Episode 22 (Security I)

Tanuki, let's talk about security for a while.
For individual users, security means that they want to protect their PCs from fake sites (phishing sites), fake emails (phishing emails), and spy cookies, and they want to protect their information.
These can be prevented by not opening email attachments easily, checking the CA (Certificate Authority of Digital Signature) by clicking the key icon to the left of the URL when entering personal information, installing anti-virus software, and always updating vaccine software.
The issue we will discuss in Episode 22 is how to protect the servers of the service providers. Servers store a large amount of confidential information, including customers' personal information, as well as scientific, technical, political, economic, and military information. They are interconnected in a web of interconnectedness and are used on a daily basis, so it is impossible to block some of them. The question is how to protect what cannot be blocked.

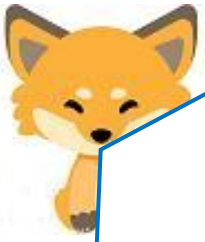
I see, I can protect the user's terminal level if I am careful, but not at the server level.

The raccoon dog, in order to hone the art of defending a server, you need a server to attack. For example, a thief cannot hone his skills in unlocking and breaking into an empty field. The same is true for security. It is only when there is a server to hack that hackers can test the effectiveness of their break-in and information-stealing software. On the other hand, the server administrator can strengthen security to prevent hacking. It's a paradox. But you can't use other companies' servers on the Internet for testing. So they have to build their own servers for testing.

I see...so, telling me to learn practical hacking and security skills where there are no servers is like telling me to practice being a thief in a field. That's not good enough!
But, Kitsune, I've never had that kind of practice in my school's information education.

In order to do hands-on security training, the teacher must prepare the PCs that correspond to the contradiction and the shield, and the students must have learned at least the basics of networking. This is a fairly advanced level of information science. The training of such human resources must be done step by step based on a solid plan. It is not a level where you can just say, "We need a million information workers, so we will start information education next year. I would like to say, "Don't be a fool".

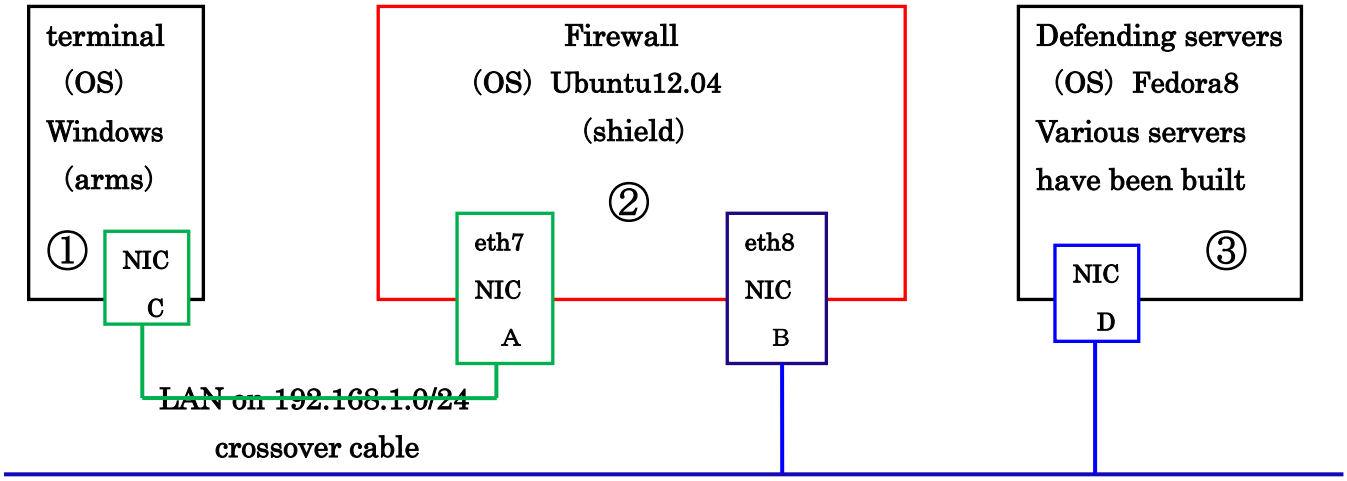
You can be angry all you want, but will that teach me anything?



Tanuki, simply put, it's a lot of work, and you'll have to learn how to do it yourself.
The first thing is how to protect the shields (servers). In other words, build a firewall. In Japanese, a firewall is a firewall. It means to build a wall to protect the inside from outside enemies. Specifically, a firewall consists of a routing function and a filtering function. Both the hardware (equipment) called a router and the Linux operating system have both of these functions. The learning goal is to learn these functions and configure them correctly.
As a way to think about it, you can put servers that are open to the public in the DMZ (demilitarized zone) and do not store important data so that they can only be hacked, or you can put internal servers locally and not make them available to the public.

In order to proceed with the practical training, the following system must be created. If you don't understand the meaning of this, you should stop studying security.
You should re-study from the basics of networking.

[Test environment for security practice]



LAN on 172.17.0.0/16
local network

What does eth7 or eth8 in ② NIC mean?

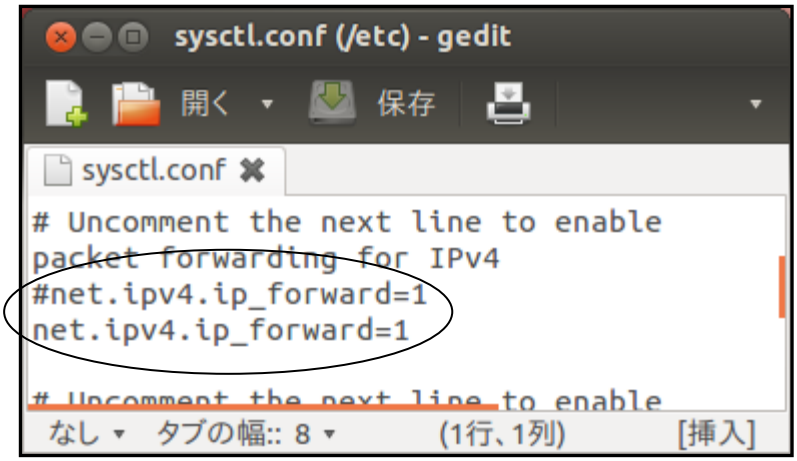
A temporary name given to a NIC (Network Interface Card). It is also called a device name. For raccoon dogs to understand, I named them "NIC A" and "NIC B," but Linux OS (Ubuntu) gives them "eth7" and "eth8" for convenience. However, this device name may change when you log in, so you should be careful.
Well, it's impossible to understand from the above diagram. So, I will briefly explain the diagram in the next section.

The PCs in ③ contain servers and important information (data) that should be protected.
The terminal PC in ① is targeting the server, and its OS is the commonly-used Windows OS.
The PC (firewall) in ② stands in the way of protecting the PC in ③.
The OS is Ubuntu with standard routing and filtering capabilities.
Now, in order to protect the PCs in ③, we will learn to configure the routing and filtering functions in ②.

You're setting up a routing and filtering function.
I know the hardware routers have the same functionality.

As Tanuki said, you can replace the PC in ② with a router (hardware). However, the router is difficult to understand because it is configured by clicking radio buttons. Detailed configuration is also difficult. But you should know that the router acts as a firewall.

Now, let's begin!
Let ② have a packet relay function as a router.
Open /etc/sysctl.conf (file) of ② and set the value of net.ipv4.ip_forward to 1 (enabled) if the value is 0.



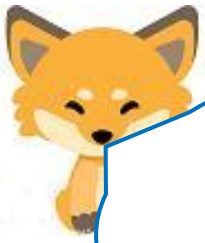
Do you allow IPv4 IP addresses to be relayed?
Now that we have IPv6, I'll have to be careful.

Let's study the settings check first.
Let's check the status of the filtering settings for ②.
The command must be executed as root to be accepted.
If you enter [# iptables -t filter -L] with filter omitted, you get [# iptables -L].

```
root@ubun1204-[redacted] ~
    @ubun1204-[redacted] ~$ sudo -i
[sudo] password for [redacted]
root@ubun1204[redacted]:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubun1204-[redacted] ~#
```



That's the default (default value) configuration state:
no filtering on INPUT, FORWARD, or OUTPUT.
Packets are allowed to pass through. We can hack into it as much as we want.
Next, let's check the routing.
For routing, enter [# iptables -t nat -L].

```
root@ubun1204-[redacted]: ~
[redacted]@ubun1204-[redacted]:~$ sudo -i
[sudo] password for [redacted]:
root@ubun1204-[redacted]:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
root@ubun1204-[redacted]:~#
```

That's also the default configuration state. This state indicates that the routing between "NIC A" and "NIC B" in ② is not configured. This means that packets cannot pass from the PC in ① to the PC in ②. It means that communication is not possible.

I see, so this is how you see the filter and routing settings.

We still have a long way to go, so let's make the rest of this episode 23.

Translated at DeepL