Project – Blue / Red
Team Game Report 1

CSCI 6706 Network Design

Christian Liu – B00415613
Computer Science Department
Dalhousie University
Halifax, NS
Chris.liu@dal.ca

Table of Contents

ABSTRACT

The first term project report will cover following materials [2]:

- Introduce the work environment of both Red and Blue team.
- Indicate what service will be used for term project.
- How will I establish the service with GNS3 topology?
- What penetration testing will I conduct.
- How will I generate normal traffic / data on my Blue team?

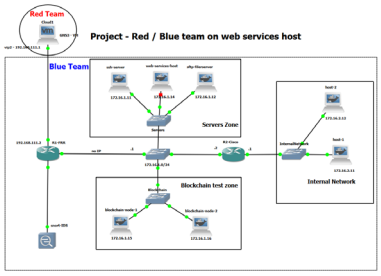
1 Introduction

The first report is within term project planning stage during the whole term project life cycle. Let us recall project life cycle will normally includes 5 stages: planning, design, implement, test, and maintenance. Therefore, I will also follow this general process to complete my term project.

2 Environment Configuration

The environment setup is one of the most time-consuming process during project life cycle, and it has to be constantly adjusted based on dynamic needs during implementation. Here, I am answering the initial plan at this moment.

2.1 Environment persistence



This section is related to many new additional software and tools installations, especially in case I planned to add Blockchain support to our Blue team strategy. To make Docker container consistence on GNS3, we need to do the additional configuration on GNS3:

2.2 Installed Software on both Blue and Red Team

I planned to install following software tools, and the details will be illustrated in the second report [13]:

Blue Team	Red Team
WireShark (Traffic Monitoring, Sniffing, and recording)	Hpring3 (DoS /DDoS)
Argue (Data Capturing, Converting and Analyzing)	Nmap (Port Scan)
TCPDump (Data Sniffing)	Medusa (Brute-Force)
TCPReplay / TCPRewrite (Traffic replay / rewriting)	Hydra (Brute-Force)
ACL (access-control)	Patator (Brute-Force)
UFW (firewall)	ZAP (Web Vulnerability)
Whitelist / Blocklist (Filter)	
Snort (Traffic Monitoring and Alerting)	
Blockchain (tentative – Personal recommendation)	

2.3 Accounts setup on Blue team

I would like to choose 4 accounts for blue team to provide a basic authorization and authentication protection during our stage 1 of project. We are trying to avoid 'root' account for basic principal of protection. They are:

Username	Password	Role
Bob	Dragon	Admin
Alice	696969	Super User
Cat	Shadow	User
Scptest	Abc123	guest

I will add those account to our victim web application by following the instruction of [14].

2.4 Project quality assurance and control

To ensure the project quality, I am planning to utilize the GIT and JIRA to provide basic project management functionalities.

3 Services chosen and Services establishment

I will choose the web services on host "Metasploitable" . And I noticed "Metasploitable" Docker image already includes "tikiviki" / "twiki" / "dvwa" / "multillidae" web applications. I will choose **DVWA** web application as target.

4 Penetration Testing

I will conduct following 4 different attacks against victim host machine. Tentatively I might want to bring Blockchain defend mechanism in.

ICMP / SYN Flood	Hping3
Nmap	Port scan
Brute-Force	Medusa, Hydra and Patator
Web Vulnerability	ZAP or SQL injection or manually

5 Data /Traffic generation

I will conduct two different methods to generate actual data /traffic [11][12]:

- Crontab: we can conduct scheduled tasks by configured via crontab, such as [9]:

- Shell Script: we can utilize the for loop to simulate services consumption with a certain interval. Such as:

```
#!/bin/sh
while true
do
  curl
     172.16.1.14/dvwa/vulnerabilities/csrf/?password_current=password&pas
     sword_new=1234&password_conf=1234&change=change
  sleep 5
done
```

The tools for sniffing / capturing data / traffic were practised a lot in previous assignment 2 and 3. I will reuse those tools to capture and store the traffic data during the traffic simulation. They are Tcpdump, WireShark, Argus, TCPReplay and TCPRewrite etc.

I list my Data / Traffic generation plan in the table:

Before Security (July 20th – 24th)	**After Security (July 27th – 31st)**
On the consecutive 5 days starting on July 20th , I will monitor the network for one hour with crontab simulation services consumption. During the monitoring, I mainly play red team to attack blue team (web services). After one-hour monitoring is done, I collect data through wireshark or tcpdump, convert data to the most suitable PCAP Datasets via Argus. Eventually, this dataset will be used to compared with the dataset after blue team security enabled.	On the consecutive 5 days starting on July 27th , I will monitor the network with Blue team security guards. After one-hour monitoring is done, I collect data through wireshark or tcpdump, convert data to the most suitable PCAP Datasets via Argus. Eventually, this dataset will be used to compared with the dataset before blue team security enabled.

REFERENCES

[1] DR. NUR ZINCIR-HEYWOOD, https://web.cs.dal.ca/~zincir/cs6706.html
[2] Brightspace: https://dal.brightspace.com/d2l/home/124069
[3] Truffle Suite: https://www.trufflesuite.com/docs/truffle/quickstart
[4] https://linuxize.com/post/how-to-install-node-js-on-ubuntu-18.04/
[5] Install truffle suite: https://medium.com/@techgeek628/how-to-install-and-execute-truffle-on-an-ubuntu-16-04-7ebb3444707e
[6] https://www.vultr.com/docs/how-to-configure-ufw-firewall-on-ubuntu-14-04
[7] TrendMicro white paper: https://documents.trendmicro.com/assets/white_papers/wp-shifts-in-the-underground.pdf
[8] Brute force attack: https://hackertarget.com/brute-forcing-passwords-with-ncrack-hydra-and-medusa/
[9] Curl command line sending HTTP Request: https://hackernoon.com/how-to-easily-use-curl-for-http-requests-db3249c5d4e6
[10] Red team tools: https://sectools.org/tool/medusa/
[11] 500 worst passwords: https://blog.skullsecurity.org/
[12] 1000 username list: https://github.com/danielmiessler/SecLists/blob/master/Usernames/Names/names.txt
[13] Network Security Tools Categories: https://sectools.org/
[14] DVWA installation and configuration: https://www.thomaslaurenson.com/blog/2018/07/12/installing-and-configuring-damn-vulnerable-web-application/