Term Project – Report 2

Yansong Li
B00755354

1. Implementation and installation of the software for **red team**.

For **web service**:

Client-side appliance:

(1) Webterm was firstly deployed as the client-side appliance. The pulling of image was successful, but it gives an error while creating a node from template as Figure 1.1 Showed.

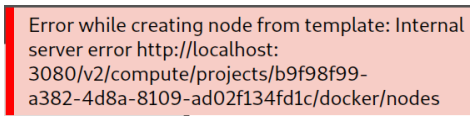

Figure 1.1 Webterm error.

(2) The Firefox appliance was used as an alternative for client-side. It also has the web browser and ipv4 address features. This appliance also gave an error when I try to open it as shown in Figure 1.2, but the error was solved with a manipulation of *gns3_server.conf* file.

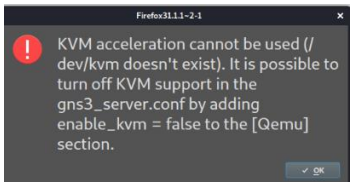

Figure 1.2 Firefox error.

Server-side appliance:

The Nginx appliance was deployed as the server-side appliance. The client-side desktops can assess the website of it using its ipv4 address.

Topology configuration: The topology is configured as shown in Figure 1.3.

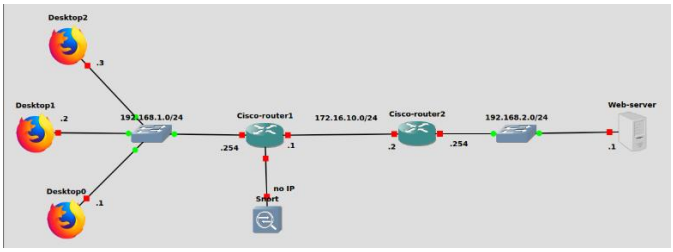

Figure 1.3 Web service topology

Account set-up:

The blue team is considered as a small enterprise with a web server and three desktops. Each desktop can access their own web page with username and password authentication as Shown in Figure 1.4 and 1.5.

Desktop 0: username: *desktop0*; password: *000000*; link: *192.168.2.1/desktop0/*

Desktop 1: username: *desktop1*; password: *111111*; link: *192.168.2.1/desktop1/*
Desktop 2: username: *desktop2*; password: *222222*; link: *192.168.2.1/desktop2/*

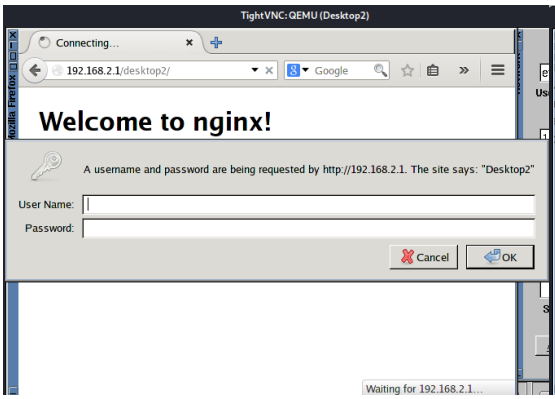

Figure 1.4 log-in page

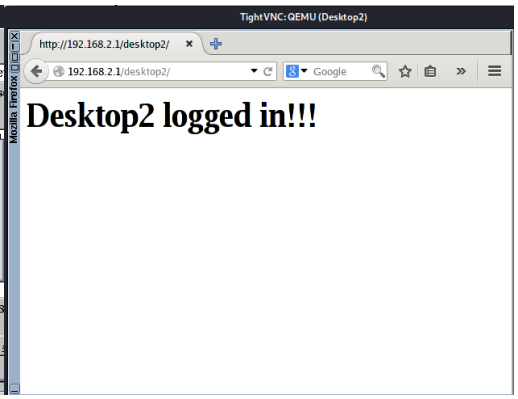

Figure 1.5 main page

Stratgy of genreating normal traffic:

(1) Manually: accessing desktops' webpage time to time using their usernames and passwords.
(2) Automatically: generating a certain amount of traffic using *iperf* command.

For **defense**:

(1) Snort-IDS is connected to Cisco router 1 for detecting probes and attacks.
(2) Access Control List will be applied on Cisco router 2 for filtering network traffic.
(3) PFSense/OPNSense Firewall is waived due to the complexity of configuration. (The change from previous plan).

2. Implementation and installation of the software for **blue team**.

For **penetration testing**:

(1) *nmap* command will be applied from the Kali VM for scanning blue team.
(2) Nessus is installed and will be used from its webpage for vulnerability assessment of the blue team.
(3) Metasploit is installed and will be applied from the Kali VM for exploiting the vulnerabilities of the blue team found in scanning.
(4) Deny-of-Service attack will be applied using *hping3* command from the Kali VM for flooding the blue team with traffic.

References:

1. https://gns3.com/managing-devices-with-ansibler-c
2. https://www.youtube.com/watch?v=cXrhG81C4mg&t=65s