iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 9 **Issue:** III **Month of publication:** March 2021

**DOI:** https://doi.org/10.22214/ijraset.2021.33462

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: 7.429*
*Volume 9 Issue III Mar 2021- Available at www.ijraset.com*

# Network Security Attacks and Countermeasures on Layer 2 and Layer 3 Network Devices

Roman Noori[1], Mr. Jasdeep Singh[2]
[1]*Pursuing Master of Technology,* [2]*Assistant Professor, Department of Computer Science and Engineering, RIMT University, Mandi Gobindgarh, Punjab, India*

***Abstract:*** ***In today's world, network security is becoming increasingly necessary, as a result of which various techniques are being used to hack it. To deter consumer data from being misused, network engineers must keep up with recent developments in both hardware and software sectors. People's focus is gradually drawn to network security. This paper briefly addresses the concept of network protection, as well as the need for it, as well as the various methods of attack and Defence against it.***
***Keywords: Network Security, DOS Attacks, MITM, Spoofing, Encryption, Port Security, AAA, TACACS+.***

## I. INTRODUCTION

For growing businesses, having quick access to knowledge on the Internet has become increasingly necessary. When corporations continue to outsource different business operations to the public internet, care must be taken to ensure that their network is not tampered with or falling into the wrong hands. If a hacker or irritated employee has access to a network, it may cause havoc with the organization's confidential records, reduce competitiveness, and hinder the company's ability to compete with other companies. Unauthorized network access will also harm a company's reputation with clients and business associates, who can doubt the company's ability to protect their sensitive data.

Furthermore, any aspect of a network may be targeted by hackers or have unauthorized access. Both routers, switches, and hosts may be hacked by company rivals or even internal workers. In order to identify the best ways to defend a company's assets from attackers, the company's Information Technology Manager must first consider the types of attacks that can be launched and the damage they can wreak on business infrastructures. Growing and strengthening computer and network security is now becoming increasingly necessary and relevant.

Because of the increased use of computer networks, many networks have been exposed to different types of internet attacks, and as a result of this exposure, increased network protection is critical and essential in any organization.To protect the integrity, availability, accountability, and authenticity of computer hardware or network infrastructure, protection can include identification, authentication, and authorization, as well as surveillance cameras.

There is no set process for creating a stable network. Network security must be adapted to the needs of a particular organization's network, not those of others.

For example, a small construction company may allow designated users on the outside of the network access to case information while still ensuring that workers on the inside of the network have complete internet access at all times, in case they need to access a case file from the workplace or on the road.

Applicability When searching for a network provider for an organization, particularly one as big as a construction company, care must be made to ensure that the network is secured in a way that is compatible with its intent. Fig 1.1 shows the topology of the network. Today's network model necessitates protection against attackers and hackers. Two forms of authentication are used in network security.

1) *Computer Protection:* Protecting data against security breaches and destruction.
2) *Information Protection:* To keep data secure from hackers. Network Defence encompasses not only the security of a specific network, but also the security of any system or network.

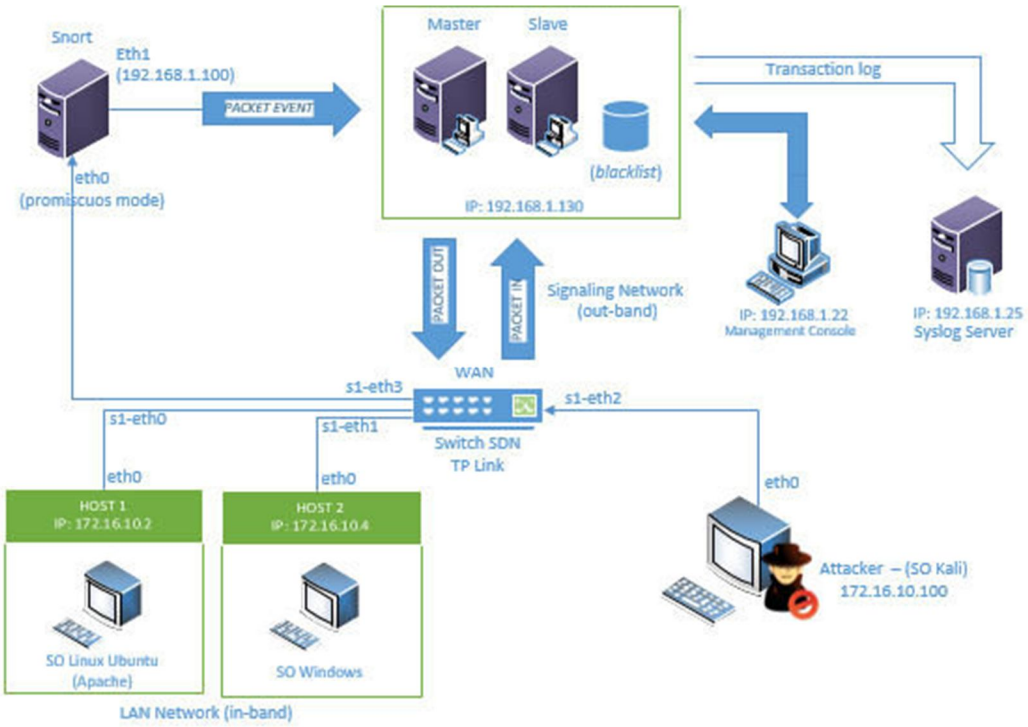



Fig.1. shows the topology of the network.

*A. Device Communication Attack*

Technically skilled hackers have devised a well-structured assault on correspondence protocols.

The OSI model has seven layers for communication between networking devices, each of which has controllable vulnerabilities. In fact, higher layers cannot be protected until lower layers are also stable. However, despite improvements in network operating practice such as nation-wide layer two networks and state and regional optical networks, there has been little attention paid to insecurities at the physical layer or data link layer in recent years. ARP spoofing, MITM (man-in-the-middle) attacks at layer two, and physical layer attacks like passive optical taps or attackers intercepting wireless network signals are all currently established threats at lower levels of the OSI stack. Despite the fact that these attacks are well-known, no research is actually being done to resolve the issues. Fig.2. OSI Model [13].

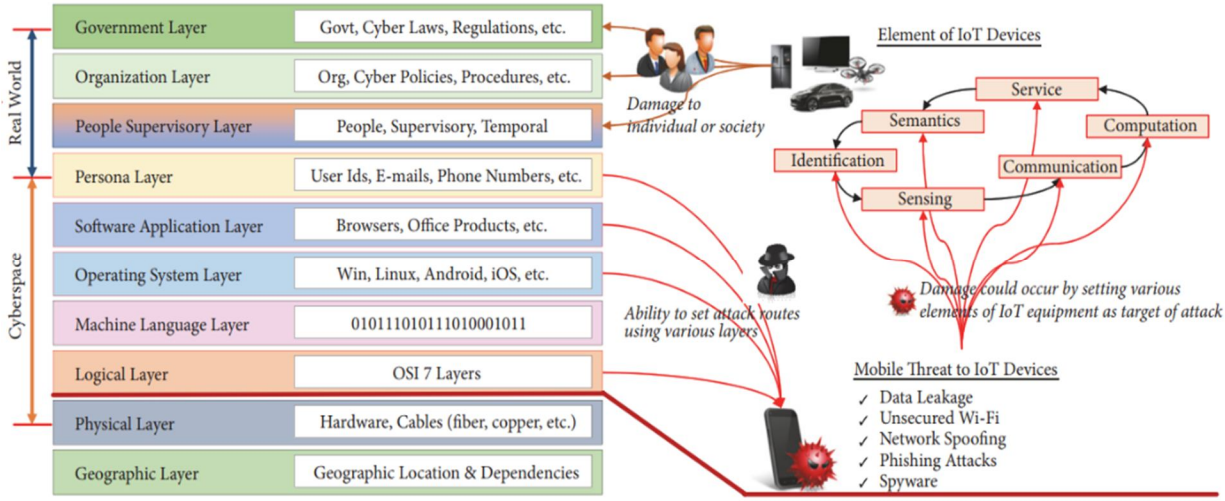



Fig.2. OSI Model

*B. Packet Sniffers*

A packet sniffer (Wireshark, Ettercap), as its name suggests, is a useful tool for network administrators to use to track or analyze and detect some sort of problems.
It is also a good tool for attackers to capture packets transmitted through networks.

*C. Access Attack*

Attackers may be outsider hackers or internal users who obtain unauthorized access to a network in order to extract vital and confidential data from the networks. They could even kill infrastructure in order to conceal any knowledge that could lead to them. Different types of attacks have different causes. Intruders use network or server access attacks for the following reasons: retrieving data, gaining entry, and escalating their access rights. The following are examples of access attacks:

*D. Password Attacks*

L0phtCrack and pwdump8 could take password hashes, but not clear-text passwords.
A brute-force password assault can be used to gain access to Accounts that can be used to change sensitive network resources and files. If an attacker modifies the network's routing tables, this is a common example of an attack that violates network integrity. As a result, the attacker guarantees that all network packets are diverted to him before being sent to their intended destination [9].
An attacker can control all network traffic in such situations. L0phtCrack has two techniques for calculating passwords:

*1)* Dictionary cracking: All of the password hashes in a dictionary file are matched and computed to all of the users' password hashes. This is a lightning-fast tool for locating very basic passwords.
*2)* Brute-force computation: This technique uses a specific character set, such as A to Z plus 0 to 9, to calculate the hash for any possible password made up of those characters. If the passwords are made up of the character set that someone has chosen to try, brute-force compilation normally computes them. The time taken to complete this method of attack is a challenge for the attacker.

*E. Denial of Sevice Attacks*

a denial of service (DoS) attack destroys or corrupts a data infrastructure or denies any means of access to networks, systems, or facilities. Since they take little effort to perform, denial of service (DoS) attacks are viewed as less essential and considered a poor type. While DoS attacks are simple to execute and can do little serious harm, security administrators should pay particular attention to them.

*F. Man-In-The Middle Attack*

A Man-in-the-middle attack requires the hacker to have access to network packets that are sent over a network. Using network packet sniffers and routing and transport protocols, a man-in-the-middle attack may be carried out. Man-in-the-middle attacks may use identity manipulation, hijacking of an existing session to obtain access to internal Network infrastructure, traffic analysis to gain information about the network and its users, denial of service, data corruption, and the introduction of new information into network sessions as methods to target a network. An ISP employee has access to all network packets and can execute all of the above operations.

*G. DHCP Starvation Attack*

The DHCP starvation attack is a form of DHCP server attack in which an attacker creates forged DHCP requests with the aim of reserving all valid IP addresses from the DHCP Server. Under this attack, legitimate network users can be denied service.

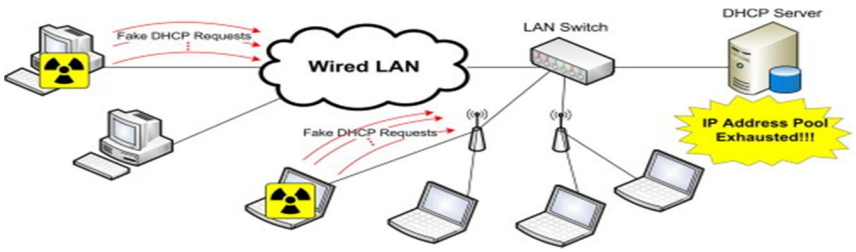



Fig.3. DHCP Attack Topology

*H. MAC Flooding Attack*

MAC Flooding is a way of hacking into network switches to breach their security. MAC Table is a table arrangement that is typically maintained by switches.

This MAC Table contains the individual MAC addresses of the network's host machines that are wired to the switch's ports. The switches use this table to steer data out of the ports where the recipient is placed.

The aim of MAC Flooding is to carry this MAC Table down. The attacker sends a large number of Ethernet frames in a standard MAC flooding attack.[2]

## II. LITERATURE SURVEY

Uday, Kumar., et.al [2016] has described a simulation-based training scenario in which student trainees observe the signs and consequences of a DDoS attack, practice their reaction in a virtual environment with the aim of preparing them for actual attacks, using a simulator and hacking equipment.

GNS3 is an emulator for network applications that was first released in 2008. It facilitates the use of both virtual and physical systems to replicate dynamic networks.

Authors used GNS3 to build various topologies and simulate attacks using automatic scripts or software like Net Tools5 or specially built operating systems like Kali Linux, which are used for ethical hacking. Routers like cisco 3725 and 7200 series are used to simulate the attacks.

Asrodia, P. and Patel H., [2018] Network Traffic Analysis Using Packet Sniffer analyzed that the amount of network traffic flowing over their nodes has increased day by day. This paper focused on the concept of packet sniffer; its working principle used for analyzing network traffic.

It also focused on various types of tools for traffic analysis, such as Wireshark tepdump, etc. packet sniffer plays a significant role and captures things like clear text password, and usernames, or sensitive material.

Arianit et. al., [2017] have described the potential damage from DOS attacks and analyze the ramifications of the damage. The author has used the same penetration testing approach that is used by malicious attackers in order to test network security. The only difference is an authorization.

They have analyzed different firewalls and other protective systems and their role in overall security during these attacks. For testing network systems, they have simulated DoS (Denial of Service) attacks on networks with different topology Dos attacks can be avoided by implementing appropriate systems for protection against these attacks.

In order to avoid such an attack, there is a need to continuously monitor the network and identify such attacks (lP address of the attacker). In addition, since it is very easy to interrupt services from the internal network, there is a paramount need to protect the servers with next-generation firewalls.

Tomar, Kuldeep, and Tyagi S.S., [2014] have introduced the computer network and importance of computer network. Different types of network attacks like passive attacks, insider attacks, distributed attacks, active attacks, close-in attacks are explained briefly.

It has also highlighted some popular dos attacks like ICMP flood attacks, teardrop attacks, SYN-flood attacks, Land attacks, Smurf attacks, Distributed Dos attacks. The writer has discussed few protective mechanisms against these Dos attacks. According to the writer by proper configuration of Firewall, IDS/IPS, ISP edge Router we can control the effect of Dos attacks. This paper also simulates the dos attack using GNS3.

ICMP-flood attacks were simulated and the result was observed. The simulation results show that the policy inspection success rate becomes very high and packets were dropped and even reached to maximum level. According to the writer, there are many mechanisms available to counter these types of attacks but for a small organizations or small networks, it is very hard to implement, configure or purchase mechanisms.

Gupta A., et.al, [2019] Terrorism in Virtual Networks: Using Social Network Analysis

Springer, Cham, pp.180-220, 292-310, in which the authors explained how hackers are categorized into various groups depending on their intent to exploit a device, such as white hat, black hat, and grey hat.

These words are taken from old spaghetti westerns in which the bad man wears a black cowboy hat and the good guy wears a white hat. https://doi.org/10.1007/978-3-319-78256-0_10

## III. CONFIGURATION REQUIRED

The Following Development Tools has been used in the development of this work.

| | |
|---|---|
| Computer | Core 5 Duo or higher |
| RAM | 8 GB |
| Processors | 8 Logical Core |
| Platform | Windows 10 |
| Other hardware | Keyboard, mouse |
| Software | GNS3 VM, VMware Workstation 16 |
| End Device | Windows Server 2012, 2016 |
| End Device | Metasploitable02 |
| Network Device | Cisco Router 15.5 |
| Network Device | Cisco Switch 15.5 |
| Attacker Machin | Kali Linux 2021.1 |

Table.1. Configuration Required

## IV. RESULT AND DISCUSSION

### A. *Tool Used*

*1)* Hundreds of thousands of network engineers around the world use Graphical Network Simulator-3 (GNS3) to simulate, setup, monitor, and troubleshoot simulated and actual networks. GNS3 enables you to run small to medium topologies ranging from a few devices on your desktop to hundreds of devices spread through several servers or even in the cloud. GNS3 is free and open-source software.

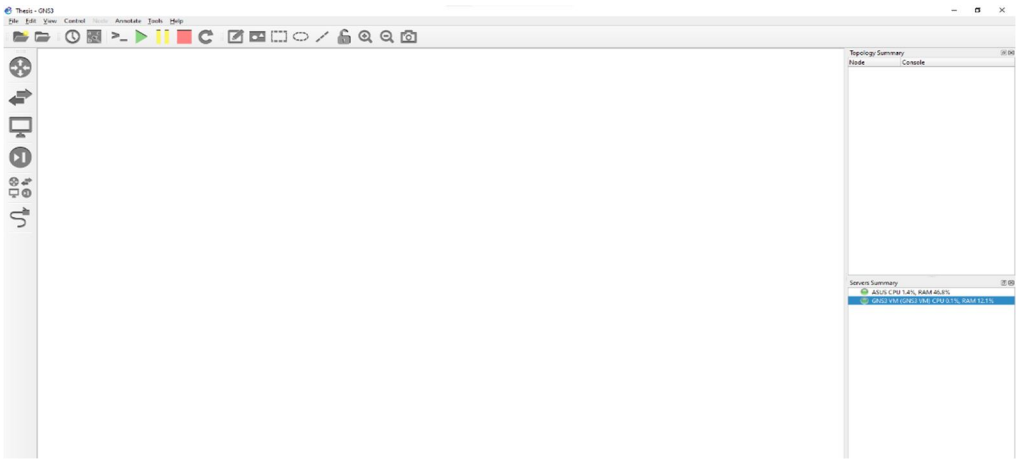


Fig.4. GNS3 LAB

*2)* GMS3 is high-performance philology for technical work out.
*3)* It integrates calculation, visualization, and programming situation.

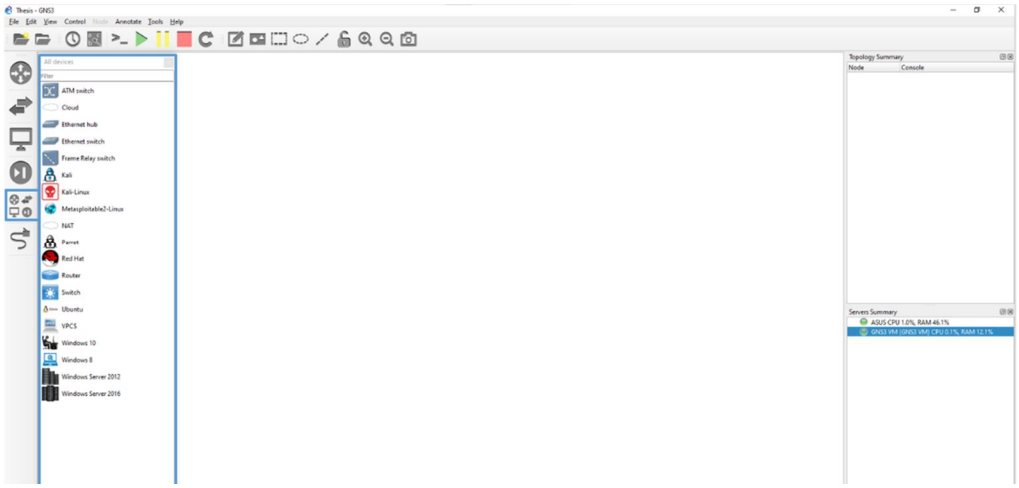


Fig.5. GNS3 LAB Devices

*4)* GNS3 is a modern software design language environment. It has sophisticated data structures, covers built-in editing and debugging tackles, and supports all Network Devices. By drag in drop the device in work space, we can Configure the device by double-clicking on the Device shortcut, by default open with command line tool putty.

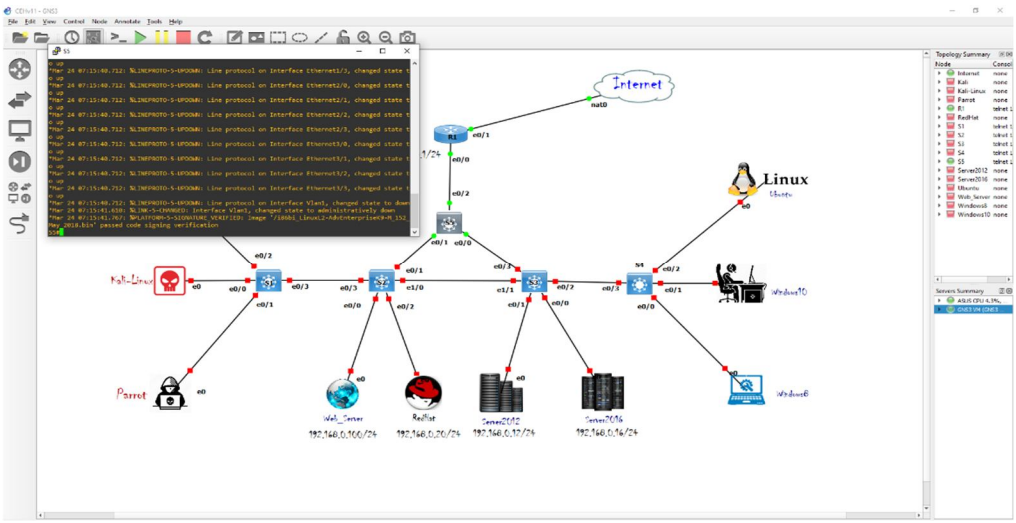



Fig.6. Command line tool putty

*B. Packet Sniffer Attack Mitigation*

The use of strong authentication as a first line of protection against packet sniffers should be the first mitigating option. Strong authentication is a method of identifying accounts that cannot be readily thwarted. Good security is shown by One-Time Passwords (OTPs).

*C. MAC Flooding Attack Mitigation With Port Security*

Various strategies can be used to avoid the MAC Flooding attack.
Any of these techniques are mentioned below.
*1)* Port Security.
*2)* AAA Server Authentication.
*3)* IEEE 802.1X Suites Implementation

*D. Arvation Attack Mitigation With Port Security & DHCP Snooping*

Furthermore, simulation findings show that our proposed approach outperforms other known strategies such as fixed allocation and DHCP request rate detection in mitigating DHCP starvation attacks. We mitigate this attack on Cisco switches by using port protection and DHCP snooping.

*E. Port Security Configuration*

Port Security feature protect the switch from MAC flooding attacks

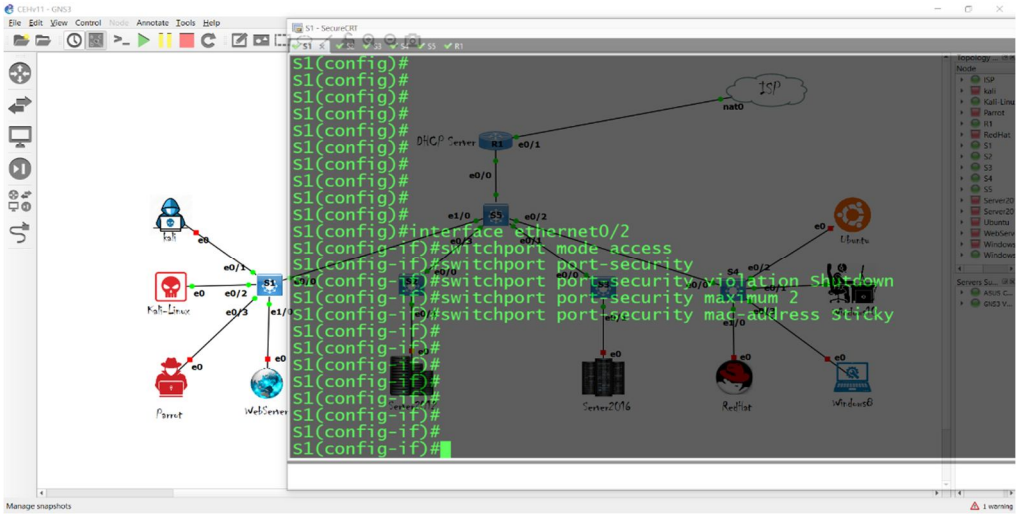



Fig.7. Port security

Fig.7. shows the switch is protected from DHCP starvation attacks thanks to port security features. On ports attached to end stations, the switches are designed to restrict the number of MAC addresses that can be learned. With the traditional MAC address table, a small table of 'secure' MAC addresses is also stored. The MAC address table is also a subset of this table. Cisco switches come with a built-in port protection system [3].

*F. Access Attacks Mitigation*

The following are a few login attack mitigation techniques:

*1)* Passwords cannot be reused across different applications by users.
*2)* Accounts can be removed after a certain number of failed authentication attempts are detected.
*3)* Passwords written in plain text should not be accepted.
*4)* Use powerful passwords (rather than my birthday, use "mY8! Rthd8y@").

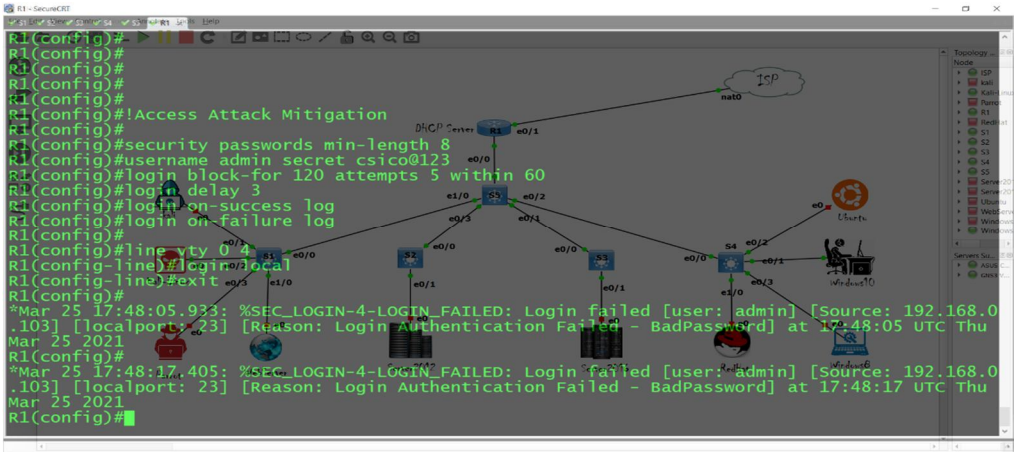



Fig.8. Password Attack Mitigation

*G. Man-In-The-Middle Of Attack Mitigation*

The first Dynamic ARP Inspection DAI will be used in the future to secure Cisco switches from MITM attacks. The second successful security method for Man-in-the-Middle attacks is cryptography (encryption). The encryption of traffic in an IP Security tunnel will help deter man-in-the-middle attacks. Intruders or hackers will only see the ciphertext using this encryption form [23].

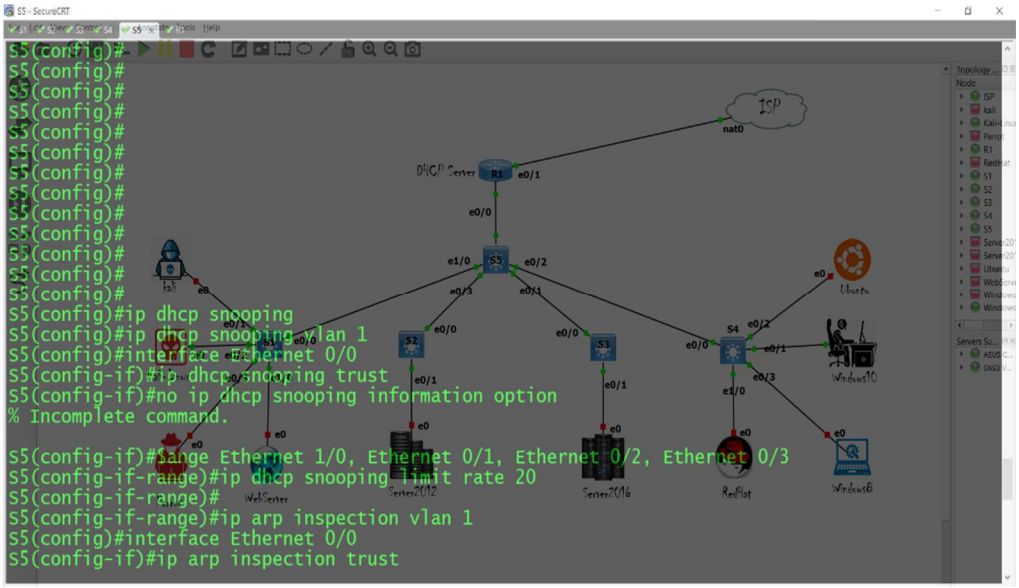



Fig.9. Man-in-the-middle attacks Mitigation

Fig.10. shows Mitigation of Man-in-the-Middle Threats. DAI stands for Dynamic ARP Inspection which is used to prevent MITM attacks on Cisco switches. Interface e0/0 is attached to the DHCP Server and contains the Mac Address Table of all hosts with dynamically allocated IP addresses.

Switch tests the actual host IP address and MAC address using the Table, and if the bot address is right, the packet is allowed.

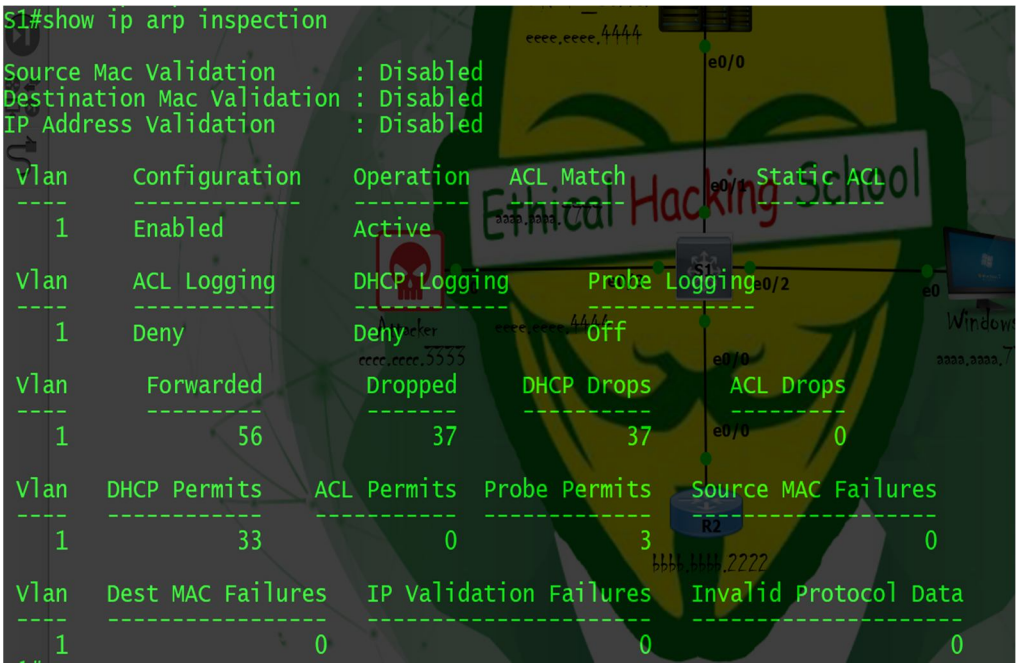



Fig.10. Man-in-the-middle attacks Mitigation Verification

*H. DoS (Denial of Service) Attack Mitigation*

The threat of DoS (Denial of Service) attacks can be reduced with the following techniques:

1) *Anti-spoof Features:* Proper configuration of anti-spoof features on routers and firewalls can reduce the risk of DoS attack. This configuration includes filtering to an RFC 2827 level. In this way, hackers would not be able to mask their identities, and they will not attack.
2) *Anti-DoS Features:* configured anti-DoS (Denial of Service) features on routers and firewall limit the effectiveness of an attack. Anti-DoS features often involve limiting the number of half-open TCP connections that a system allows at any given time.
3) *Traffic rate-limiting:* Some ISPs provide the implementation of traffic rate limiting. In filtering, the amount of unnecessary traffic that crosses the network segments at a certain rate is limited.

Mitigation DDOS Attack what Storm Control Configuration[17]

S1(config)# interface ethernet 0/2
S1(config)# storm-control unicast level 90
S1(config)# storm-control multicast level 90
S1(config)# storm-control broadcast level 90

if attack hoping form Interface Ethernet 0/2 automatic port goes to err-disabled Mode and shut down the port and Mitigating the DDOS and DOS Attack.

*I. Securing Remote Access Netowrk Devices*

Authentication, authorization, and accounting (AAA) access control using line passwords, a local security database, or remote security server databases is supported by Cisco networking (Cisco 2005) devices. Using the username XYZ and the powerful password command, the local security database is installed on the router for a community of network users.[12]

1) Users must enter username and password.
2) Usernames and passwords are transmitted through the network to the RADIUS server.
3) For remote access protection, we use SSH in this thesis. Recognize The user's authentication has been effective. Abandon On the local Database and AAA Server, the username and password are invalid.

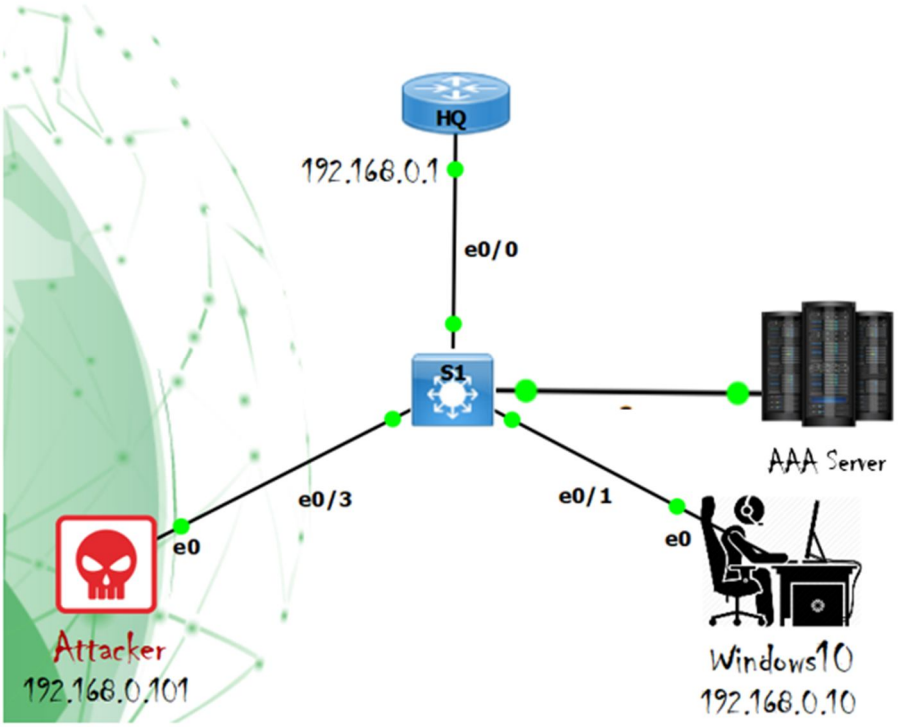



Fig.12. Access Network Devices

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue III Mar 2021- Available at www.ijraset.com*

*J. AAA With TACACS+ Server Configuration*

"The TACACS+ server discussed in this paper was written by Devrim Seral and can be downloaded from www.gazi.edu.tr/tacacs"

```
# tar zxvf tac_plus_v9a
# cd tac_plus_v9a
# ./configure
# make tac_plus
# make install
```

After compiling and installation, copy default configuration to the /etc directory and open it on any text-editor.
The following sections will explain each part of the configuration in details

```
###################################################################
# Default Config
###################################################################
# Key, very important
key = this should belong random string
# Use /etc/passwd file to do authentication default authentication = file /etc/passwd
# Accounting records log file
accounting file = /var/log/tacacs/tac_acc.log
```

The "key" directive is the first configuration line, and it specifies the mutual secret that will be used by all devices and the TACACS+ server. The TACACS+ needs to be the same on the devices and the server in order for TACACS+ to function efficiently. The next line shows the TACACS+ server the location for authentication; in this case it looks into the local UNIX /etc/passwd file. Finally, the TACACS+ server writes the accounting logs, which will be setup to log command execution and logon/logoffs to all devices

The next configuration is for users and groups:

```
###################################################################
# Group Definitions
###################################################################
group = netadmin { default service = permit service = exec {
priv-lvl = 15
} }
group = users {
default service = deny service = exec {
priv-lvl = 1
} }
```

To keep things simple, two groups will be used, a privileged group and a non-privilege group. The "netadmin" group in the configuration code will include all network administrators who need enable access to the devices, and is granted privilege level 15, this is the highest level of access on Cisco devices.

Users configuration:

```
# Netadmin users
###################################################################
user = bjones {
member = netadmin
}
###################################################################
# Unprivileged Users
###################################################################
user = sjones { member = users cmd = show { deny ip
deny tacacs permit .*
}
cmd = quit {
permit .*
```

```
}
cmd = exit {
permit .*
}
cmd = logout {
permit .*
}
cmd = ssh {
permit 192\.168\.1\.[0-9]+
deny .*
} }
```

In the first section of the code above we place the user “bjones” in the netadmins group, to grant privilege level 15 on all devices on the network. “bjones” also exists in the local Unix /etc/passwd file, and it’s the same case for all users whom company wish to grant access through TACACS+. The next section of code is unprivileged user “sjones”, in which level privilege granted. The group members on the TACACS+ server has a default deny statement, by so doing, no commands are allowed default. Users are allowed to run nearly every “show” command for debugging purposes, but not given the privilege to see any IP or TACACS+ information. And also SSH is allowed to machines on 192.168.1.0/24 subnet, with use of a regular expression in the Secure Shell (SSH) section. Finally, exit is allowed from the router, using any of the three commands that allow logoff. This section could be modified to fit company needs. Once the configuration file is adjusted to fit company needs, the TACACS+ command can follow:

# /usr/local/sbin/tac_plus -C /etc/tac_plus.cfg -d 248

The “-C” options shows the daemon the location of the configuration file while the “-d 248” is the debugging level, which is set to 248, giving plenty of information in the logs (see the tacplus man page for more details). User account should be created on the system and added to the tacplus.cfg file. Thus, it is recommended to have minimum of two TACACS+ servers and use of "rsync" for user accounts synchronization and TACACS+ configuration. IOS Configuration The section below configuration can be added to all of the IOS (Internetwork Operating System) based network devices (primarily routers and switches). Proper orderliness should be ascertained when putting the commands; otherwise, someone could be easily locked out of the device. Firstly, setup the TACACS+ servers:

tacacs-server host 192.168.1.5 tacacs-server host 192.168.1.6

tacacs-server key this should belong random string The device uses the first server on the list if available, and then uses the second, and so on. The key should be set to the same value as set on the TACACS+ server. The next line of configuration codes creates a local user; called “admin”, with privilege level of 15, and a good password:

Username Admin privilege 15-password ACDI@123

This is the username/password pair that is needed to be use if the TACACS+ server is unavailable. Local account IS needed in order to provide remote access via SSH only, and providing this local account will allow telnet access turned off to the device while still allowing access if the TACACS+ server is unavailable.

The AAA configuration code:

```
aaa new-model
aaa authentication login default group tacacs+ local enable
aaa authorization exec default group tacacs+ local none
aaa authorization commands 0 default group tacacs+ local none
aaa authorization commands 1 default group tacacs+ local none
aaa authorization commands 15 default group tacacs+ local none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacac+
```

The configuration above directs the device to handle all interactive user logins and what users will be able to do once logged in. The first line creates a new AAA schema, which allows user to enter all commands that follows.

The second line which is the authentication tells the device that once a user logs in it will confirm the username and password against the TACACS+ server, then check through a local username and password database, and finally, it defaults to the enable password. The only period it defaults to the enable password is when local username is not setup. The exec and command authorization work the same way. [cisco 2020]

## V. CONCLUSION AND FUTURE SCOPE

Because security is a long-term issue, Network Engineer need to develop a security strategy Educating employees on best practices is a healthy way to start. When putting together a security strategy, it's vital to begin with the most obvious safeguards and then move on to equipment worthy of the most sophisticated safeguards. AAA Services, for example, can offer privileged-EXEC authentication and a greater degree of scalability than line-level equipment. Other straight forward steps include: protection of servers and routers by using one-time passwords and allowing only authorized users to get to routers, by applying authorization systems based on TACACS+ or RADIUS. Administrators can also set up a framework to handle incoming traffic, which can include DoS attacks on router control processors. Operators should switch off redundant and unneeded resources in general, even though this means shutting off server functionality. Finally, the growth of physical technology, as well as its increasing importance to an enterprise, has necessitated the need to physically defend the networks themselves, not just from cyber-attacks but also from physical attacks. Implementing policy-based protection further adds to the security arsenal's benefits by automating the security philosophy's execution and reducing the risk of user error in network security.

*1)* Focus on best practices of the using Computer and internet to protect company assets.
*2)* All network devices should have an ACL (Access Control List) that only allows network management workstations access to the device.
*3)* The TACACS+ server should be behind a firewall that only allows TACACS+ traffic (TCP port 49) in from all network devices.
*4)* To better avoid man-in-the-middle attacks that use ARP spoofing techniques, administrators can use the port authentication function and hardcoded MAC addresses on switches and routers.
*5)* Finally, network administrators should stay up to date with the latest threats and attacks, monitor their network security architecture and see if it is vulnerable to the current threats and attacks, and then revisit the security design or strategy and make the necessary changes.

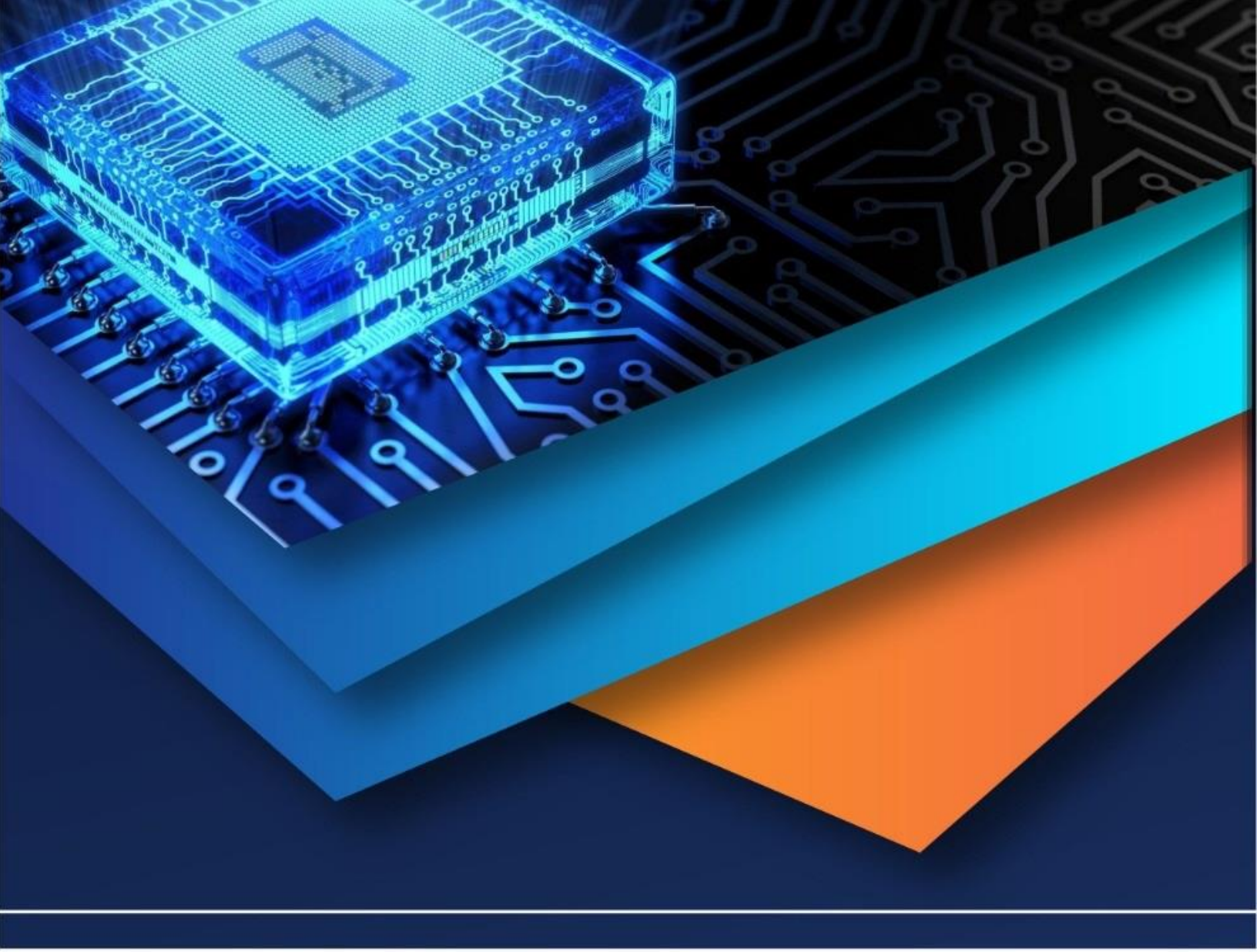
## VI. FUTURE SCOPE

In the future, an authentication module can be coupled with the trust base scheme, to immune the network against other attacks too. This work may be extended to mitigate combined attacks in the routing path by evaluating other protocols instead of using SSH, AAA port-security dynamic APR Inspection protocol. The future work can also deal with the 802.1x performance analysis of security protocols in terms of energy consumptions and their end-to-end delay. As there are a lot of constraints in the sensor networks which need to be taken care of for the proper evaluation of the lifetime of the network.

## REFERENCES

[1] Patel, A., Patel, N. and Patel, R(2015), “Defending against Wormhole Attack in MANET”, IEEE Fifth International Conference on Communication Systems and Network Technologies, 674–678.
[2] Uday, Kumar., et.al “Analysis of Network Security Issue and Its Attack and Defence” Uday Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3), (2016)
[3] S.E. Smaha, Haystack: an intrusion detection system[A]. Aerospace Computer Security Applications Conference[C] (IEEE, 2002), pp. 37–44
[4] J.P. Anderson, Computer security threat monitoring and surveillance[A] (James P Anderson Co Fort [C], Washington, 1980), pp. 26–32
[5] C. Phillips, L.P. Swiler, A graph-based system for network-vulnerability analysis[A] (The Workshop on New Security Paradigms[C]. IEEE, 1998), pp. 71–79
[6] R.W. Ritchey, P. Ammann, Using model checking to analyze network vulnerabilities[A] (Proceedings of IEEE Symposium on Security and Privacy[C]. IEEE, 2000), pp. 156–165
[7] T. Bass, Multisensor data fusion for next generation distributed intrusion detection systems[A] (Proceedings of the Iris National Symposium on Sensor & Data Fusion[C]. Hopkins University Applied Physics Laboratory, 1999), pp. 24–27
[8] T. Bass, Intrusion systems and multisensor data fusion: creating cyberspace situation awareness. Commun. ACM 43(4), 99–105 (2000). https://doi.org/10.1145/332051.332079]
[9] J. Mcdermott, Attack-potential-based survivability modeling for highconsequence systems[A] (IEEE International Workshop on Information Assurance[C]. IEEE Comp. Soc, 2005), pp. 119–130
[10] W. Yuanzhuo, L. Chuang, C. Xueqi, et.al., Analysis for network attack-defense based on stochastic game model[J]. Chin. J. Comput. Phys. 33(33), 1748–1762 (2010)

[11] N. Poolsappasit, R. Dewri, I. Ray, Dynamic security risk management using Bayesian attack graphs[J]. Dependable Secure Comput. 9(1), 61–74 (2012)
[12] J. Theureau, Nuclear reactor control room simulators: human factors research and development[J]. Cogn. Tech. Work 2(2), 97–105 (2000)
[13] M.R. Endsley, Design and evaluation for situation awareness enhancement[J]. Proceed. Hum. Factors Ergon. Soc. Ann. Meet. 32(1), 97– 101 (1988)
[14] M.R. Endsley, Toward a theory of situation awareness in dynamic systems[J]. Hum. Factors 37(1), 32–64 (1995)
[15] Boyd J R. A Discourse on Winning and Losing[C]// Strategic game of 1987. 16. G.P. Tadda, J.S. Salerno, Overview of cyber situation awareness. Cyber Situational Awareness[M] (Springer US, 2010), pp. 15–35
[16] X.W. Liu, H.Q. Wang, H.W. Lü, J.G. Yu, S.W. Zhang, Fusion-based cognitive awareness-control model for network security situation[J]. J. Soft. 27(8), 2099–2114 (2016)
[17] U. Franke, J. Brynielsson, Cyber situational awareness a systematic review ofthe literature. Comput. Secur. 46, 18–31 (2014). https://doi.org/10.1016/j.cose.2014.06.008
[18] J. Gong, X.D. Zang, Q. Su, X.Y. Hu, J. Xu, Survey of network security situation awareness[J]. J. Softw 28(4), 1010–1026 (2017)
[19] D.E. Denning, An intrusion-detection model. IEEE Trans. Softw. Eng 13(2), 222–232 (1987) 21. H. Debar, M. Dacicr, Andreas wespi towards taxonomy of intrusiondetection systems. Comput. Netw 31(8), 805–822 (1999)
[20] G. Vigna, R.A. Kemmerer, NetSTAT: a network-based intrusion detection system. Journal of Computer Security 7(1), 37–71 (1999)
[21] B. Mukherjee, L.T. Heberlein, Network Intrusion Detection[M]. IEEE Netw., 26– 41 (1994) 26. J. Shi, S.Q. Guo, Y. Lu, L. Xie, An intrusion response method based on attack graph. J. Softw. 19(10), 2746–2753 (2008)
[22] Z.H. Tian, X.Z. Yu, H.L. Zhang, B.X. Fang, A real time network intrusion forensics method based on evidence reasoning network. Chin. J. Comput. Phys. 5(37), 1184–1193 (2014)
[23] X.H. Bao, Y.X. Dai, P.H. Feng, P.F. Zhu, J. Wei, A detection and forecast algorithm for multi-step attack based on intrusion intention. J. Softw. 16(12), 2132–2138 (2005)
[24] K. Ilgun, R.A. Kemmerer, P.A. Porras., State transition analysis: a rule-based intrusion detection approach. IEEE Trans. Softw. Eng. 21(3), 181–199 (1995)
[25] T. Bass, R. Robichaux, in Proc., of the Communications for Network-CentricOperations: Creating the Information Force (MILCOM). Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations (IEEE, 2001), pp. 64–70



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY