# Penetration Testing and Mitigation of Vulnerabilities Windows Server

Deris Stiawan[1], Mohd Yazid Idris[2], Abdul Hanan Abdullah[2], Mohammed AlQurashi[3], Rahmat Budiarto[3]

*(Corresponding author: Deris Stiawan)*

Department of Computer Science, Universitas Sriwijaya, Indonesia[1]
Department of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia[2]
College of Computer Science and Information Technology, Al Baha University, Kingdom of Saudi Arabia[3]
(Email: deris@unsri.ac.id)

*(Received Jan. 15, 2015; revised and accepted Apr. 11 & Aug. 24, 2015)*

## Abstract

Cyber attack has become a major concern over the past few years. While the technical capability to attack has declined, hacking tools - both simple and comprehensive - are themselves evolving rapidly. Certain approaches are necessary to protect a system from cyber threats. This work engages with comprehensive penetration testing in order to find vulnerabilities in the Windows Server and exploit them. Some forms of method penetration testing have been used in this experiment, including reconnaissance probes, brute force attacks based on password guessing, implanting malware to create a backdoor for escalating privileges, and flooding the target. This experiment was focused on gaining access in order to ascertain the identities of hackers and thus better understand their methods and performed penetration testing to evaluate security flaws in the Windows Server, which is a famous OS for web applications. It is expected that this work will serve as a guideline for practitioners who want to prepare and protect their systems before putting them online.

*Keywords: Mitigation, penetration testing, vulnerabilities, windows server*

## 1 Introduction

A definition of hacking is presented by [9, 25]. These sources also identify security violation trends in internetworking and their effects. More illegal activities such as hacktivism, hacking and exploiting weaknesses have been described by [12, 16, 29] offer a different perspective by highlighting the potential economic threats and impacts of cyber attacks. A growing problem, hacking activities combine easy to learn pentest with a variety of tools such as those offered by C.E.H [11]. Moreover, they use both simple and comprehensive tools (defined as 'Metasploit'), as defined by [5, 21]. This reinforces the findings of previous work [14] which compares attack sophistication with attacker skill knowledge.

Meanwhile, analysis by [6, 12, 18] highlights an explosion of security threats in recent years such as Trojans, viruses, worms, adware, spyware and DoS which are continuing to grow, multiply and evolve. According to [14] indicate the technical capability to attack tended to decrease. On the other hand, hacking tools are getting more effective and also increasingly available and accessible to the public. Moreover, attackers are able to detect vulnerabilities faster than security experts or vendors and can cause time delays by patching in vulnerabilities.

Research conducted by [26, 27] found that Windows Server has more serious vulnerabilities, as several of its services and daemons are unsecured and open to access. This lays open the possibility of exploitation. Additionally [32] located vulnerabilities in the Apache and IIS HTTP server on the Windows Server operating system. [28] conducted an attack scenario on the Windows Server.

In order to understand how to protect against and prevent attacks, it is useful to understand from the attacker's perspective what methods they will use, what goals they have and how they launch their attacks. This experiment takes improvised actions to highlight several types of attacks carried out such as: probes to obtain detailed information, brute force for guessing passwords, gaining privileges access and flooding the target to reduce the availability of services.

The remainder of this paper is organized as follows. Section 2 presents the related works. Section 3 presents the taxonomy of the attack this experiment is concerned. Section 4 describes experimental experiments. This section deals with data collecting and an attack scenario including scanning and exploitation for mitigating vulnerability. Finally, Section 5 offers a conclusion and suggestions for future work.

## 2 Related Works

Penetration testing has been described in different ways since 1989 by [24]. New methods and approaches are continuously being expanded from year to year. In 2001, [7] described certain steps needed to prevent threats and convey the importance of understanding the mindset of an attacker, as well as their methods and goals. In line with that, [2] has suggested a methodology to ensure that the penetration testing exercise is reliable, repeatable and reportable.

Analyses and predictions by [12, 18] indicate that there has been an explosion of security threats in recent years. This has been corroborated and previously predicted by [17, 19], which describe a future war based on cyber attacks. More recently, [23] has predicted and analysed cyber attacks in the context of further security violation trends. Meanwhile, [10] has referred to Microsoft warning users about the strengths of character passwords such as: a combination of case sensitive letters and digits, maximum-minimum password age, and minimum password length.

Furthermore, it seems that every bug can cause vulnerabilities which are existent and undocumented, often never being revealed, discovered or exploited. From the attacker's perspective, vulnerability is an opportunity that can be exploited. A vulnerability database is a collection of records containing technical descriptions of vulnerabilities in computer systems. Common Vulnerabilities and Exposures (CVE) began in 1999 as a result of the adoption of a common naming practice for describing software vulnerabilities and including security tools and services as well as on the fixed sites of commercial and open source software package providers. We argue that dependencies exist between scanning phases and information holes from CVE vulnerability databases. This has consequences for access.

Additionally, work by [13, 15, 20] describes the benefits of CVE compatibility, integrating vulnerability services and tools allowing more complete security provision and more alert advisory services. Every month CVE MITRE receives between 150 and 300 new announcement alert and advisory submissions from ISS, Security Focus, Neohapsis, and the National Infrastructure Protection Centre. Currently CVE identifies compatible enablement data exchange between security products and provides a baseline for evaluating coverage of tools and services. There are thousands of information vulnerabilities within the CVE database. Unfortunately, time is required to make a patch release after exploitation has been found. Consequently, there is usually a a time delay between an exploitation identification and a patch and signature release. It can be argued that there are dependencies in the results between the scanning stages [15] and information vulnerabilities in the CVE database. This means that the vulnerability could be a security flaw exploitable by attackers.

In this experiment followed four dominant categories of attack: Probes, Remote to Local (R2L), User to Root (U2R) and DoS as widely used in the field of intrusion detection/prevention system, with reference to [3, 4, 8, 31].

## 3 Experiments

The dataset employed in this study was Intrusion Threat Detection Universiti Teknologi Malaysia (ITD UTM), as shown in Figure 1, available in [30]. All attacks were executed and infiltrated on ITD UTM. The network environment is set up for exploitation using Windows Server and two terminal clients running as attackers. They are connected to 3COM Superstack II 100 Mb/s, as shown in Figure 1.

### 3.1 Data Collecting and Procedures

Several steps must be taken to conduct these experiments. This work is an improvement on some of the advice offered by [22] and this research agrees with the argument expressed by [1], particularly on these problems: (i) recent trends and new methods of attack have been involved, (ii) control and guideline steps for penetration, and (iii) various methods of attack for penetration and mitigation become comprehensive. In this experiment, three weeks were spent collecting data and finding vulnerability within CVE and security communities. Moreover, five weeks was spent attempting penetration testing on the victim. There are some differences in the results obtained in the first and second data collection. The first data were collected directly from the server, regardless of the network broadcast. Conversely, the second data were collected using the hub terminal which also captured the broadcast network. Furthermore, this procedure was followed in this section:

1) To distinguish between normal traffic and attack, the attack was separated and divided into several stages based on time, machine target and method of attack.

2) Machine 10.10.10.1 is a NAT Firewall server that both allows and denies private traffic to and from the internet.

3) TCPdump is used to sniff real traffic. It uses the libcap library to capture packets and has the ability to consider the properties of an ideal as a packet sniffer. TCPdump produced raw data (pcap files) during experiments conducted via 10.10.10.30.

4) Machine 10.10.10.40 running on Snort IDS 2.8.5.2 (Build 121), PCRE ver 8.12. This is used to identify the threat as well as to compare attacks carried out which can be recognised by snort signature.

5) Two machine attackers, 10.10.10.15 (called Hacker XP) running on Windows XP SP3 and 10.10.10.20 based on Backtrack 4 (called Hacker BT) to penetrate Windows Server SP3 in 10.10.10.25.

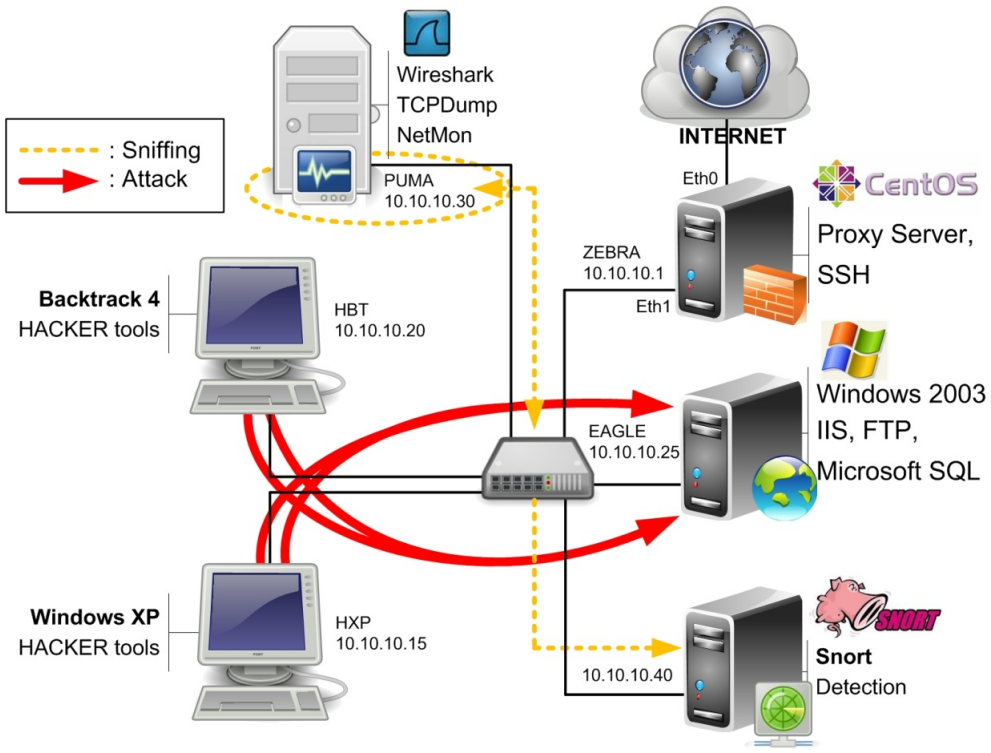



Figure 1: Topology of test bed environment

Meanwhile, in this experiment all attacks were executed on ITD UTM. The attack scenario for penetration is further illustrated below.

**Step 1. Scanning**

- Attackers probe the network 10.10.10.25 via GFI Scanning, Nessus, N-Stealth and Nmap;
- Attackers port reconnaissance of HTTP services via Nikto;
- Attackers find open port to potential penetration, 21 (FTP), 23 (Telnet), 80 (HTTP), 445 (SMB), 1433 (Microsoft SQL Server), 1026 (Remote Server).

**Step 2. Brute Force**

- Attackers attempt password of FTP & Telnet via brute-force tools;
- Attackers attempts to host 10.10.10.25 for guessing password remote access via TSgrinder;
- Attackers attempt SQL Ping and Brute force SQL Login;
- Attackers successfully find user authenticated of FTP;
- Nessus confirms user access "anonymous" enable and allowed in FTP;
- Attackers log in to the host via FTP Client.

**Step 3. Gaining privileges**

- Attackers try to escalate privilege to administrator level;
- Attackers attempt web attack via HTTP and launch "/.... access", "/ root access", "/etc/passwd", "/usr/bin/id", "/etc/shadow access" via HTTP port 80;
- Attackers attempts XSS attack - Attackers sniff the network via Cain Abel by utilising of ARP;
- Attackers launch man in the middle attack and SMB Unicode;
- Attackers add user "puma" password : 12345678 via console;
- Attackers add user "mike" password : 12345678 via console;
- Attackers add user "john" password : 12345678 via console;
- Attackers create directory /mkdir "tools" in 10.10.10.25 via console;
- Attackers crack root level hashing password via localhost;
- Attackers upload some files including Trojan to the victim via FTP;
- Attackers successfully implant the netbus to create backdoor via FTP;
- Attackers execute and enable netbus via remote desktop, then implant keylogger.

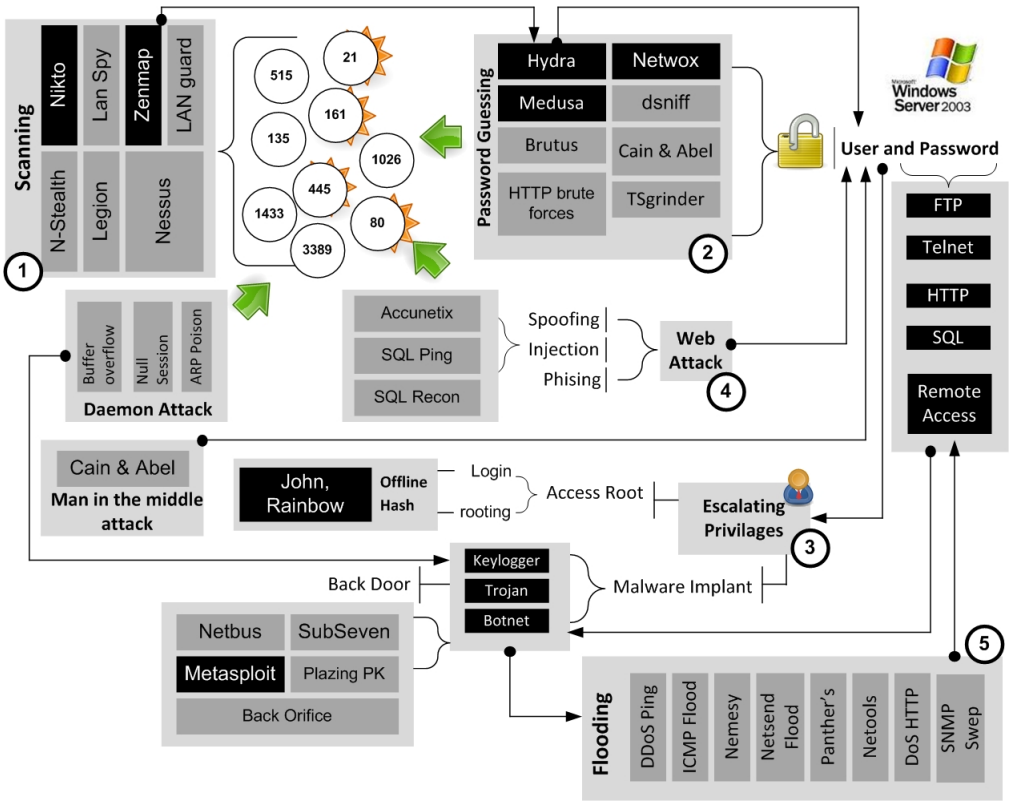



Figure 2: Attack scenario diagram

**Step 4. DoS**

- Hacker XP and Hacker BT send a large number of ICMP packets repeatedly to flood 10.10.10.25;
- Attackers launch attack LAND via sending TCP SYN;
- Attacker flood packets using forged source;
- Attackers flood traffic host victim via UDP to slow down the response of the target.

## 3.2 Scanning

An attacker's first steps need to obtain information about the victim and its environment. They map the network to determine the target, followed by scanning in order to interrogate and reconnoitre the victim. The attacker tries to map out the IP Address/subnet mask information and operating system that is in use, what services daemons are actively run and the kernel/services pack used. In other words, the attacker tries to map out the infrastructure and resources of the network.

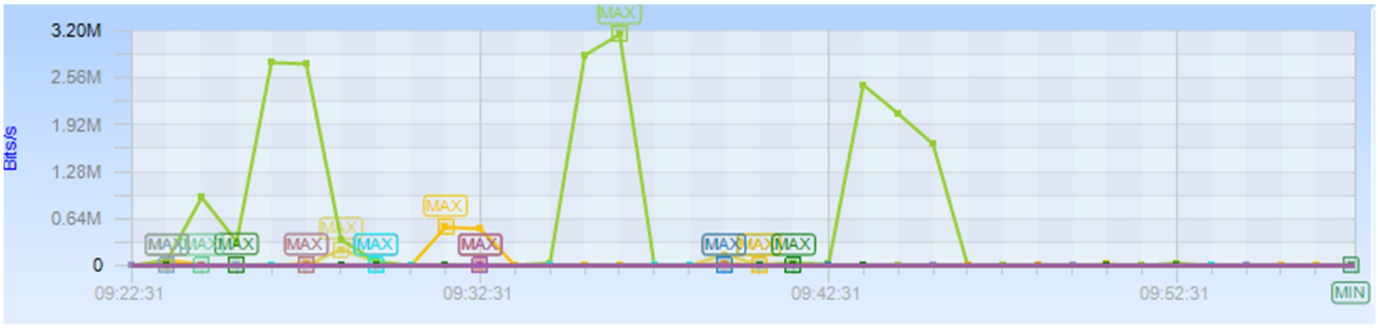
In this stage, several tools and scenarios are used to gather information, and findings known as vulnerabilities are mixed and combined to achieve the expected results. Some of the measures are adopted to enable these tools to complement each other. Moreover, none of these tools can provide all the detailed information. They have limitations particularly in translating the feedback packet from the target host. Some tools identify the open port and the rest are closed.

As mentioned in Section 3.1's attack scenario, some open ports were found and used to scan data coming from such ports. The success of this process depends on the operating system and the application that is run on the server. Some tools are used in Hacker BT running Zenmap, Xprobe2, Nikto, HTTPrint, and Hping2. Meanwhile, the Hacker XP machine runs these tools: GFiLAN, Legion, Nessus, N-Stealth, X-Scan, and LanSpy, which is a comprehensive target and a slow mode of scanning. This stage of attack depicted in Figure 2 produces visualisation, as shown in Figure 3(a) and (b) below.

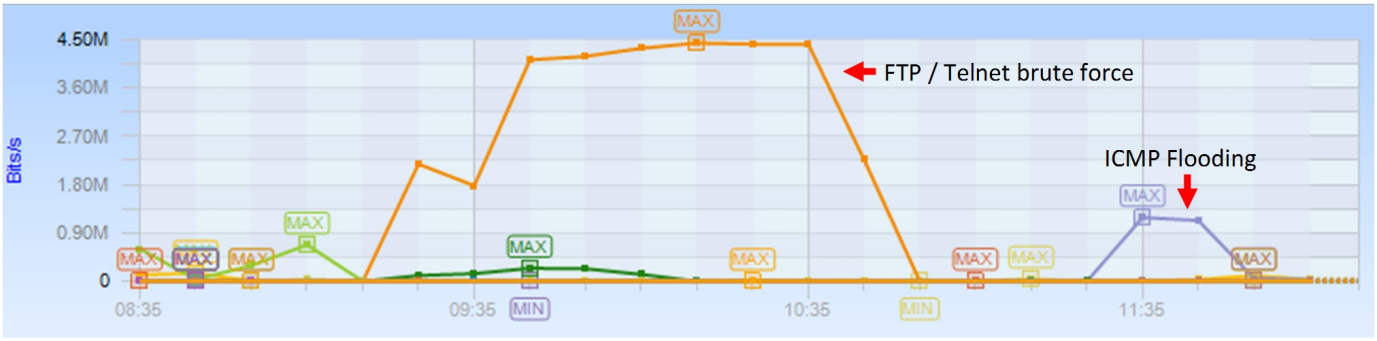
## 3.3 Vulnerability

This section presents vulnerabilities that arose during the scanning stages. From a hacker's perspective, searching for any kind information that can be exploited from the CVE database may identify vulnerabilities. It can be argued that there are dependencies between scanning and information holes within a CVE vulnerability database with respect to gaining access. The critical and medium risk vulnerabilities are as follows:

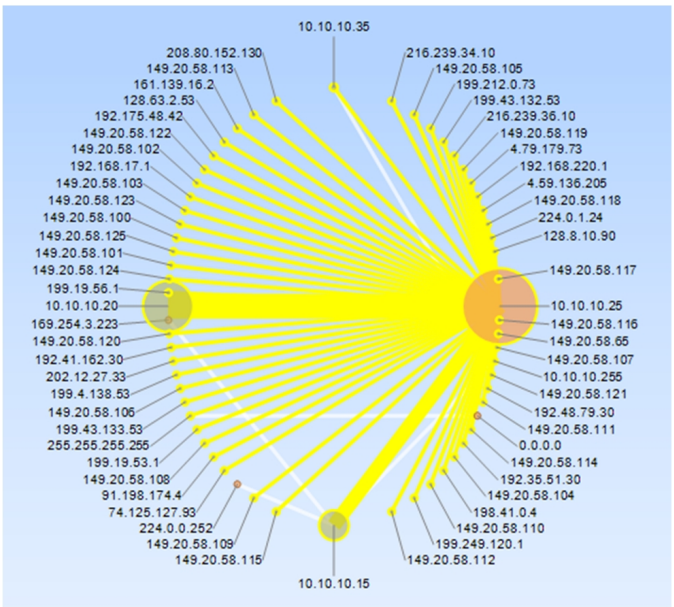
1) CVE-2011-1267, CVE-2011-1268, CVE-2011-0476 confirm SMB Server-Client to allow remote code ex-



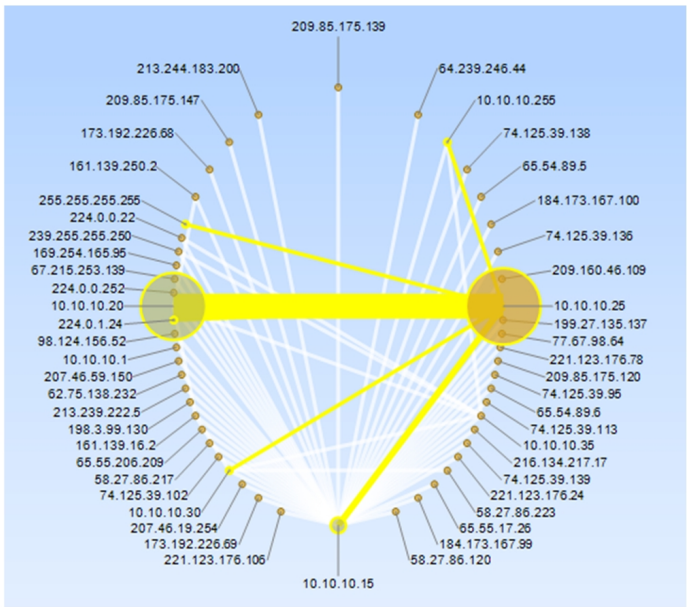

(a)




(b)




(c)




(d)

Figure 3: (a) Overall scanning traffic, (b) overall traffic of penetration stages. (c) refers to handshaking traffic attackers with victim in scanning stages and (d) shows penetration.

ecution if an attacker sends a specially crafted SMB response to a client-initiated SMB request.

2) CVE-2008-4250, RPC vulnerabilities allow remote code execution. An attacker could exploit this vulnerability without authentication to find arbitrary code & worm exploitations.

3) CVE-2006-5583 is vulnerable and can be exploited with regard to buffer overflow SNMP, allowing a remote attacker to execute arbitrary codes via a crafted SNMP packet via exec code overflow.

4) CVE-2006-3439 confirms vulnerability from buffer overflows. This attack allows remote attackers, including anonymous users to execute an arbitrary code via a crafted RPC message.

5) CVE-2006-0026 and CVE-2000-0071 is vulnerable to IIS. This attack can allow local and possibly remote attackers to execute arbitrary codes via crafted Active Server Pages (ASP) and allows a remote attacker to obtain the real pathname of a document.

6) CVE-2003-0352, CVE-2003-0003, Buffer overflow in a certain DCOM interface for RPC allows remote attackers to execute arbitrary codes via a malformed message, as exploited by the Blaster/MSblast/LovSAN and Nachi/Welchia worms.

7) CVE-2011-1247, Path vulnerability from Microsoft active accessibility enables local users to gain privileges via a Trojan horse DLL in the current working directory.

8) CVE-2011-0654, Buffer overflow in Active Directory services. This attack allows remote attackers to execute arbitrary codes or cause a denial of service via a malformed BROWSER ELECTION message.

### 3.4 Penetration Testing

The stages identified certain holes to be exploited from previous stages and launched the attack, a so-called User-to-Root (U2R) attack. This extends the user's privilege to administrator/root to obtain full authorization access. The attacker can create the new user, implant the malware, create the backdoor and clean their track from the log server. Normally, the attacker starts with accessing a normal local user account then later exploits vulnerability to privileges. Moreover, the attackers also launched brute force for guessing the password, cracking the password, web injection and man in the middle attack.

This step is called the Remote-to-Local (R2L) attack. Request packets were sent to a machine over a network which then exploits machine's vulnerability to illegally gain local access as a user without privileges. In this stage, the attacker focused on brute force in order to gain access and escalate privileges. According to the scenario presented in Section 3.1 and Figure 2 above, attackers discovered multiple vulnerabilities. They successfully found the legitimate users then created a new user, and successfully used a brute force FTP log-in resulting in the malware to successfully create a backdoor. Figure 2 shows illustrated penetration of Windows, as follows:

1) Hacker BT and Hacker XP attempted to conduct surveillance whereby the attacker tries to map out of IP Address/subnet mask information, operating system being used, and which services are running in 10.10.10.25. In other words, these stages are called probes or scanning to map out and reconnoitre the victim's network infrastructure. Nessus, Nmap, Nstealth, Legion and GFILanGuard are used to communicate with the data base server several times to check available updates of existing vulnerabilities. There are some potential vulnerabilities to be exploited which are as follows:

| PORT | STATE | SERVICE |
|---|---|---|
| 21/tcp | open | ftp |
| 23/tcp | open | telnet |
| 80/tcp | open | http |
| 111/tcp | open | rpcbind |
| 161/udp | open | snmp |
| 445/tcp | open | microsoft-ds |
| 1027/tcp | open | IIS |
| 1433/tcp | open | ms-sql-s |

2) Specific techniques are used to escalate privilege, attempt password one by one via guessing, theft, sniffing and cracking the password direct to target. From the attacker's perspective, the challenge is to find the legitimate user and implant the Trojan to create a backdoor. The attackers must prepare a dictionary/word list, accuracy in selecting the dictionary is a must and cracking the password in time depends on the length of the password's characters. Otherwise, a brute force password via user "administrator" can be successfully performed of FTP by Hydra and failed attempt Telnet.

```
root@bt:~# hydra -l administrator -P
passdict.txt 10.10.10.25 ftp
[DATA] 16 tasks, 1 servers, 26870 login tries
(l:1/p:26870), ~1679 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 10.10.10.25   login:
administrator   password: intrusion
```

Moreover, the attacker launched TSgrinder to guess the password of the remote desktop. This failed and the dsniff was launched to the sniff user and password in broadcast network. HTTP brute force was used to guess the web directory. Meanwhile, the traffic attempt of brute force is dominant, as shown in Figure 3(a).

3) The attacker launched powerful tools such as Metasploit, Cain and Abel and Netcat to find the command prompt. They attempted to obtain privileges and attack launches via the command prompt, which freely creates a new user account and removes the traces. In this step, after obtaining a valid user, the attackers attempted to implant a Trojan to create the backdoor. They successfully implanted the Netbus Trojan and executed the "Abel" in an ARP poison attack. New users "puma", "mike" and "john" were created before the attackers attempted to crack the administrator password via John the Ripper and Rainbow.The attacker attempted an IIS attack via buffer overflow and SQL injection to break into a system. During that time, they tried to find the weaknesses and structure of the website via SQL injection in order to ascertain certain information and the error page from HTTP server.

4) Finally, to reduce availability the attackers continuously launched DoS attacks by flooding the ICMP and UDP. They were successful; the system could not respond and crashed after a few minutes. Repeated requests meant that the target was unable to handle the service and reduce the availability. The results of this scenario are shown in Figure 3(b) below.

# 4 Experiment Results and Discussion

Snort is used to identify and recognize threats from data traffic. It produces lots of logs contained in machine 10.10.10.30 "var/log/snort" directory. The scanning stages produces 677,914 packets and snort identified 45,139 alerts among them as threats. Meanwhile, in the penetration stage there were 33,865,687 packets and 265,200 were identified by the existing signature as a threat.

## 4.1 Attack Pattern

This section presented some sample attack patterns (Probe, U2R, R2L and DoS) from the experiment. Every alert was compiled via snort and pcap files. In this case, the pcap file was extracted and revealed some features such as: time stamp, source IP Address, destination IP Address, Protocol, size of protocol, Flag of Protocol, Total Length of packet and content of packet.

From observations that were made, specific characteristics of line to line attacks from can be recognised from the header and payload of packets. They have a unique pattern which tends to iterate in a particular line. Some characteristics of pattern are as follows:

1) Web scanning, especially HTTP and HTTPS reconnaissance, has the following characteristics: (i) each packet has a source and destination IP address and port numbers are spoofed, (ii) connections are said to be state and number of ports accessed by a single source, (iii) TCP flags are used randomly during the attack, (iv) packet size and packet length are changed frequently.

2) Netbus have these characteristics: (i) computer victims or servers typically listen on specific ports waiting for instructions from attackers, (ii) they use TCP protocol and port address 12345 to communicate and each message has a fixed-length header, (iii) the variable-sized data section follows the header and its size is specified in the message-size field of the header, (iv) the flag is fixed to the computer victim during the communication process.

3) Brute force of FTP: (i) this attack generates repetition response, particularly content of flags and protocol length, (ii) anonymous user login attempts will occur, (iii) the port address and flags are fixed during attack, (iii) data connection uses the well-know port 20 at the server side and control connection is established on port 21.

4) Scenario of NetBIOS NULL session attack tries to attack enumeration user and getting administrator level, it have characteristic: (i) Packet size, total length and flags fixed with randomly generated on Port 139 (NetBIOS Session Service) and Port 445 (Common Internet File System), (ii) The flag value is fixed and dominate by NetBIOS protocol session, (iii) Vulnerability in Port 445 is possible to launched SMB or Common Internet File System (CIFS) attack, (iv) The TCP protocol are fixed during attack attempt, NetBios Session Services (NBSS) port 135, Remote Procedure Call (RPC) port 137, NetBIOS Name Service port 138 and NetBIOS Datagram Service port 139.

5) The characteristics of man in the middle attacks are: (i) the ARP packet lack flag and protocol length value, (ii) the ARP broadcasts from the attacker to all IP addresses in one subnetmask and without information of port source and destination, (iii) NetBIOS datagram fixed used port 138 and NetBIOS Name Service port 137.

Meanwhile, the number of rows that were generated by snort due to repetition of the same information were observed. This can be simplified by initialising the signature-id and priority. Each alert comprises of signature-id, priority, source of IP Address, source port, destination of IP Address, destination of port address, timestamp, Time To Live, Type of Service, IP Length and Datagram length.

## 4.2 Identify of Probe

In this phase, snort confirms that there are 4078 lines identified as "SCAN FIN" as shown in Figure 4 below and Table 1 shows the total attempts at probe attacks.

[**] [1:621:7] SCAN FIN [**]
[Classification: Attempted Information Leak]
[Priority: 2] 11/15-14:34:47.694055 10.10.10.20:3777 -> 10.10.10.25:0TCP
TTL:64 TOS:0x0 ID:55275 IpLen:20 DgmLen:40
*******F Seq: 0x26B3BDE5 Ack: 0x7895D1C4 Win: 0x200 TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS27]

| No | Timestamp | SRC_IP | DST_IP | SRC_port | DST_port | Protocol | Size | Flag | Total_Len | Content |
|---|---|---|---|---|---|---|---|---|---|---|
| 535623 | 34:47.5 | 10.10.10.20 | 10.10.10.25 | 4022 | 0 | TCP | 60 | R | 40 | P…P…… |
| 535735 | 34:47.7 | 10.10.10.20 | 10.10.10.25 | 3777 | 0 | TCP | 60 | F | 40 | x…p…G…… |
| 535737 | 34:47.7 | 10.10.10.25 | 10.10.10.20 | 0 | 3777 | TCP | 60 | A.R | 40 | &…P…5…… |

Figure 4: Probe stages

[**] [1:1497:6] WEB-MISC cross site scripting attempt [**]
[Classification: Web Application Attack] [Priority: 1]
08/07-02:32:58.279106 10.10.10.15:4579 -> 10.10.10.25:80
TCP TTL:128 TOS:0x0 ID:56110 IpLen:20 DgmLen:467 DF
***AP*** Seq: 0xDAEC1AA2 Ack: 0x1102B98D Win: 0xFFFF TcpLen: 20

| No. | Timestamp | Src_IP | Dst_IP | Src_Port | Dst_Port | Protocol | Size | Flags | Length | Summary |
|---|---|---|---|---|---|---|---|---|---|---|
| 14723 | 32:58.3 | 10.10.10.15 | 10.10.10.25 | 4579 | 80 | HTTP | 481 | AP | 467 | C: GET /citrix/nfuse/default/login.asp?NFuse_LogoutId= &NFuse_MessageType=Error&NFuse_Message= <SCRIPT>alert('Ritchie') </SCRIPT>&ClientDetection=ON HTTP/1.1 |
| 14724 | 32:58.3 | 10.10.10.15 | 10.10.10.25 | 4577 | 80 | HTTP | 54 | A.R | 40 | Seq=0428859739,Ack=2717741707,F=.A.R..,Len= 0,Win= 0 |
| 14725 | 32:58.3 | 10.10.10.25 | 10.10.10.15 | 80 | 4579 | HTTP | 1,514 | A | 1500 | S: HTTP/1.1 404 Not Found |
| 14726 | 32:58.3 | 10.10.10.25 | 10.10.10.15 | 80 | 4579 | HTTP | 389 | AP | 375 | S: Continuation of existing HTTP stream, 335 bytes text data |
| 14732 | 32:58.3 | 10.10.10.15 | 10.10.10.25 | 4580 | 80 | HTTP | 400 | AP | 386 | C: GET /devdescr.xml HTTP/1.1 |
| 14733 | 32:58.3 | 10.10.10.25 | 10.10.10.15 | 80 | 4580 | HTTP | 1,514 | A | 1500 | S: HTTP/1.1 404 Not Found |
| 14734 | 32:58.3 | 10.10.10.25 | 10.10.10.15 | 80 | 4580 | HTTP | 408 | AP.F | 394 | S: Continuation of existing HTTP stream, 354 bytes text data |
| 14735 | 32:58.3 | 10.10.10.15 | 10.10.10.25 | 4580 | 80 | HTTP | 54 | A | 40 | Seq=3941520320,Ack=0432962896,F=.A....,Len= 0,Win=65535 |
| 14736 | 32:58.3 | 10.10.10.15 | 10.10.10.25 | 4579 | 80 | HTTP | 487 | AP | 473 | C: GET /citrix/MetaframeXP/default/login.asp? NFuse_LogoutId= &NFuse_MessageType=Error&NFuse_Message= <SCRIPT>alert('Ritchie')</SCRIPT>& ClientDetection=ON HTTP/1.1 |
| 14737 | 32:58.3 | 10.10.10.15 | 10.10.10.25 | 4580 | 80 | HTTP | 54 | A.R | 40 | Seq=3941520320,Ack=0432962896,F=.A.R..,Len= 0,Win= 0 |
| 14738 | 32:58.3 | 10.10.10.15 | 10.10.10.25 | 4581 | 80 | HTTP | 62 | S | 48 | Seq=1832059795,Ack=0000000000,F=....S.,Len= 0,Win=65535 |
| 14739 | 32:58.3 | 10.10.10.25 | 10.10.10.15 | 80 | 4579 | HTTP | 1,514 | A | 1500 | S: HTTP/1.1 404 Not Found |

Figure 5: Root to Local (R2L)

Table 1: The Number of Alert from Scanning stages

| No | Detected Alert | Priority | Total |
|---|---|---|---|
| 1 | SCAN FIN | 2 | 4078 |
| 2 | NETBIOS SMB repeated logon failure | 1 | 453 |
| 3 | WEBROOT DIRECTORY TRAVERSAL | 3 | 433 |
| 4 | WEB-MISC http directory traversal | 2 | 142 |
| 5 | NETBIOS SMB repeated logon failure | 1 | 101 |
| 6 | NETBIOS SMB-DS repeated logon failure | 1 | 74 |
| 7 | (portscan) TCP Portscan | 2 | 49 |
| 8 | ICMP Timestamp Reply | 1 | 31 |
| 9 | SQL ping attempt | 3 | 17 |
| 10 | ICMP Information Request | 3 | 15 |
| 11 | SCAN nmap XMAS | 2 | 10 |
| 12 | ICMP webtrends scanner | 2 | 9 |
| 13 | RPC portmap listing TCP 111 | 2 | 6 |
| 14 | SCAN Amanda client version request | 2 | 4 |
| 15 | ICMP superscan echo | 2 | 4 |
| 16 | NETBIOS SMB-DS ADMIN$ unicode share access | 3 | 4 |
| 17 | NETBIOS SMB-DS D$ unicode share access | 3 | 2 |
| 18 | (portscan) TCP Portsweep | 3 | 2 |
| 19 | NETBIOS SMB-DS C$ share access | 3 | 1 |
| 20 | NETBIOS SMB-DS ADMIN$ share access | 3 | 1 |

### 4.3 Identify R2L

Figure 5 shows one of the attacks as described in the 2nd scenario above. This attack focuses on obtaining privileges for the system. The attacker launched several methods to attempt to find the passwords for FTP and Telnet. Moreover, Figure 3(b) demonstrates that traffic of brute force becomes very dominant. Meanwhile, Table 2 shows the number of alerts from this attack. The attackers tried repeatedly to guess the password by using the default user.

### 4.4 Identify U2R

The attackers just focused on how to gain escalating privileges via level "administrator/root". They succeeded in creating some new users with administrator level, implanting the malware and finding the backdoor. Figure 6 shows a sample from this attack and how the attackers got into the system via an "anonymous" user, then attempts privileges infiltration via change working directory (CWD) of FTP. Table 3 shows the number of alerts from this attack.

### 4.5 Identify DoS

Flooding to Denial of Services (DoS) is the final scenario. Within hours the attackers attempted to disrupt the normal functioning to affect the availability of the target and succeeded. The system response delay value rose slightly as compared to before the attack. The result was system failures and crashes shows in Figure 7. Table 4 shows the number of alerts from this attack.

### 4.6 Network Traffic Visualisation

This section presented the overall network traffic from scanning and penetration stages shown in Figure 3 below. Item (a) depicts the overall traffic of HTTP from scanning stages and item (b) shows the dominant traffic from brute force attacks. Pecentage of SSH/Telnet is allocated 84.96% and ICMP allocated 6.41% from total overall traffic.

This attack focused on achieving access and escalating privileges, especially penetration via brute force to FTP and Telnet. Point (c) in Figure 3 shows some scanning tools from attackers to victim and some of the tools with open connections to the internet. We also see here whether there are any updates of existing vulnerabilities in their database. Meanwhile, item (d) is handshaking traffic attackers and victims in penetration stages; the mark indicates that the attacker launched a comprehensive attack. Items (c) and (d) highlight greater traffic flows from 10.10.10.20 and 10.10.10.15 to victim.

## 5 Conclusions and Future Works

We believe that penetration testing is vital in the search for all kinds of vulnerabilities and for evaluating overall systems. However, the small amount of vulnerability information obtained should be of particular concern. This paper presents the vulnerabilities of Windows Server.

Table 2: The Number of Alert from R2L stages

| No | Detected Alert | Priority | Total |
|---|---|---|---|
| 1 | INFO FTP Bad login | 2 | 67625 |
| 2 | WEB-PHP remote include path | 1 | 2709 |
| 3 | WEB-MISC cross site scripting attempt | 1 | 1380 |
| 4 | COMMUNITY WEB-PHP XSS attempt | 1 | 596 |
| 5 | COMMUNITY WEB-PHP XSS attempt | 1 | 510 |
| 6 | NETBIOS SMB repeated logon failure | 1 | 453 |
| 7 | NETBIOS SMB-DS repeated logon failure | 1 | 106 |
| 8 | WEB-MISC Tomcat servlet mapping cross site scripting attempt | 1 | 19 |
| 9 | (ftp_telnet) Invalid FTP Command | 3 | 18 |
| 10 | WEB-CGI perl command attempt | 2 | 13 |
| 11 | FTP CWD ãttempt | 2 | 2 |

Table 3: The Number of Alert from U2R stages

| No | Detected Alert | Priority | Total |
|---|---|---|---|
| 1 | WEB-MISC /etc/passwd 2 | 1876 | |
| 2 | NETBIOS SMB repeated logon failure | 1 | 1161 |
| 3 | ATTACK-RESPONSES Invalid URL | 2 | 150 |
| 4 | BACKDOOR netbus active | 1 | 36 |
| 5 | WEB-IIS CodeRed v2 root.exe access | 1 | 19 |
| 6 | BACKDOOR sensepost.exe command shell attempt | 2 | 16 |
| 7 | DOUBLE DECODING ATTACK | 1 | 14 |
| 8 | WEB-ATTACKS /etc/shadow access | 2 | 12 |
| 9 | BACKDOOR c99shell.php command request | 1 | 4 |
| 10 | WEB-MISC bad HTTP/1.1 request, Potentially worm attack | 2 | 3 |
| 11 | BACKDOOR netbus getinfo | 1 | 1 |
| 12 | FTP CWD ... | 1 | 1 |
| 13 | FTP CWD Root directory transversal attempt | 3 | 1 |

Table 4: The Number of Alert from DoS stages

| No | Detected Alert | Priority | Total |
|---|---|---|---|
| 1 | BAD-TRAFFIC tcp port 0 traffic | 3 | 12548 |
| 2 | ICMP PING Windows | 3 | 8334 |
| 3 | ICMP PING | 3 | 6300 |
| 4 | ICMP Echo Reply | 3 | 2125 |
| 5 | ICMP Destination Unreachable Port Unreachable | 3 | 2082 |
| 6 | (snort decoder) Bad Traffic Loopback IP | 3 | 1332 |
| 7 | (snort decoder) Bad Traffic Same Src/Dst IP | 3 | 678 |
| 8 | ATTACK-RESPONSES Invalid URL | 2 | 150 |
| 9 | SNMP trap udp | 2 | 30 |
| 10 | NETBIOS SMB Trans Max Param/Count DOS attempt | 3 | 12 |
| 11 | DDOS Stacheldraht client check gag | 2 | 7 |
| 12 | COMMUNITY WEB-MISC Hasbani-WindWeb GET DoS attempt | 2 | 4 |
| 13 | DDOS mstream client to handler | 2 | 2 |
| 14 | NETBIOS SMB-DS Trans unicode Max Param DOS attempt | 3 | 1 |

[**] [1:1229:7] FTP CWD ... [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
08/07-02:33:30.183629 10.10.10.15:5241 -> 10.10.10.25:21
TCP TTL:128 TOS:0x0 ID:60987 IpLen:20 DgmLen:94 DF
***AP*** Seq: 0xA0670E4B Ack: 0x38AD9A35 Win: 0xFF4E TcpLen: 20
[Xref => http://www.securityfocus.com/bid/9237]

| No | Timestamp | SRC_IP | DST_IP | SRC_port | DST_port | Protocol | Size | Flag | Total_Len | Content |
|---|---|---|---|---|---|---|---|---|---|---|
| 24186 | 33:30.0 | 10.10.10.25 | 10.10.10.15 | 21 | 5241 | FTP Ctrl | 70 | AP | 56 | 220 FTP SERVER |
| 24187 | 33:30.0 | 10.10.10.15 | 10.10.10.25 | 5241 | 21 | FTP Ctrl | 70 | AP | 56 | USER anonymous |
| 24188 | 33:30.0 | 10.10.10.25 | 10.10.10.15 | 21 | 5241 | FTP Ctrl | 126 | AP | 112 | 331 Anonymous access allowed, send identity (e-mail name) as password. |
| 24189 | 33:30.0 | 10.10.10.15 | 10.10.10.25 | 5241 | 21 | FTP Ctrl | 78 | AP | 64 | PASS nessus@nessus.org |
| 24190 | 33:30.0 | 10.10.10.25 | 10.10.10.15 | 21 | 5241 | FTP Ctrl | 85 | AP | 71 | 230-WELCOM TO FTP SERVER 2003 |
| 24191 | 33:30.2 | 10.10.10.15 | 10.10.10.25 | 5241 | 21 | FTP Ctrl | 54 | A | 40 | |
| 24192 | 33:30.2 | 10.10.10.25 | 10.10.10.15 | 21 | 5241 | FTP Ctrl | 85 | AP | 71 | 230 Anonymous user logged in. |
| 24193 | 33:30.2 | 10.10.10.15 | 10.10.10.25 | 5241 | 21 | FTP Ctrl | 108 | AP | 94 | CWD .../.../.../.../.../.../.../.../.../.../.../.../ |
| 24194 | 33:30.2 | 10.10.10.25 | 10.10.10.15 | 21 | 5241 | FTP Ctrl | 83 | AP | 69 | 250 CWD command successful. |
| 24195 | 33:30.2 | 10.10.10.15 | 10.10.10.25 | 5241 | 21 | FTP Ctrl | 60 | AP | 46 | PASV |
| 24196 | 33:30.2 | 10.10.10.25 | 10.10.10.15 | 21 | 5241 | FTP Ctrl | 101 | AP | 87 | 227 Entering Passive Mode (10,10,10,25,18,4). |
| 24197 | 33:30.2 | 10.10.10.15 | 10.10.10.25 | 5241 | 21 | FTP Ctrl | 62 | S | 48 | |
| 24198 | 33:30.2 | 10.10.10.25 | 10.10.10.15 | 21 | 5241 | FTP Ctrl | 62 | A.S | 48 | |
| 24199 | 33:30.2 | 10.10.10.15 | 10.10.10.25 | 5241 | 21 | FTP Ctrl | 54 | A | 40 | |
| 24200 | 33:30.2 | 10.10.10.25 | 10.10.10.15 | 21 | 5241 | FTP Ctrl | 69 | AP | 55 | RETR boot.ini |
| 24201 | 33:30.2 | 10.10.10.15 | 10.10.10.25 | 5241 | 21 | FTP Ctrl | 113 | AP | 99 | 550 boot.ini: The system cannot find the file specified. |
| 24202 | 33:30.2 | 10.10.10.25 | 10.10.10.15 | 21 | 5241 | FTP Ctrl | 54 | A.R | 40 | |
| 24203 | 33:30.2 | 10.10.10.15 | 10.10.10.25 | 5241 | 21 | FTP Ctrl | 60 | AP | 46 | QUIT |

Figure 6: User to Root (U2R)

[**] [1:402:8] ICMP Destination Unreachable Port Unreachable [**]
[Classification: Misc activity] [Priority: 3]
11/16-12:04:44.947792 10.10.10.15 -> 10.10.10.25
ICMP TTL:128 TOS:0x0 ID:20401 IpLen:20 DgmLen:83
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP: 10.10.10.25:7 -> 10.10.10.15:59130
UDP TTL:128 TOS:0x0 ID:28414 IpLen:20 DgmLen:55 Len: 27 Csum: 17179 (27 more bytes of original packet)
** END OF DUMP
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2005-0068] [=> http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0790]

| No | Timestamp | SRC_IP | DST_IP | SRC_port | DST_port | Protocol | Size | Flag | Total_Len | Summary |
|---|---|---|---|---|---|---|---|---|---|---|
| 33763346 | 12:04:44.944406 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 190 | - | 176 | Destination Port Unreachable |
| 33763355 | 12:04:44.947278 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 97 | - | 83 | Destination Port Unreachable |
| 33763356 | 12:04:44.947282 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 97 | - | 83 | Destination Port Unreachable |
| 33763360 | 12:04:44.947792 | 10.10.10.15 | 10.10.10.25 | - | - | ICMP | 97 | - | 83 | Destination Port Unreachable |
| 33763361 | 12:04:44.947798 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 97 | - | 83 | Destination Port Unreachable |
| 33763362 | 12:04:44.948045 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 97 | - | 83 | Destination Port Unreachable |
| 33763363 | 12:04:44.948050 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 97 | - | 83 | Destination Port Unreachable |
| 33763370 | 12:04:44.955090 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 83 | - | 69 | Destination Port Unreachable |
| 33763371 | 12:04:44.955095 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 83 | - | 69 | Destination Port Unreachable |
| 33763372 | 12:04:44.955099 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 83 | - | 69 | Destination Port Unreachable |
| 33763373 | 12:04:44.955311 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 83 | - | 69 | Destination Port Unreachable |
| 33763374 | 12:04:44.955316 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 83 | - | 69 | Destination Port Unreachable |
| 33763375 | 12:04:44.955319 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 83 | - | 69 | Destination Port Unreachable |
| 33763392 | 12:04:45.053473 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 190 | - | 176 | Destination Port Unreachable |
| 33763414 | 12:04:45.104769 | 10.10.10.25 | 10.10.10.15 | - | - | ICMP | 82 | - | 68 | Destination Port Unreachable |

Figure 7: Denial of services (DoS)

This server presents many open invitations for attackers to exploit as can be gathered from all the experiments conducted: implanting malware, password guessing, rooting, web injection, creating a backdoor and DoS. It can be concluded that the OS is vulnerable and open to exploitation, and thus requires more effort to be secured. Our conclusions are as follows: (i) there are relationships resulting from the scanning and information from the CVE vulnerability database, (ii) update policy and management of authentication for user, (iii) it is important that security operators assume that they will be hacked and should better secure themselves for that reason.

Meanwhile, what this experiment indicates is that there a large number of new attacks that could remain hidden in the data and would not be identified using existing Snort signature. Snort cannot be used as a security platform to protect against threats; it cannot be expected to detect all threats and trigger the necessary response. However, Snort is adept at protocol analysis, content matching, and packet logging. Therefore, some future work must be conducted such as: (i) how to extract the data to analysed, (ii) how to classify the threat and normal access, and (iii) how to visualise alert to show details of taxonomy information from Snort.

## References


[1] N. Athanasiades, R. Abler, J. Levine, H. Owen, and G. Riley, "Intrusion detection testing and benchmarking methodologies," in *First IEEE International Workshop on Information Assurance (IWIA'03)*, pp. 63–72, 2003.

[2] N. Barrett, "Penetration testing and social engineering: Hacking the weakest link," *Information Security Technical Report*, vol. 8, pp. 56–64, 2003.

[3] R. Beghdad, "Critical study of neural networks in detecting intrusions," *Computers & Security*, vol. 27, pp. 168–175, 2008.

[4] R. Beghdad, "Efficient deterministic method for detecting new U2R attacks," *Computer Communications*, vol. 32, pp. 1104–1110, 2009.

[5] D. Bradbury, "Hands-on with metasploit express," *Network Security*, vol. 2010, pp. 7–11, 2010.

[6] V. Broucek and P. Turner, "Technical, legal and ethical dilemmas: Distinguishing risks arising from malware and cyber-attack tools in the 'cloud'-a forensic computing perspective," *Journal of Computer Virology and Hacking Techniques*, vol. 9, pp. 27–33, 2013.

[7] R. Bruen, "Intrusion detection systems: Problems and opportunities," *Software Focus*, vol. 2, pp. 151–156, 2001.

[8] S. Chebrolu, A. Abraham, and J. P. Thomas, "Feature deduction and ensemble design of intrusion detection systems," *Computers & Security*, vol. 24, pp. 295–307, 2005.

[9] B. Clive, "Hacking: An abuse of privilege," *Computer Audit Update*, vol. 1990, no. 1, pp. 21–24, 1989.

[10] E. Conrad, S. Misenar, and J. Feldman, *Domain 2: Access Control (Chap. 3)*, CISSP Study Guide, pp. 37–89, 2010.

[11] J. Conrad, "Seeking help: The important role of ethical hackers," *Network Security*, vol. 2012, pp. 5–8, 2012.

[12] S. David, "The state of network security," *Network Security*, vol. 2012, pp. 14–20, 2012.

[13] H. Gascon, A. Orfila, and J. Blasco, "Analysis of update delays in signature-based network intrusion detection systems," *Computers & Security*, vol. 30, no. 8, pp. 613-624, 2011.

[14] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers & Security*, vol. 24, pp. 31–43, 2005.

[15] H. Holm, "Performance of automated network vulnerability scanning at remediating security issues," *Computers & Security*, vol. 31, no. 2, pp. 164–175, 2012.

[16] J. Hua and S. Bapna, "The economic impact of cyber terrorism," *The Journal of Strategic Information Systems*, vol. 22, no. 3, pp. 175–186, 2013.

[17] G. Kenneth, "Cyber Weapons Convention," *Computer Law & Security Review*, vol. 26, pp. 547–551, 2010.

[18] S. Mansfield-Devine, "DDoS: Threats and mitigation," *Network Security*, vol. 2011, pp. 5–12, 2011.

[19] N. Martin and J. Rice, "Cybercrime: Understanding and addressing the concerns of stakeholders," *Computers & Security*, vol. 30, pp. 803–814, 2011.

[20] R. A. Martin, "Managing vulnerabilities in networked systems," *IEEE Computer*, vol. 34, no. 11, pp. 32–38, 2001.

[21] K. K. M. D. Maynor, *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research*, Elsevier Inc, pp. 1-64, 2007.

[22] P. Mell, V. Hu, R. Lippmann, J. Haines, and M. Zissman, *An Overview of Issues in Testing Intrusion Detection Systems*, Technical Report NISTIR 7007, July 11, 2003.

[23] D. E. Neghina and E. Scarlat, "Managing information technology security in the context of cyber crime trends," *International Journal of Computers Communications & Control*, vol. 8, pp. 97–104, 2013.

[24] C. P. Pfleeger, S. L. Pfleeger, and M. F. Theofanos, "A methodology for penetration testing," *Computers & Security*, vol. 8, pp. 613–620, 1989.

[25] R. J. Potts, "Hacking: The threats," *Computer Audit Update*, vol. 1990, no. 1, pp. 14–15, 1989.

[26] E. Schultz, "RPC in Windows systems: What you don't know could hurt you," *Network Security*, vol. 2004, pp. 5–8, 2004.

[27] E. Schultz, "Windows 2000 security A postmortem analysis," *Network Security*, vol. 2004, pp. 6–9, 2004.

[28] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Computers & Security*, vol. 31, pp. 357–374, 2012.

[29] M. D. Steve, "Hacktivism: Assessing the damage," *Network Security*, vol. 2011, pp. 5–13, 2011.
[30] D. Stiawan, M. Y. Idris, and A. H. Abdullah, "Penetration testing and network auditing: Linux " *Journal of Information Processing Systems*, vol. 11, pp. 104–115, 2015.
[31] G. C. Tjhai, M. Papadaki, S. M. Furnell, and N. L. Clarke, "The problem of false alarms: Evaluation with snort and DARPA 1999 dataset," in *Trust, Privacy and Security in Digital Business*, LNCS 5185, pp. 139-150, Springer, 2008.
[32] S. W. Woo, H. Joh, O. H. Alhazmi, and Y. K. Malaiya, "Modeling vulnerability discovery process in Apache and IIS HTTP servers," *Computers & Security*, vol. 30, pp. 50–62, 2011.

**Deris Stiawan** (SCOPUS ID: 36449642900), received his Ph.D degree in Computer Science from Universiti Teknologi Malaysia in 2013. Currently he is an senior lecturer in Faculty of Computer Science, University of Sriwijaya, Indonesia. In 2011, He holds Certified Ethical Hacker (C—EH) & Certified Hacker Forensic Investigator (C—HFI) licensed from EC-Council. His research interests concern network & information security fields, focused on network attack and intrusion prevention/detection system.

**Mohd Yazid Idris** (SCOPUS ID: 36448800600), is a senior lecturer at of Computing, Universiti Teknologi Malaysia. He obtained his M.Sc and Ph.D in the area of Software Engineering, and Information Technology (IT) Security in 1998 and 2008 respectively. In software engineering, he focuses on the research of designing and development of mobile and telecommunication software. His main research activity in IT security is in the area of Intrusion Prevention and Detection (ITD). He is currently active in various academic activities and involves in university-industry link initiative in both areas.

**Abdul Hanan Abdullah** (SCOPUS ID: 11338934800), received his B.Sc. and M.Sc from University of San Francisco, California, and Ph.D from Aston University, Birmingham, United Kingdom. He is a Senior Professor at Faculty of Computing, Universiti Teknologi Malaysia (UTM). Currently, he is the Head of Pervasive Computing Research Group. His research areas of interest include Pervasive Computing, Network Security, Cloud and Grid Computing.

**Mohammed AlQurashi** received B.Sc. in Computer from King Abdul Aziz University, Saudi Arabia in 2009, and M.Sc. in Computer Science from University of Texas at San Antonio, USA, in 2013. Currently, he is a lecturer and researcher at Smart Network Research Group, at College of Computer Science and IT, Albaha University, Saudi Arabia. His research interests include, Information Security, Cloud computing, and Network Security.

**Rahmat Budiarto** (SCOPUS ID: 6603477220) received B.Sc. degree from Bandung Institute of Technology in 1986, M.Eng, and Dr.Eng in Computer Science from Nagoya Institute of Technology in 1995 and 1998, respectively. He is currently a professor and the head of Smart Networked Research Group at College of Computer Science and IT, Albaha University, Saudi Arabia. His research interests include IPv6, network security, Wireless sensor networks and MANETs.