Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Journal of University Studies for Inclusive Research

Vol.5, Issue 28 (2024), 13515- 13532

USRIJ Pvt. Ltd

Prevent Attack for online educational system using Intrusion Detection System and Penetration Testing in SCRUM.

Dr. Anas Ahmed Nicola[1]	Dr.Muneer A.S. Saeed[2]	Dr.Aboubaker Y.A. Elmahadi[3]	Mohammad Algarni [4]
Future University –Sudan	Al-baha University–KSA	Al-baha University–KSA	Al-baha University–KSA
Anasnicola2018@gmail.com	moneer5000@yahoo.com	drbakryyousif@gmail.com	malgarni@bu.edu.sa

Abstract

Today's world hackers use different type of attacks for getting the valuable information, many of the intrusion detection techniques methods and algorithms help to detect those several attacks. Selecting system administrators, network administrators, audit managers and response personnel is much more important than the type of networking hardware. Although education provides the theoretical tools needed to understand and address security needs. The main objective of this research is to provide a complete method about security issues related to the cloud and proposed solution to fully protect it. Researchers identify key solution by developing the intrusion detection system (IDS), use tools, for research purpose. That tools are capable of detect and prevent the intrusion from the intruder. Information systems in the field of educational learning sectors are distributed and interconnected via local area and wide area networks. Intrusion detection technology allows universities to protect themselves from losses associated with network. Researchers have focused on to solve the problem by deployed validation software using scrum form by adding member in scrum team called penetration tester, the technique tool based on IDS.

Keyword: security management, software engineering, management, IDS, SCRUM software penetration.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

1. Introduction

Intrusion detection technology allows organizations to protect themselves from losses associated with network security problems, [1]. Intrusion Detection System (IDS) are Hardware and Software Systems that monitor events which occurred on computers and computer networks in order to analyses security problems.

IDS have become key component in ensuring the safety of systems and networks. IDSs automate monitoring and analyzing the attacks, [2, 3]. Nowadays with the spread of the Internet and online procedures requesting a secure channel, it has become an inevitable requirement to provide the security of such networks, [4]. Intruders who do not have rights to access these resources can steal valuable and private information belonging to network users. Snort's network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Nevertheless, Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. University networks designed using fiber optic-based backbone comprising of two rings on the two section Permanent Site, design City control sector, and College connect with same part. The network runs on Cisco and juniper Devices (Router, Firewall, CORE Switch, DMZ (demilitarize Zone) Switch, Split Switch, and Transparent Switch). The University proposal Network divided into two segments (LAN & DMZ network). All University client machines are connected to LAN network segment on CORE-Switch. However, the whole of the University Servers that hosted their services which are accessible in and outside their network are connected to DMZ (demilitarize Zone). This research will focus on solve this problem in scrum software validation form, IDS, by adding member in scrum team called penetration tester this penetration tester must use tools and test if the product is secure or not secure, then reporting it and be aware by penetration testing life cycle, tools, and process with high

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

level of skills in security issue and vulnerabilities must develop apps, which useful to create secure products in application client server, [5].

1.1 Background and related work

agile software development process, the usage of PETA methodology will result in identification of security vulnerabilities in the company IT landscape that will feed the security requirements in the product backlog [6], proposed an agile risk analysis method as a trade-off between agility and security for threat identification [7]. IDSs automate monitoring and analyzing the attacks [8]. Ismail & Ismail [9] proposed a framework of Intrusion Detection System (IDS) implementation using Snort application on campus network environment. Yi & Zhang [10-13], Master thesis provided analysis and compared security risk which is none prevent attack, researcher proposed an implementation of a campus network security system based on distributed network intrusion detection technology. Development Based on Penetration Testing In SCRUM, [14].

1.2 Stage of scrum development

Agile is incremental approaches that focus to customer satisfaction its have many form such XP, Kanban, SCRUM Kanban and SCRUM. Scrum provides the structure of roles, meetings, rules, and deliverables. To solve security issue in SCRUM will develop my Client-server application based on penetration testing in SCRUM in case Study by implement penetration testing phases already know my target.

2. Problem Statement

Network security issues have been a major challenge on distance learning (e-learning), mostly using firewall for protect malicious for long time. However, firewall does not have the ability to detect hostile intent or identify types of attack on allowed services. University Servers are on DMZ (demilitarize Zone) network, sometimes part of the universities using one server hosted all services and some using more than one servers connected together. These services are being public to everyone connected to the Internet. Therefore, these servers available for to students login

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

through platform online system study 24 hours available .Thus can be anytime be compromise by hackers that may lead to the breach of their security. This problem can be tackled by deploying Snort Intrusion Detection System and scrum penetration testing software on the universities DMZ. Furthermore, none – secure software product becomes official gate of the hacker for to gather information from online system database.

The following figure explain the proposal process of development based on penetration.

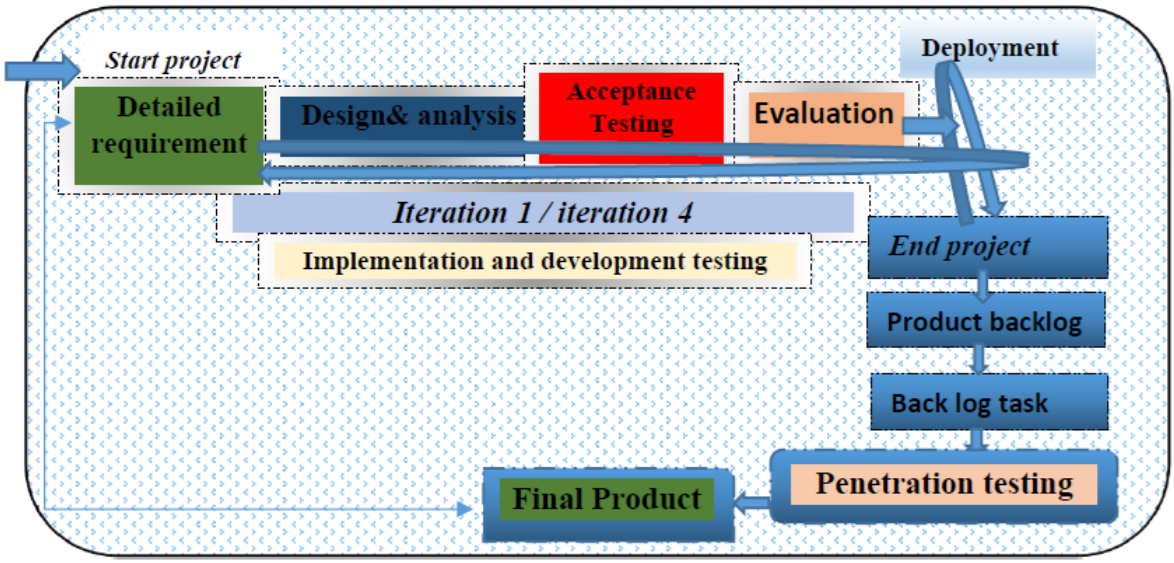


Figure 1. the proposal process of development based on penetration.

2.1 Justification

Development based on penetration testing led to product secure software by implement penetration testing life cycle model.

2.2 Requirements

Advanced client server taster requirement and control Server with high specification hardware, software, table1.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Table 1. Tester requirements

Tester requirements	
Component	Property
Operating System	Kali-Linux2021
RAM	16 GB more than
Processor	Intel core i7 -8Gen more than
Storage	SDD at least 320 GB more than

Table 2 Server requirements

Server requirement	
Component	Property
Operating system	Microsoft Windows-server 2016 -2023
RAM	E-RAM 64 GB
Processor	Xeon E5
Storage	500 GB, one Tera
Web-server	Microsoft internet information server (IIS) server version 10.0
.net framework	3.5, 4.0 and 4.5
Database management system DBMS	Microsoft SQl- server 2014.

2.3 Tools

Tools which need to use in this research help for monitoring and controlling, most popular operating system using for penetration testing for penetration testing. In addition, there is three

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

type of tools OPENVAS, NESSUS, and OWSAP ZAP its very powerful tools especially on variabilities analysis and assessment. Attack be on the middle location between client and Server flowing diagram will examine MITM concept.

Kali Linux is the most recent live disk security distribution released by Offensive Security. OpenVAS is a full-featured vulnerability scanner. Its capabilities with Unauthenticated and authenticated testing implement any type of vulnerability test. OpenVAS has been developed by the company Green bone Networks since 2006. As part of the commercial vulnerability management product family Green bone Company Appliance, the scanner forms the Green bone Vulnerability Management together with other Open Source modules.

OTP (OpenVAS Transfer Protocol) by the new stateless, request-response XML-based and generic OSP (Open Scanner Protocol), [11].

Nessus is a remote security scanning tools, which looking for computers and raises alerts, Nessus is not a complete security solution, and rather it is one small part of a good security strategy. Nessus does not actively prevent attacks; it is only a tool that checks your computers to find vulnerabilities that hackers could exploit [12].

ZAP

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible. Development based on penetration testing in SCRUM process in flowing flowchart.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

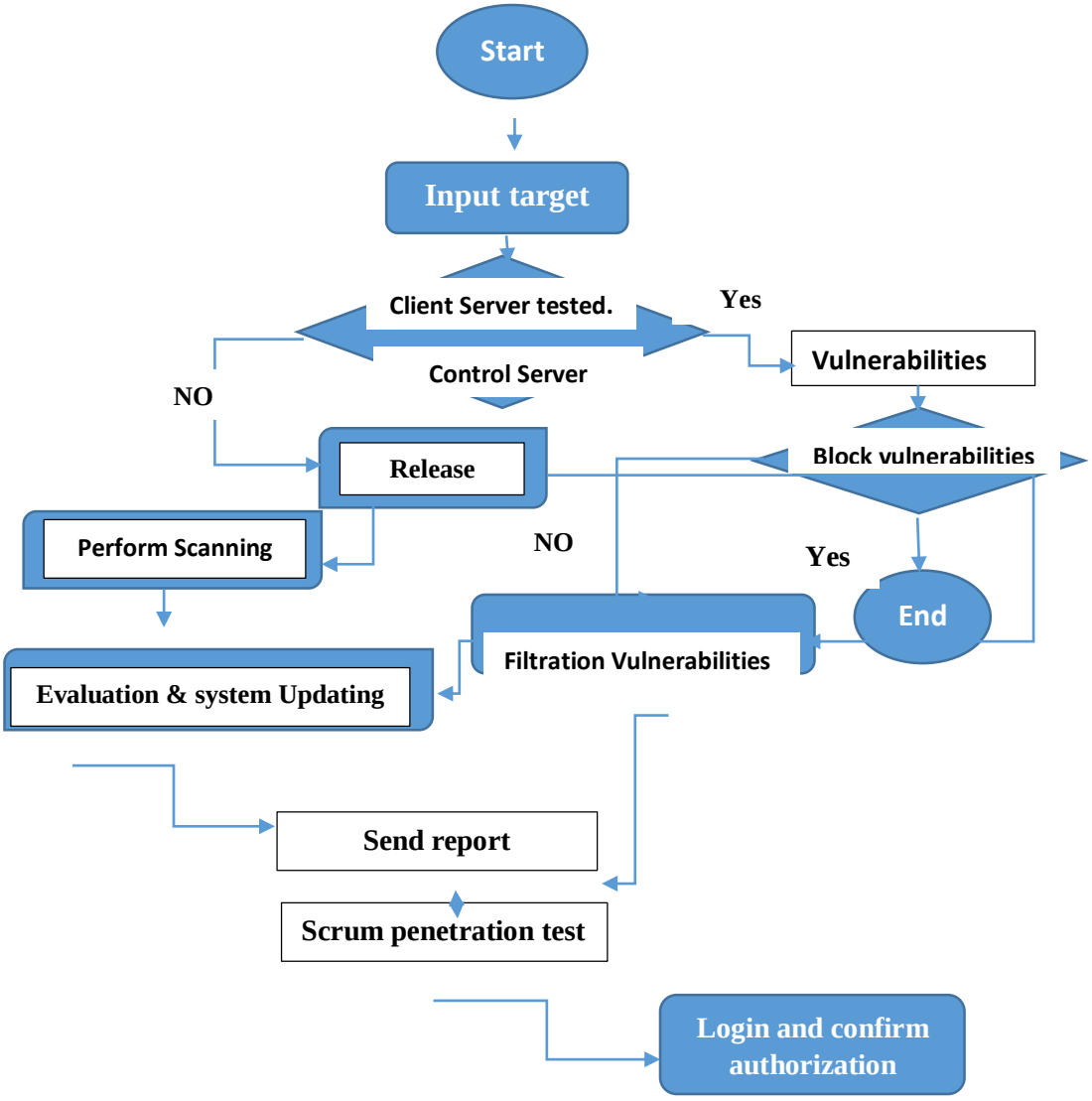


Figure 2 algorithm development

Researcher considering on this research OPENVAS, NESSUS, and OWSAP ZAP installed and using man in the middle attack (MITM), this type of middle between client and Server to listen and analysis requests its very powerful tools specially on variabilities analysis and assessment concept.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

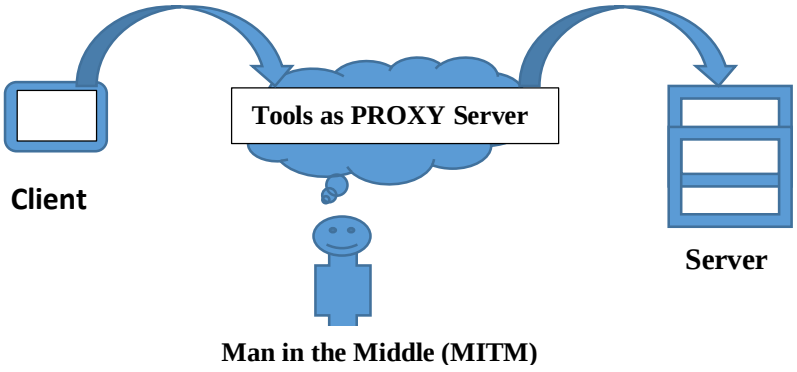


Figure 3. Man in the middle attack.

2.4 Products owner

- Always re-prioritize product backlogs and adjust long-term expectations such as release plans.
- Final decision on requirements issue.
- Approve or reject increments for each product.
- Have a leadership role.

2.5 SCRUM Master

- Helps clear obstacles.
- Creates an environment that helps teams self-organize.
- Gathers empirical data to adjust predictions.
- External protect your team from confusion and distractions and maintain a group flow.

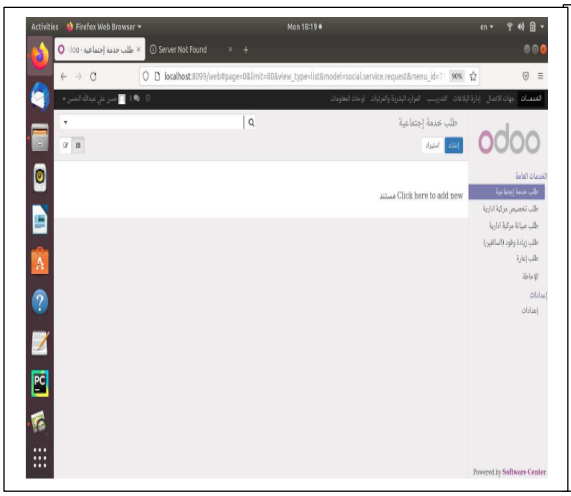
2.6 SCRUM Development Team

- Cross-functional (for example, members with test skills and other members previously not labeled as developers.
- Self-Organizing / Self-Management, No externally assigned role/ Domain Experts.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

3. Case Study Scenario

The case implemented in ERP system which developed by odoo9, for security Issue its not authorized to mention customer, and this product developed by (micro net), forsmart solutions company, this case study it's about highlighting problem and system its already released to customer.



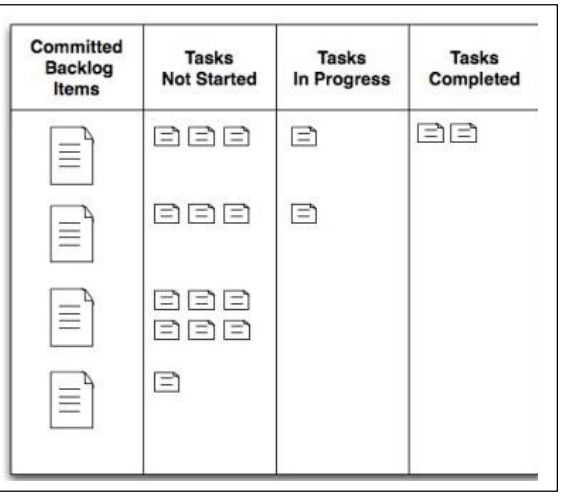


Figure4, main screen, system exploitation **Figure5, tasks monitoring**

In this step figure4,5 shown scanned all ERP system vulnerabilities by using zap and classified all vulnerabilities inapplication according to OWSAP top 10 which we mentioned before. in the following displayed all vulnerabilities important one which called Sql injection, it's very dangerous and its maybe lead to destroy the system reputation.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

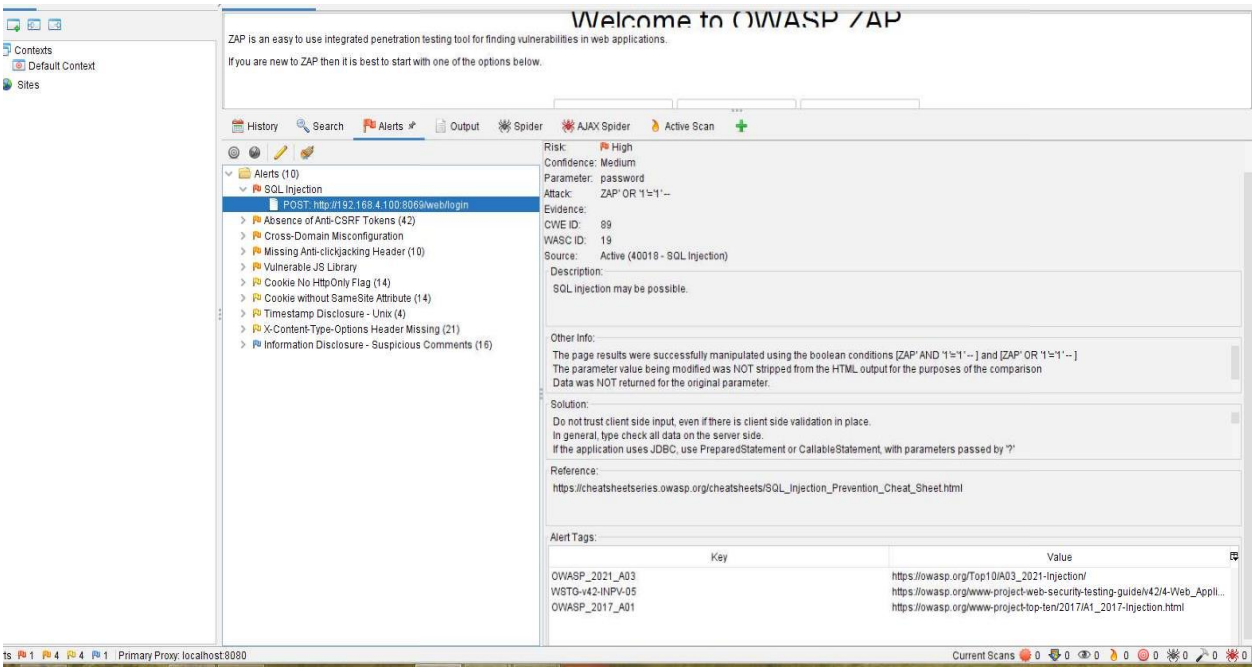


Figure 6. displayed all vulnerabilities and specially one called sql injection

3.1 SYSTEM IMPLEMENTATION

SNORT IDS various tools such as Snort Application, Pulled pork, Barnyard, Apache, MySQL, PHP, BASE, and ADODB Snort Application, implemented together with such as to achieve web base intrusion detection system for analyzing intrusive attacks.

3.2 SNORT APPLICATION

Snort application was installed on a server running on Operating System Ubuntu Linux 14.04. Snort captures attack data through snort. Config: file in /etc./snort directory. In this file we specified our block of IP address for DMZ network segment and parameters that specified link to our rule files that will be executed whenever there is suspicious traffic on the DMZ network zone.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

3.3 Explanation concepts words

Intrusion Detection System (IDS): Intrusion Detection System are Hardware and Software Systems that monitor events which occurred on computers and computer networks in order to analysis security problems.

DMZ: Demilitarized Zone (DMZ) is a segment of an Organizational Network that is accessible to general Public over the Internet.

• **Firewall**: Firewall is a system designed to prevent unauthorized access to or from a private network.

3.4 Snort Experimental Procedure

This Server will be connected to the DMZ Switch on interface and a Console Monitoring port. The minimum recommended hardware and software requirement for this experiment are as follows:

Required Hardware:

• Processor clock speed of at least 1.5GHz for an AMD Athlon or Intel Pentium 4brand processor.

• 16GB of RAM.

• At least 500GB of hard drive.

Required Software:

• Ubuntu Linux 14.04 Operating System

• Snort Application

• Snort Rules

A Snort application will be installed on Server running Ubuntu Linux 14.04. The latest version

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

of snort application can be downloaded and install from Snort web site (http://www.snort.org). Other tools that can be used with Snort are listed below.

A comprehensive working Snort system utilizes these tools to provide a web-based user interface with a backend database.

• MySQL is used with Snort to log alert data.

• Apache acts as a web server.

• PHP is used as an interface between the web server and MySQL database.

• BASE (Basic Analysis and Security Engine) is a PHP package that is used to view and analysis Snort data using a web browser.

Experimental Setup described snort application can be downloaded and install from Snort web site (http://www.snort.org). In order to evaluate performance of Snort-ids, we captured ICMP (Ping) traffic from the initiating System with 82.101.145.63 IP address from LAN network segment for the period of 15 minutes. We initiated ping attempt from System with 82.101.145.63 IP address to the System with 41.78.224.42 IP address on DMZ network segment.

Table 3. Comparison of Snort-Ids suspicious traffics against the total no of traffics captured from it.

Application	Initiating System	SNORT-IDS	% of Total Traffic
ICMP (Ping)	203	203	100%
Total no. of Traffic	203	203	100%

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Table 4. Comparison of Snort-ids suspicious traffics against the total no. of traffics captured from it.

Application	**Traffic Captured from Snort-ids System**	**Suspicious Traffic Detected by Snort-ids System**
ICMP (Ping)	203	205
Total no. of Traffic	203	205

3.5

Identity Management scenario

The scenario provides new face for to identify security management is defining and identity for each user (human or process), which is try to access the network system. The central concept of identity management system is using for a user to access all network resource after verifying single authentication, following figure illustrates entities and data flows in a generic identity management architecture. In this scenario for human users attacker try to access the network resource need to provide authenticate attributes, and authentication information such as passwords and biometric information. An attributes services manage the creation and maintenance such as for example, a user needs to provide a shipping address each time an order is placed at a new Web merchant, and this information needs to be revised when the user moves from network to others. The process of Identity management enables the user to provide this information from which time users login the client access server shown in proposal figure 7.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

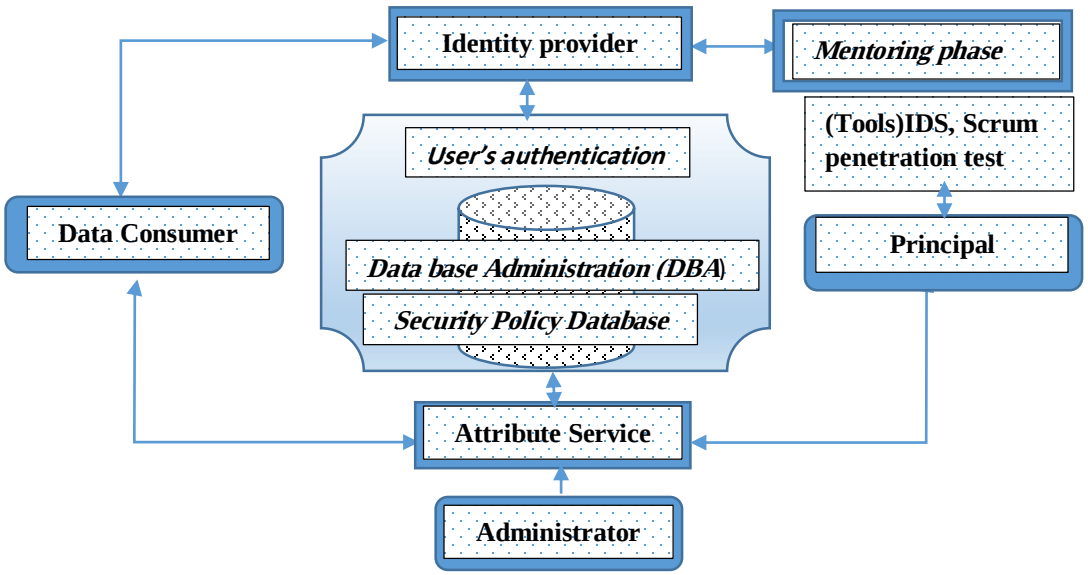


Figure 7. Generic Identity Management Architecture

Figure 8 illustrates entities and data flows in a generic identity management scenario Architecture. A Principals authenticate themselves to an identity provider. The identity provider associates authentication information with a principal, as well as attributes and one or more identifiers. An attribute service manages the creation and maintenance of such attributes. Administrators may also assign attributes to users, such as roles, access permissions, and employee information. Data consumers are entities that obtain and employ data maintained and provided by identity and attribute providers, which are often used to support authorization decisions and to collect audit information. Monitoring Phase, the tools scanning all the vulnerabilities attack network resources shown in Algorithms scenario proposed system platform online figure no 8.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

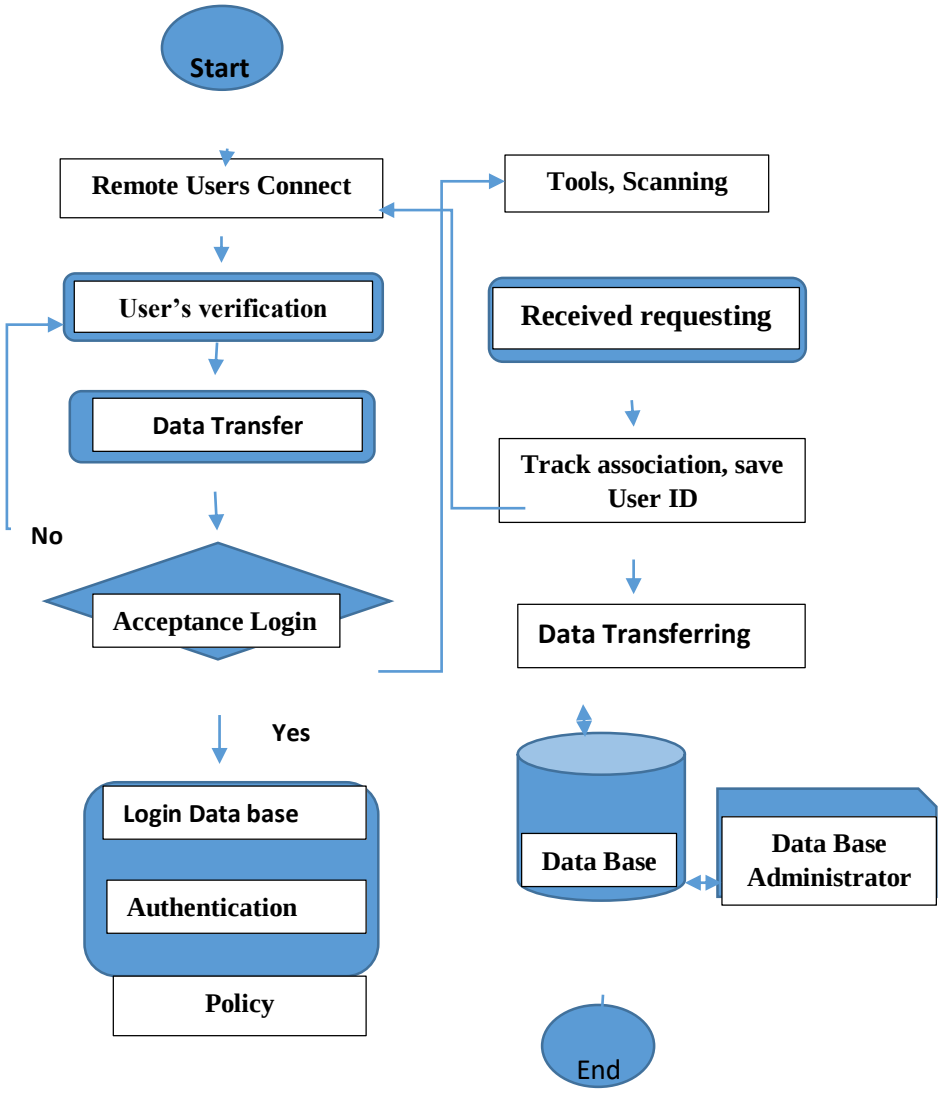


Figure 8, (a) Generic transmission diagram (from A) (b) Generic reception diagram (to B)

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

4. Summery

Now days, online learning interconnected via local area and wide area, government or private sector educational learning. The system of information system which is connected online provide potential avenues of attack by hacker, thus, internet visible systems are attempts to breach the security of the information system online. Intrusion detection technology allows organizations to protect themselves from losses associated with network security problems. Network security issues have been a major challenge for to protect the system online learning. These issues of network insecurity can be overcome by deploying Snort Intrusion Detection System with scrum penetration on the University DMZ network for effective.

5. Conclusion

Network security issues have been a major challenge on online learning for long time, mostly university protect themselves from malicious hackers using firewall. However, firewall is limited to identify the malicious hackers and prevent attacks on allowed services. These services are being public to everyone online learning system connected to the internet, Therefore, the system which is has been available 24 hours for to student's login through platform. However, these services can any time be compromised by hacker that may lead to breach the security server, therefore on this paper focusing furthermore for implementing the risk of educational learning system exploring the possibility of implementing mixed tools and proposed algorithms-based detection technique for better detection of suspicious traffic. By provided tools algorithms for to prevent and scanning before and authenticated user's id, analysis methods which is combined verified better result proposed to online educational system learning universities.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Reference

[1]. Mohapatra H. (1). at veer surendra sai university of computer science and technology. 2005

[2]. computer security divition information communication laboratory national institude of standards and technology gaithersburg, MD 20899-8930. 2007

[3]. Bace, R. (1999). An introduction to intrusion detection and assessment for system and network security management. ICSA Intrusion Detection Systems Consortium Technical Report, pp 236-241.

[4]. Bace, R. (2000). Intrusion detection, First Edition, Macmillan Technical Publishing, Indianapolis, USA, (ISBN 1-57870-185-6), pp 23-35.

[5] Usman Rafi, Tasleem Mustafa, Nayyar Iqbal, Waseeq-Ul-Islam Zafar: US-Scrum: A Methodology for Developing Software with Enhanced Correctness, Usability and Security:International Journal of Scientific & Engineering Research, Volume 6, Issue 9, September-2015 377 ISSN 2229-5518 .

[6] hacking with kali jamesbindner 2014

[7] Software Testing and Quality Assurance author Dr.Salah malik 2021

[8]. Bace, R. (1999). An introduction to intrusion detection and assessment for system and network security management. ICSA Intrusion Detection Systems Consortium Technical Report, pp 236-241.

[9]. Ismail, M.N. & Ismail, M.T. Framework of Intrusion Detection System via Snort Application on Campus Network Environment, proceedings of IEEE International Conference on Future Computer and Communication (ICFCC), pp 455-459. 2009

[10]. international journal of network security and its applications, DOI: 10.5121/ijnsa 2010.2411

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

[11]. Xiong, C.H. & Peng, Z. Applied Research on Snort Intrusion Detection Model in Campus Network. Proceedings of IEEE 2012 Symposium on Robotics and Application, pp 596-599. 2012

[12]. Sumani, R. and Vikram, S. Snort: An Open Source Network Security Tool for Intrusion Detection System in Campus Network Environment, proceedings of IJCTEE, Volume 2, pp 212-214. 2013.

[13]. Garg, M. Intrusion Detection System in Campus Network: SNORT- The most powerful Open Source Network Security Tool, proceedings of International Journal of Advancement in Engineering Technology, Management & Applied Science, Volume 1, pp 913-918. 2014.

[14]. Samaila Abubakar Gumbi, “Intrusion Detection System (Usman Dan fodio University Case of study) Master thesis -2021,future university , Mohammed Fathelrhman Bashir Ismail, “Development Based On Penetration Testing In SCRUM” , Master thesis, july 2022