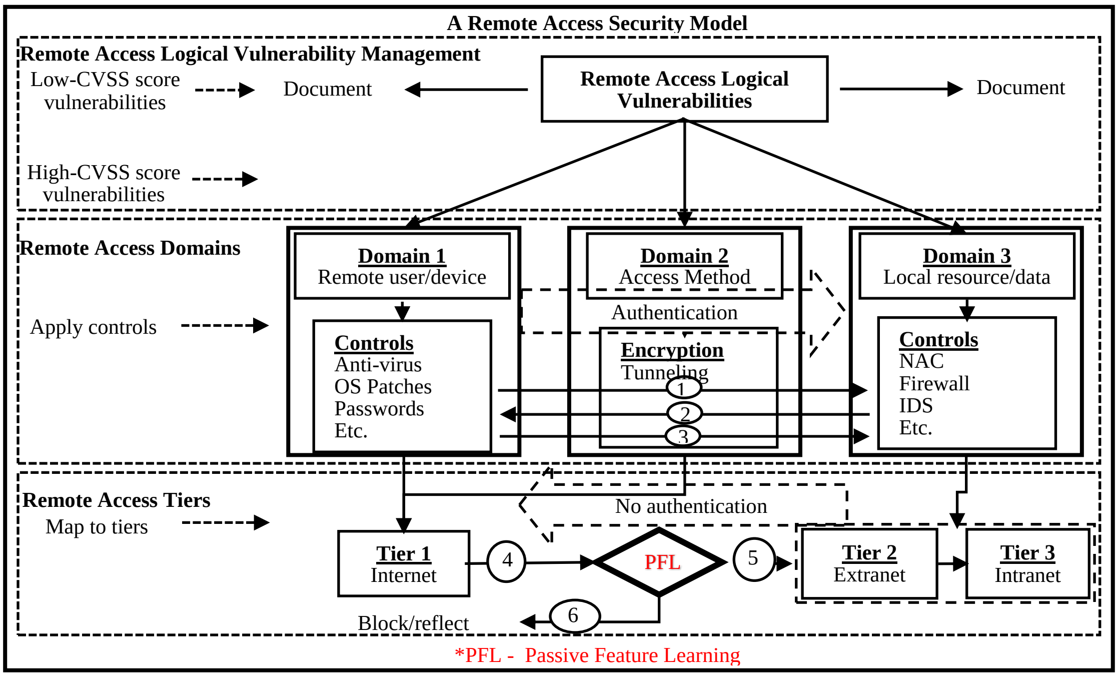

Fig.8. A conceptual remote access security model.

Model key

1. A remote device is authenticated.
2. A NAC server probes remote devices for security policy compliance.
3. Remote access is granted.
4. Passive Feature Learning (PFL).
5. Legitimate remote access traffic is allowed.
6. Illegitimate remote access traffic is blocked/reflected.

Model functionalities

a. Remote access logical vulnerabilities are categorized and scored to evaluate their vulnerability rating (CVSS score). The high CVSS score vulnerabilities are categorized into domains 1, 2, and 3.
b. Vulnerabilities with low CVSS scores are reflected or not considered but documented for future reference.
c. According to the vulnerability type, security controls are applied to the domain affected and to that domain only, thereby avoiding unnecessary security controls deployment.
d. Each of the domains has unique security controls deployed warranted by the vulnerability type or attack vector such as Anti-virus, anti-spyware, and passwords in domain 1, encryption in domain 2 and NAC, firewalls, IDS and IPS in domain 3.
e. A user in domain 1 procures access to resources or data in domain 3 through an access method in domain 2.
f. Each of the remote access domains is mapped to a network tier; domains 1 and 2 to tier 1 and domains 3 to tiers 2 and 3.
g. Security controls are placed between the network tiers to control and manage access of data and information to

prevent unauthorized access; user Identification (ID) and passwords between tier 1 and tier 2 and tokens, personal identification numbers or digital certificates between tier 2 and tier 3.

h. A user in tier 1 is authenticated, for example, through a user ID and password to get access to tier 2.
i. A NAC server in domain 3 probes the user device for compliance or adherence to security policy requirements, for example, whether the device has an antivirus program installed, whether the antivirus program is updated, whether patches have been applied to the O.S and proper configurations.
j. Access is granted to the user device after passing the compliance check and verification of the user device tokens, personal identification number, or digital certificates.
k. Passive feature learning (PFL) is introduced between tiers 1 and 2. PFL will examine the packets being transmitted for compromises, for example, malware and DDoS traffic features.
l. If the transmitted traffic is considered legitimate, it is allowed into tier 2 and 3. However, the traffic is reflected if considered compromised. The compromised traffic may be stored for further analysis of attack sources, type, and frequency.

Model characteristics

a. Ensures conventional security controls work in harmony with each other and with the passive feature learning (PFL) being introduced as part of the study.
b. VM ensures that only necessary controls are deployed because only highly rated vulnerabilities are considered for remediation.
c. VM ensures documentation of both low and high CVSS score vulnerabilities for verification of a vulnerability re-occurrence in the future.
d. Security domains ensure that vulnerabilities are appropriately categorized.
e. Security domains ensure controls are uniquely applied to each domain.
f. Tiered networks manage and control access to information and data.
g. Tiered networks facilitate proper placement of security controls between tiers.
h. Tiered networks prevent unauthorized access through phased authentication.
i. The use of the NAC server ensures compliance and adherence to set security policy.
j. PFL ensures privacy by ensuring that there is no need for decryption of remote access traffic for analysis.
k. The use of fixed length vectors ensures faster remote access scanning.
l. Traffic classification ensures detection of compromised remote access traffic, for example, DDoS or malware.
m. The use of automatic remote access traffic features learning ensures high detection accuracy and detection of compromised remote access traffic variants.

4. Results and Discussion

The section contains the output of the simulations presented as transient graphs for transmitted packets as events/amount against time in tick units. The traffic is captured at the links between remote access router and the firewall. Then, from the firewall to the core router. Traffic for individual devices in the internal network is also included. The first part presents regular traffic simulation, which is a bandwidth benchmark for the experiments. The second part presents a simulation for malware attack followed by a DDoS attack simulation by continuous flooding. Lastly, the effects of malicious attacks in a DMZ, such as a DDOS continuous flooding attack on a proxy server, are shown. The assumption for the experiments is that the botnets are initially legitimate remote access devices, which have been infected with malware, and hence the perimeter controls will allow the traffic through by judgment on traffic origin.

4.1. Regular traffic simulation

Regular traffic simulation entailed the use of remote devices with TCP client application profiles transmitting packets to the internal network via a firewall. Fig.9., below shows events in the links from remote access router to the firewall, firewall to core router, and in web and Database (DB) servers. 8,500 packets are transmitted at both links and 2,100 packets at web and DB servers for 5,000 ticks. Assuming that remote devices are capable of sending traffic at a rate of 100 pings per second, a single tick may represent 0.01 seconds giving a total time of 50 seconds and a total data rate of 170pps for links 42pps for servers. The Maximum Transmission Unit (MTU) is 1500 bytes, and the MTU translates 2.04 Mbit/s at the links and 0.504 Mbit/s for servers, which will make the baseline bandwidth.

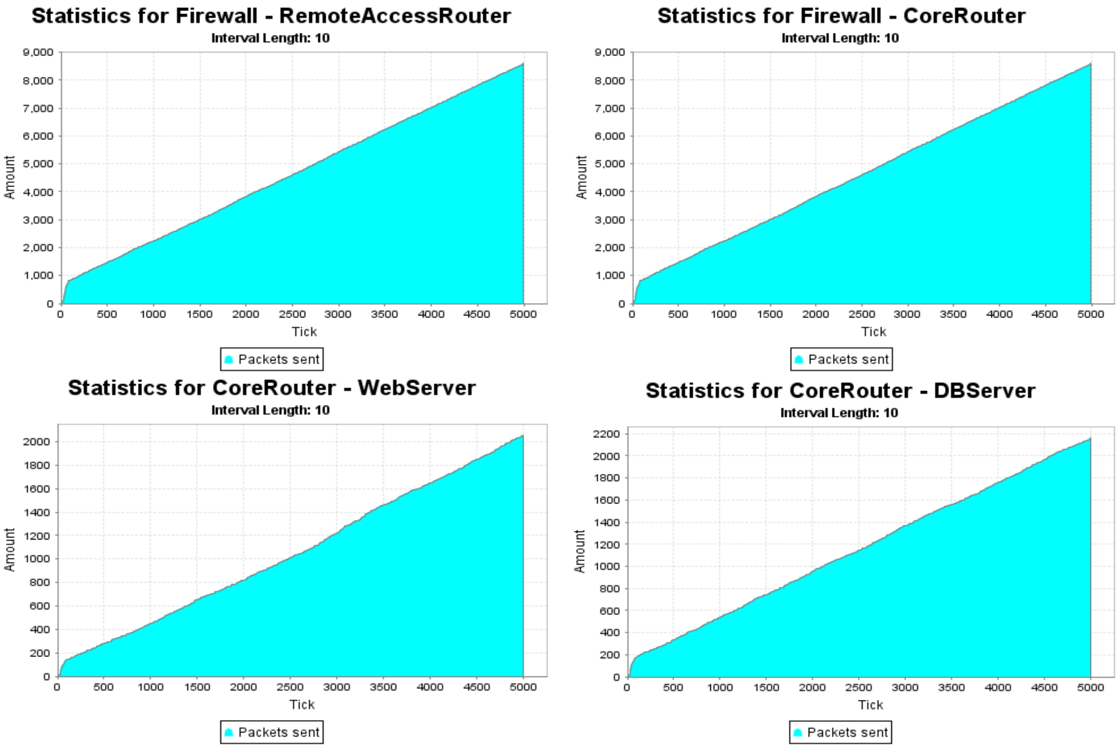

Fig.9. Regular traffic simulation.

4.2. *Malware attack simulation*

For malware attack simulation, remote devices installed with a worm application profile were used. Fig.10., below shows the results of the simulation at the links between remote access router and firewall and between firewall and core router, where both links show 8,500 packets being transmitted for 5,000 ticks. The firewall filters no traffic; therefore, it is essential to note that the compromised traffic can pass through the firewall undetected to the internal network.

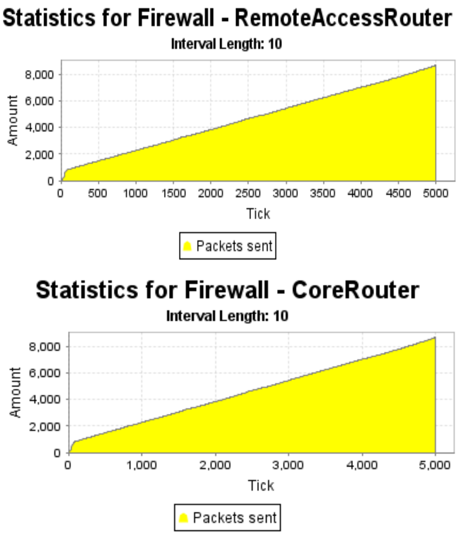

Fig.10. Malware attack simulation.

4.3. *DDoS attack simulation*

For a DDoS attack simulation, remote devices installed with DDoS continuous flooding application profiles were used and set to activate at the 500th tick. The attack target is set to be a DB server 10.1.0.8. Fig.11., below shows the results for a DDoS attack simulation. The attack resulted in 28,000 packets at links and 20,000 packets at the target server for 5,000 ticks. Assuming that remote devices are capable of sending traffic at a rate of 100 pings per second, a single tick may represent 0.01 seconds giving a total time of 50 seconds and a total data rate of 560pps for links 400pps for the target server. The MTU is 1500 bytes, and the MTU translates to 6.72 Mbit/s at links and 4.8 Mbit/s for the target server, which is way above the baseline at 329.41% and 952.38% at the links and target server consecutively. It is important to note that the web server at 10.1.0.6 despite being in the same network remains unharmed with only 2,100 packets reaching it.

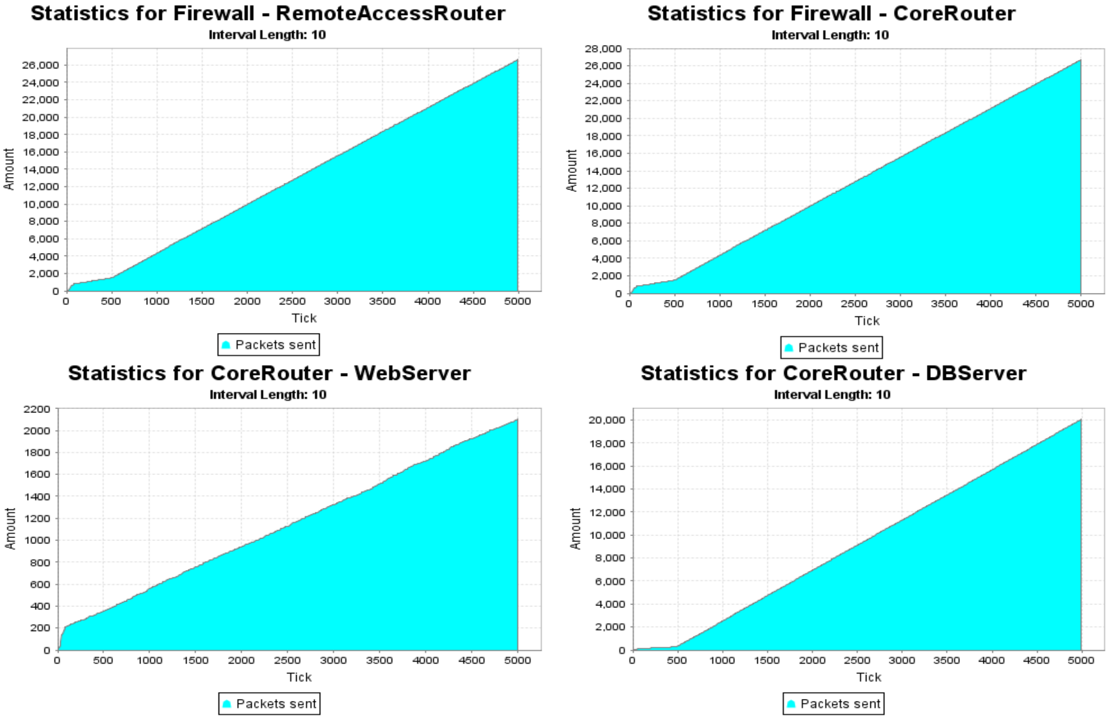

Fig.11. DDoS attack simulation.

4.4. *DDoS Attack in a DMZ*

In this experiment, an extra firewall is introduced to provision for a DMZ, as shown in Fig.12., below. First, compromised devices (botnets) are used to target a DB server 10.1.0.8 in the internal network, and then the same set of botnets is used to target a proxy server 10.2.0.44 in a DMZ.

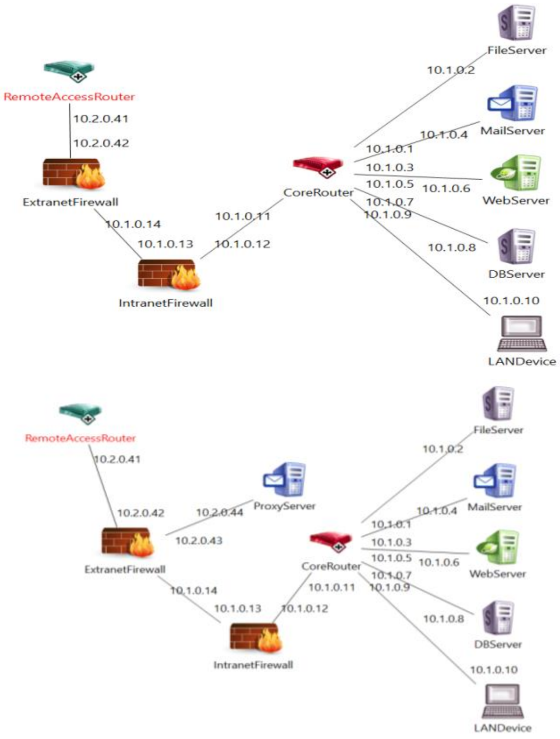

Fig.12. DDoS attack in a DMZ network setup.

Fig.13., below shows the results of the simulation for a DDoS attack targeting a DB server in the internal network and a proxy server in a DMZ. In the simulation, two firewalls are used to create a DMZ. Botnets targeting the DB server sends close to 17,000 packets. However, as evident in the simulation results, the second firewall can drop a significant number of packets allowing only 8,500 packets. The compromised devices (botnets) are capable of sending traffic at a rate of 100 pings per second, and a single tick may represent 0.01 seconds, giving a total time of 50 seconds and a total data rate of 170pps for allowed traffic. The MTU is 1500 bytes, and the MTU translates to 2.04 Mbit/s, which is equivalent to the baseline bandwidth. The firewall can successfully avert the attack by dropping 50% of the packets sent, and hence, the targeted DB server remains unharmed in the simulation with only 2,100 packets the same number as the webserver. However, despite the existence of a DMZ, the proxy server is not spared by the second attack receiving 20,000 packets, a data rate of 400pps, and 4.8 Mbit/s, way above the baseline bandwidth.

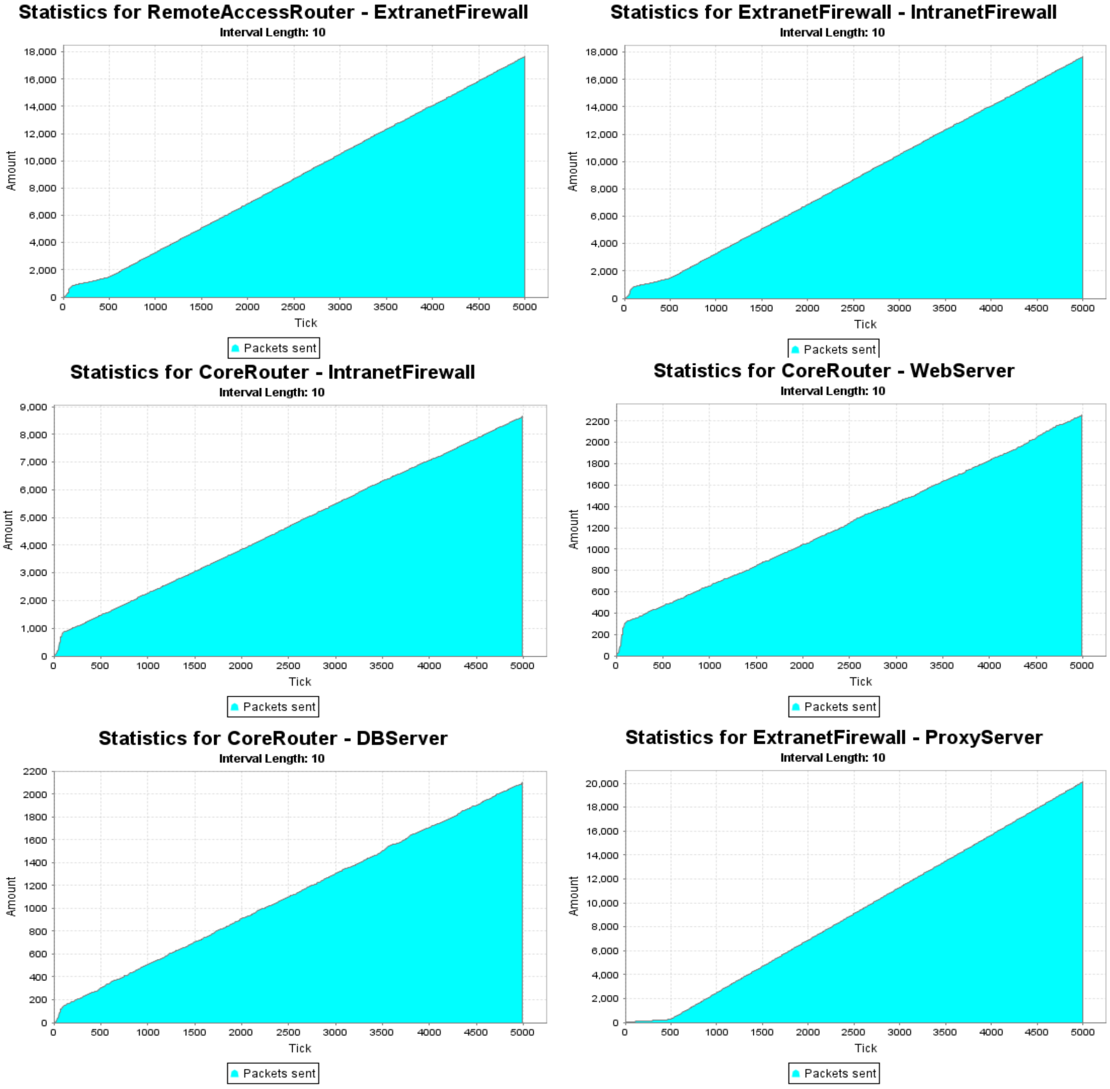

Fig.13. DDoS attack in a DMZ.

5. Discussion

Conventional approaches to security of data and resources during remote access have, to some extent being able to avert breaches when faced with unencrypted traffic. Encrypting data and traffic is inevitable in the current threat landscape. The existing detection approaches have resulted in compromising the idea behind encryption by decrypting encrypted traffic for analyses and the effective detection of malware. The decryption approach would be against security policies and standards.

Furthermore, the experimental results provide evidence that conventional approaches to securing remote access have exploitable vulnerabilities, which in addition to failure to filter compromised traffic, may, to some extent, aide attackers and facilitate attacks by providing evasion mechanisms. A case in point is malware in encrypted traffic, which existing controls such as firewall, IDS and antivirus software are not capable of analyzing. The remote access vulnerabilities are further enhanced by a combination of two or more security controls, for example, firewall plus tunneling. For a tunnel that terminates inside a firewall, the firewall has no capability of inspecting the traffic, and it can only confirm the origin of the traffic. If the origin is known or the remote device is legitimate, then the traffic is let through, if the encrypted traffic is compromised, it may lead to the introduction of malware in the internal network. An alternative to confirming remote access traffic origin would be to terminate the tunnel outside the firewall, which would allow the firewall to inspect the traffic before it is allowed into the internal network. However, the termination would require traffic to be decrypted in unsecured network rendering encryption efforts useless and exposing data to eavesdroppers and sniffers. The other option would be to deploy a DMZ, which as evident in the experiment results above, is still vulnerable to threats, as an attack targeting a proxy server would be carried out successfully using encrypted malware. Encryption is the foundation of tunneling and VPN in remote access, which ensures confidentiality and integrity of data—as such, securing remote access calls for novel approaches capable of detecting and predicting malware not only in plain text but also in encrypted traffic.

6. Conclusion

There are three main areas of concern for remote access security; remote device/user, access method, and target systems/resources. Scoring vulnerabilities in remote access brings to light the gap in the current remote access security methods and technologies. The gap has further been proved by simulations to evaluate the remote access security model. As a means to secure the remote access method, tunneling is indisputably a robust mechanism. However, other factors are in play when it comes to comprehensively securing remote access. Encrypted traffic provides innumerable advantages for organizations in terms of security and privacy for data in transit and static states. During remote access, encryption is even of more importance as public and insecure networks are used to access internal networks. However, the very fundamental idea and advantage of encryption technology are used by attackers to circumvent prevention, detection, and response mechanism, thereby compromising confidentiality, integrity, and availability of data. It is, therefore, imperative to detect compromised traffic accurately and quickly. We propose the detection of compromised traffic by packet capture feature learning.

Contrary to other approaches where encrypted traffic is first decrypted for malware and DDoS traffic detection, the approach passively learns packet capture file features, thereby preserving the privacy of data, which is very important for encrypted data. The study provides a model for the detection of compromised encrypted traffic during remote access by passive feature learning (PFL). As future work, we will implement the PFL part of the model using a machine learning model and a classifier model.

Acknowledgements

The research was partly supported by the Higher Education Loans Board through Grant HELB/45/003/VL.1 of Postgraduate Award 2014/2015.

References

[1] Ndichu, S., McOyowo, S., Okoyo, H., and Wekesa, C. (2019). A Domains Approach to Remote Access Logical Vulnerabilities Classification, *International Journal of Computer Network and Information Security (IJCNIS)*, Volume 11, Number 11, Pp.36-45.

[2] Foreman, P. (2010). Vulnerability management. *Boca Raton, FL, Auerbach Pub*. Pp.2-3.

[3] EC-Council. (2012). Virtual Private Networks, *Network Defense: Security and Vulnerability Assessment, Cengage Learning*, Volume 5 of 5, Chapter 4, Pp.1-20.

[4] Ciampa, M. (2012). Security+ Guide to Network Security Fundamentals. *3rd ed. Boston, MA: Course Technology, Cengage Learning*, Pp.291-292.

[5] Fung, K. (2005). Network Security Technologies. *Boca Raton, FL*: *Auerbach Publications*, PP.69-70.

[6] Dong, J. (2007). Network Dictionary, *Javvin Technologies, Inc*. Pp.199.

[7] Talukdar, M. (2014). Dictionary of Computer and Information Technology, *Prabhat Prakashan*, May 20, 2014.

[8] EC-Council. (2013). Viruses and Worms, *Ethical Hacking and Counter Measures*, Module 7, Volume 1, Pp.1079-1081.

[9] Arconati, N. (2002). One Approach to Enterprise Security Architecture, *SANS Security Essentials GSEC version 1.3*, SANS Institute 2002.

[10] Duffy, B. (2008). Network Defense Training through CyberOps Network Simulations, *Proceedings of the Modelling, Simulation, and Gaming Student Capstone Conference*, April 9, 2008.

[11] Guild, R. J. (2004). Design and Analysis of a Model Reconfigurable Cyber-Exercise Laboratory (RCEL) for Information Assurance Education, *Naval Postgraduate School, Monterrey, California, USA*.

[12] Hill, J. M., Surdu, J. R., Lathrop, S., Conti, G., Carver Jr C. A. (2003). MAADNET NetBuilder: A Service and Demand Focused Network Simulator, *International Conference on Simulation and Multimedia in Engineering Education (ICSEE'03), Communication Networks and Distributed Systems Modelling and Simulation (CNDS 2003).*

[13] Irvine, C., Thompson, M., and Allen, K. (2005). CyberCIEGE: Gaming for Information Assurance, *IEEE Security and Privacy Magazine*, vol. 3, Pp.61-64.

[14] Liljenstam, M., Liu, J., Nicol, D., Yuan, Y., Yan, G., and Grier, C. (2005). Real-time Immersive Network Simulation

Environment (RINSE) for Network Security Exercises, *Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation, IEEE Computer Society*, Pp.128.

[15] Schwab, S., Wilson, B., Ko, C., and Hussain, A. (2007). SEER: A Security Experimentation Environment for DETER, *Proceedings of the DETER Community Workshop on Cyber Security Experimentation and Test on DETER Community Workshop on Cyber Security Experimentation and Test 2007*, USENIX Association.

[16] Pastor, V., Diaz G., and Castro M. (2010). State of the Art Simulation Systems for Information Security Education, Training and Awareness, *IEEE EDUCON Education Engineering – The Future of Global Learning Engineering Education, April 2010*, Pp.1907-1916.

[17] Chinnow, J., Bye, R., Schmidt, S., Bsufka, K., Camtepe, S. A., and Albayrak, S. (2009). An Extensible Simulation Framework for Critical Infrastructure Security, *DAI Laboratory, School of Electrical Engineering and Computer Science of the Berlin Institute of Technology, Technical Report: TUB-DAI 09/09-1*, September 14, 2009.

Authors' Profiles

Samuel Ndichu holds an MSc in Data Communication and a BSc in Information Technology from KCA University, Kenya. He is a Computer Science Ph.D. candidate in the School of Computing and Informatics, Maseno University, Kenya. His MSc thesis was focused on developing a framework to evaluate information security preparedness in law enforcement agencies. His current research interests include Information Security, Cybersecurity, and Network Security.

Sylvester McOyowo holds a Ph.D. degree in Computer Science from the Peoples' Friendship University. He is the Dean, School of Computing and Informatics, and a lecturer at the Department of Computer Science Maseno University, Kenya. His main teaching and research interests include Research Methods, Digital, and Analogue Electronics, and he is a Ph.D. supervisor to Mr. Ndichu.

Henry Okoyo holds a Ph.D. degree in Computer Science from the University of Manchester, an MSc degree in Microprocessor Engineering and Digital Electronics from the former University of Manchester Institute of Science and Technology (UMIST), and a BSc degree from the University of Nairobi, Kenya. He is a lecturer at the Department of Computer Science, School of Computing and Informatics, Maseno University, Kenya. His main teaching and research interests include Artificial Intelligence, and he is a Ph.D. supervisor to Mr. Ndichu.

Cyrus Wekesa holds a Ph.D. degree in Electrical Engineering from the University of Tokushima, Japan, and an MSc, and a BSc in Electrical Engineering from the University of Nairobi, Kenya. He is currently an associate professor in the School of Engineering, University of Eldoret, Kenya. His teaching and research interests include and Information Security, Telecommunications and Computer Networks, Computer Architecture, and Electronics, and Distributed Systems, and he is a Ph.D. supervisor to Mr. Ndichu.

How to cite this paper: Samuel Ndichu, Sylvester McOyowo, Henry Okoyo, Cyrus Wekesa, "A Remote Access Security Model based on Vulnerability Management", International Journal of Information Technology and Computer Science(IJITCS), Vol.12, No.5, pp.38-51, 2020. DOI: 10.5815/ijitcs.2020.05.03