A Development of Hands-on Training Materials to learn Network Technology in a Police Academy

Hiroaki Hata[*, a]

[a] National Institute of Technology, Fukui College

*E-Mail hata@fukui-nct.ac.jp

Abstract

We present hands-on training materials to learn network technology in a police academy for officers who are not specialized cybercriminal. This material environment contains three virtual machines running Linux in a PC, but it requires the PC to come with 8GB memory and 50 GB space in storage. This is not severe conditions, and they can do this practice with ordinary home PCs. In this material, students could learn data link layer connection between machines, IP address assignment, difference between IP routing, NAT and proxy, and cache and load balancer functionality in reverse proxies in half day class.

Keywords: *non-engineer, network, practice, Linux, Virtual Machines*

1.Introduction

Traditionally, the purpose to learn network technology has been training engineers who can build and operate networks. In recent years, however, students who learn network technology do not always hope to be engineers, because their study purpose is investigating cybercrime or promoting security skill. We categorized them into two groups. The former are the engineer-oriented students, and the latter are the non-oriented group.

Network technology training often comes in classroom lecture and practical training; hands-on. The lectures are for learning the concepts necessary for network technology, and do not differ between engineer-oriented learners and non-engineer-oriented learners. The hands-on are to aim to learn the configuration skills of specific network vendor's equipment. However, device configuration is not a necessary skill for the non-oriented learners. Therefore, this tends to result in classroom-only training that omits hands-on for the for the non-oriented learners. However, since the daily work of non-engineers is not engineering, the lectured knowledge is quickly forgotten. So, hands-on is necessary for them. What kind of environment and content should be used for the hands-on of the non-engineer-oriented learner? This is the subject of this paper.

An example of such a non-oriented learner would be a police officer who does not specialize in cybercrime, but works in the criminal division, non-cyber security or a police department.

As a prerequisite for the development of hands-on materials, organizations of non-engineers do not have a test bed, space or budget to install network equipment, etc. So, we would like to do the hands-on using only PCs. The PCs should not have free access to the Internet for security reasons. The participants are not familiar with advanced command operations, but they hope to be able to use a minimum of commands through the practical training.

We present virtual machine environment working standalone PCs to learn network technologies. This environment contains three virtual machines running Linux, but it requires PC to come with 8GB memory and 50GB space in storage. This is not severe conditions, and they can do this practice with ordinary home PCs. In this material, participants could learn data link layer connection between machines, IP address assignment, difference between IP routing, NAT and proxy, and cache and load balancer functionality in reverse proxies in half day class of a police academy.

In the following, we present some related works in chapter2, and discuss environment of practice. Chapter 3 presents specific practical nine issues. The items are designed to assume the techniques and skills that police officers will need in their operations.

2.Related Works

There have been several studies [1][2] on teaching engineers in special environments [3] and on teaching non-engineering disciplines to engineers. There is also an initiative called Challenge-Base Learning, which provides hands-on training and deepens knowledge [4]. In this study, we are conducting an educational initiative that includes hands-on training for participants in non-engineering positions. However, we could not find any papers dealing with the education of non-engineering students in engineering. Although this project is unique, it is not a rare case, and it is expected that the need for education like this project will be recognized in the future as network technology becomes more widespread.

3.Environment and Objectives

In police academies, there are almost no restrictions on computer specifications, and we assume a laptop computer of a class that is generally available on the market.

- ✓ CPU of about IntelCore5i
- ✓ Memory: 8G

- ✓ About 50 GB of free storage space
- ✓ No network equipment other than PCs may be used for training.

Network use is restricted, and it is forbidden to connect from outside to inside, to download files from external servers, or to log in to external servers via ssh or other means.

The goal to be achieved in this environment is to deepen the knowledge of participants who have completed a classroom course on IP networking through hands-on training.

The limitation of using only PCs networking equipment, prohibited connecting routers and other network devices, is due in part to a small budget and inability to purchase networking equipment that is more expensive than PCs, but the goal of the training is not to familiarize the trainees with the use of a particular manufacturer's networking equipment. What is the technology being learned used for? The goal is to understand how these technologies affect police investigations. The trainees are not technicians, and the purpose of the course is not to become network technicians. The course material needs to be designed with this difference in mind.

(Assumed skills of the student)

- ✓ Students do not have the skills to create and modify configuration files using an editor or other tools.
- ✓ They can use basic Linux commands such as file copy command (**cp**) and server start command (**systemctl**).

For these prerequisites, the following materials should be prepared in advance.

- ✓ Linux will be used as the network node.
- ✓ Students will not perform any Linux installation work.
- ✓ Linux distribution will be Linux Mint with low memory usage.
- ✓ Linux will be run on a PC as a Virtual Machine.
- ✓ Application software required for the training should be installed in advance.
- ✓ Application configuration files required for the training will be installed in advance, and students will replace them with cp commands as needed.

Based on these assumptions, instead of using network equipment from a specific network vendor, a hypervisor that can virtually generate multiple network nodes within a single PC was used. In particular, we chose VirtualBox [6], which runs on both Windows PCs and MacBooks. In addition, open source Linux is used as the operating system that runs in the virtual machine generated by the hypervisor. In particular, we will use Mint Linux [5], which is lightweight and easy to operate and can run multiple virtual machines on a PC.

4.Practice Exercises

To create educational materials for the investigation of server logs, which will enable students to understand basic network technology and its meaning. To this end, the following nine exercises were made to the students.

Ex1) Start and Three Virtual Machines in your PC and Login them.

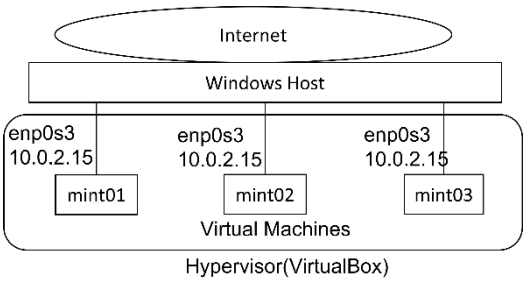

Fig.1 Virtual Machines and Hypervisor used in this hands-on course. Each Machine is installed Linux Mint

The virtual machines required for the training are copied to the trainees' PCs in image files and imported into VirtualBox, hypervisor software. It is assumed that the initial network configuration has three separate VMs as shown in Figure 1. Each VM has its own link for Internet access, but there is no inter-VM connection. The trainee powers up the three VMs and logs in. logs in to the VMs.

After logging in, the desktop of each VM appears. The three VMs, each with the hostname mint01/02/03, have different desktop wallpapers pre-set for easy identification shown in Figure2.

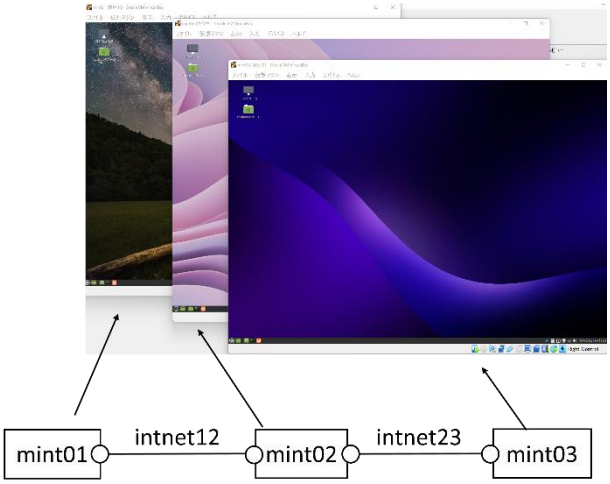

Fig.2 Desktops of Virtual Machines

Ex2) Install Network Adaptors and Connect them to build a Network of Star Topology.

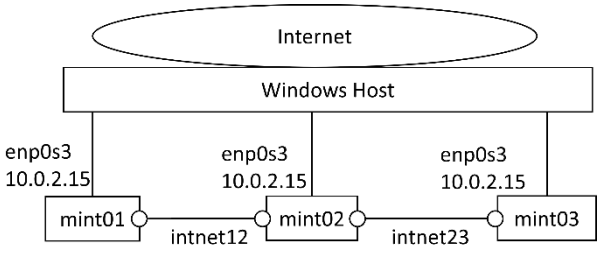

Fig.3 Data Link Interconnections between VMs

As shown in Figure3, add the necessary network adapters to the VMs and connect them to the internal network. Internal network, although it is a connection between VMs, corresponds to the process of attaching network adapters and connecting them to each other via Ethernet in actual network equipment. Make them aware that they can work on the physical layer and the data link layer.

The internal network connecting mint01 and 02 is intnet12, and the internal network connecting mint02 and 03 is intnet23.

Ex3) Assign IP address on each interface and Confirm Link connection with the ping command.

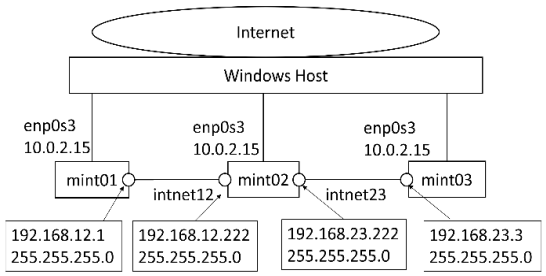

Fig.4 IP Address Assignment on each Interface

Assign IP addresses to the network interfaces added in Ex2: the network address of intnet12 is 192.168.12.0 and the network address of intnet23 is 192.168.23.0 in Figure4. To avoid simply digesting the assignment, as an optional assignment, mint02 is asked to experience that when the network mask is varied, it was possible to connect on 192.168.12.0/24 but not on 192.168.12.0/25, and to consider why this is the case. The host number is assigned a larger value than 128.

Ex4) Set IP forwarding on mint02 and Conform Network Connection between mint01 and mint03.

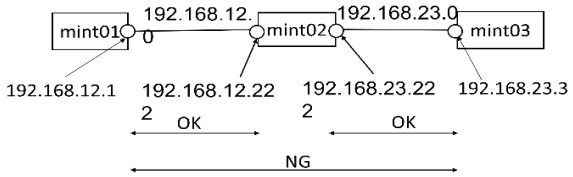

Fig.5 mint02 would not replay any packets before IP forwarding setting.

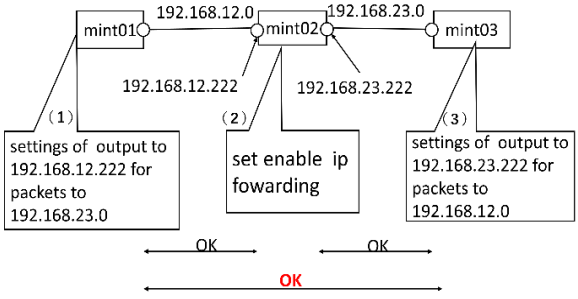

Fig.6 mint01 can reach mint03 after IP forwarding setting on mint02.

The ping command confirms that IP reachability between adjacent VMs has been achieved by assigning IP addresses. However, reachability between mint01 and mint03 can not reach each other (Figure 5). This is where the concept of a router must be understood: mint02 must be configured to relay packets not addressed to itself.

This is accomplished with a kernel configuration command called ***sysctl***.

```
# sysctl -w net.ipv4.ip_forward=1
```

However, there is another important setting: mint01 must be made to send packets destined for mint03 in the direction of mint02, not in the direction of the Internet (up direction in Figure 4). This is a work instruction to make mint01 realize that intnet23 will be on the other side of mint02. In other words, there are routers on the Internet, which are network devices that forward packets destined to destinations other than themselves, and both hosts and routers have knowledge of which direction packets should be sent in depending on the destination, which is set in each network device. The mint01and mint03 become to enable to communicate each other after these operations in Figure 6.

Ex5) Start nginx on mint03 and Access from mint01. Watch access log on the server and confirm IP address of the client.

Start nginx, the http server, on mint03(Figure 7). Then, confirm that it can be accessed from the browser of mint01. If the training is for engineers, it is important for them to understand how to start applications and the meaning of configuration files. However, in training for non-engineers, the objective of the course is not equipment operation. For exercises at the police academy, it is important to be able to read log files. In the exercise, the location of the nginx log file for mint03 and the IP address of the access source are confirmed. The access source IP address is mint01, where the browser is running, and it is understood that it is possible to determine who writes to S N S and so on from that IP address.

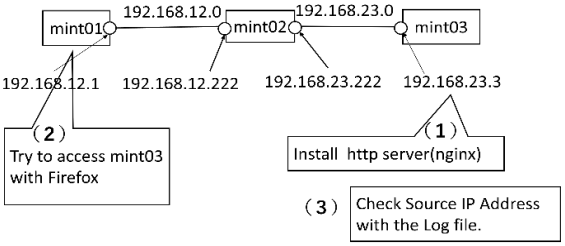

Fig.7 start nginx on mint03

Ex6) Start NAT (ufw) on mint02. How does the Client IP address change?

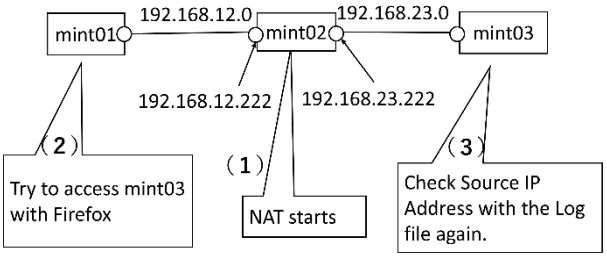

Fig.8 NAT on mint02

Activate NAT on mint02 (Figure 8). NAT is used for security and to prevent IP address exhaustion in homes and by some cell phone companies. The following snippet has to be added in /etc/ufw/before.rules

```
*nat
-F
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 192.168.12.0/24 -o enp0s9
-j MASQUERADE
COMMIT
```

This rule is placed in mint02 from the beginning, and students can start NAT by simply submitting the following command.

```
root@mint02:~# ufw enable
```

After NAT is started, it is important to check that the access log in mint03 has changed to mint02. The IP address in the log is not necessarily the address of the writer's computer. Learn that a steady investigation to find the true source of the message is necessary, using the IP address in the log as a clue.

Ex7) Start Squid (HTTP Proxy) on mint02 and Change proxy settings of the client browser. What difference logs between NAT and Proxy in access log on mint02?

Activate HTTP Proxy instead of NAT on mint02 (Figure 10). A firewall similar to NAT is the HTTP proxy, which is used by public facilities and stores that provide Internet access services. The Squid server used in this

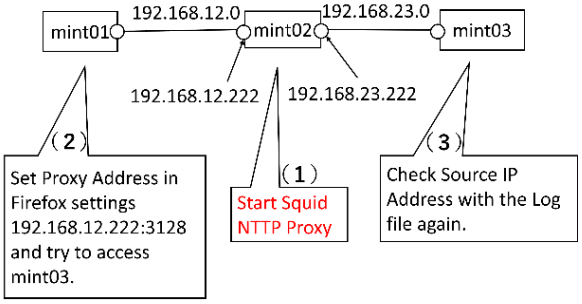

Fig.9 Start HTTP Proxy (squid) instead NAT on mint02

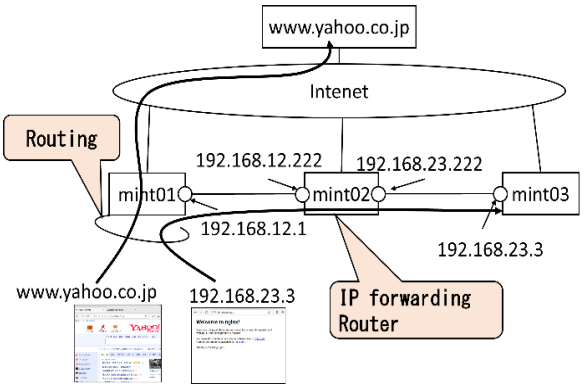

Fig.10 Separated Routes of packets before install HTTP Proxy

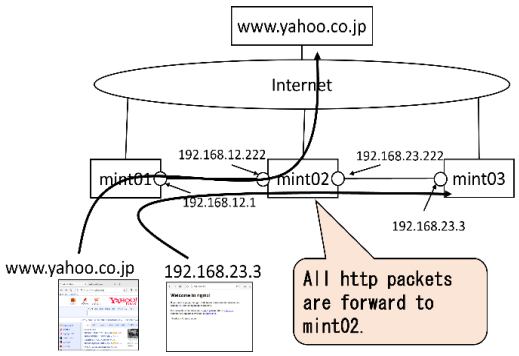

Fig.11 All HTTP Request packets are transmitted to mint02 after install HTTP Proxy

course is an HTTP proxy server application with a long history; it differs from NAT in that all HTTP requests pass through an HTTP proxy. For this reason, the IP address of the HTTP proxy server must be set in the mint01 browser.

Unlike when mint02 is under NAT (Figure 10), when the HTTP proxy is activated, a record of what URLs mint01 has accessed is kept (Figure 11). It is necessary to understand where and what kind of content may be left in the access history, depending on whether it is NAT or HTTP proxy.

Ex8) Start nginx as Reverse Proxy on mint02 and eliminate proxy settings of the client browser. What difference of logs between Proxy and Reverse Proxy.

HTTP proxy are placed near access terminals such as public facilities and stores. On the other hand, HTTP reverse proxies are placed near servers such as data centers and cloud services. Activate HTTP Proxy instead

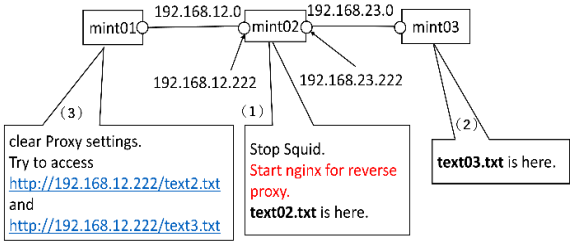

Fig.12 Start HTTP Reverse Proxy (nginx) instead squid on mint02

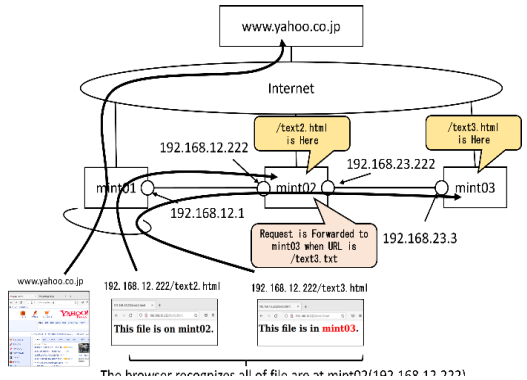

Fig.13 mint02 relays HTTP request to mint03 depending on URLs

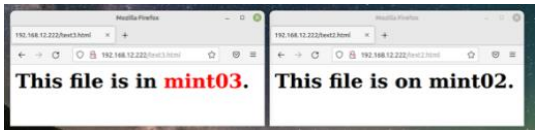

Fig.14 http://mint02/text03.txt is on mint03

of HTTP proxy on mint02 (Figure 12). A reverse proxy acts as a load balancer or an accelerator. mint02 reverse proxy will act as proxy of mint03. The domain name (or IP address) of mint02 to be entered in the U R L window of mint01's browser. All HTTP request packets are received on mint02 and some packets are relayed to mint03. Figure.14 shows a couple of access requests of text content with different URLs.
http://mint02/text03.txt
http://mint02/text02.txt
One shows a text file in mint02 and the other in mint03.

Ex9) Activate cache features of the reverse proxy. What difference of logs on mint03 after that?

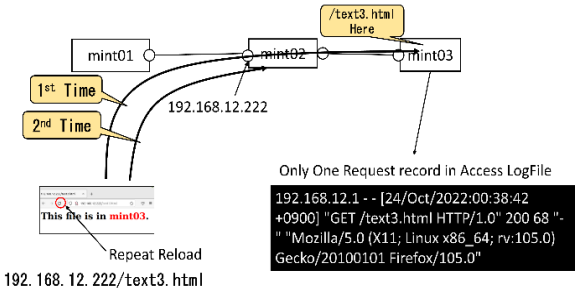

Fig.15 Activate Cache function. The Second request would not be replied to mint03.

Enable the cache function of the HTTP reverse proxy (Figure 15). text03.txt is located only in mint03, so the first access will forward the request to mint03g. However, on the second access, the cache generated in mint02 will respond. Therefore, only the first access record remains in mint03.

Practice

These materials were really used in a class for acquiring networking skills for police officers at a police academy where the author serves as an instructor, using a pair programming method in which pairs are formed and hands-on practice is conducted. One person performs a task while the partner watches and provides advice. When one task was completed, the operator was switched. This allowed the participants to average out the differences in level to some extent and complete the nine exercises within the time allotted.

Conclusions

The following were the findings of the actual course, which was an exercise originally designed to train engineers, but adapted for police academies.

- ✓ Exercises using VM do not require actual routers or servers to confirm functionality.
- ✓ Even a commercial-class PC can run three Linux machines simultaneously.
- ✓ All Linux machines can be operated from a single screen on a single PC rather than using actual machines. This simplicity of operation is beneficial for non-engineers who do not need to handle actual equipment.
- ✓ By installing the applications and configuration files necessary for the exercises on Linux in advance, the exercises were not delayed by misconfigurations. Non-engineers do not need troubleshooting skills.

Non-engineers have different reasons for having to learn technology than do engineers. The conclusion is that the materials created for training engineers are not necessarily suited to the needs of non-engineers, even if they are used as they are in a course designed for non-engineers. They need to be reworked to meet the needs of the students. In the future, there will be an increasing number of situations in which non-engineers will need to learn network technology. It will be necessary to adapt the course materials accordingly.

References

[1] G. Morris, et al. "*Prepare for Career as a Network Engineer*", Information Systems Education Journal (ISEDJ) Feb.2012, pp.13-20
[2] Julie . Goldberg, "*Graduate Women In Engineerng*", Research Report #18-95, Counselling centre University of Maryland at College Park,1995
[3] A. W. Khan," *Engineer's Guide to Technical Writing: Insights for Budding Engineers*", Advances in Language Literary Student",
DIO:10.7575/aiac.alls.v.10n.4p.80
[4] Torres-Barreto et al, *"A Learning Model Proposal Focused on Challenge-Based Learning*" Advances in Engineering Education vol.8,issue 2,2020
[5] Fredricka Thomas," *Install Linux Mint: The Ultimate Beginner's Guide To Installing Linux Mint",* Independently published ISBN:979-8393513665 (2023)
[6] Noe Gruesbeck, *"Virtualbox: Discover How To Virtualize Computers"* Independently published ISBN:979-8840001820 (2022)