# Computer Science (Episode 24)

## Episode 24 (Security III: Contraption)　network hacking

Tanuki, episodes 22 and 23 were about defensive (shield) security, but now we're going to talk about offensive (spear) security.

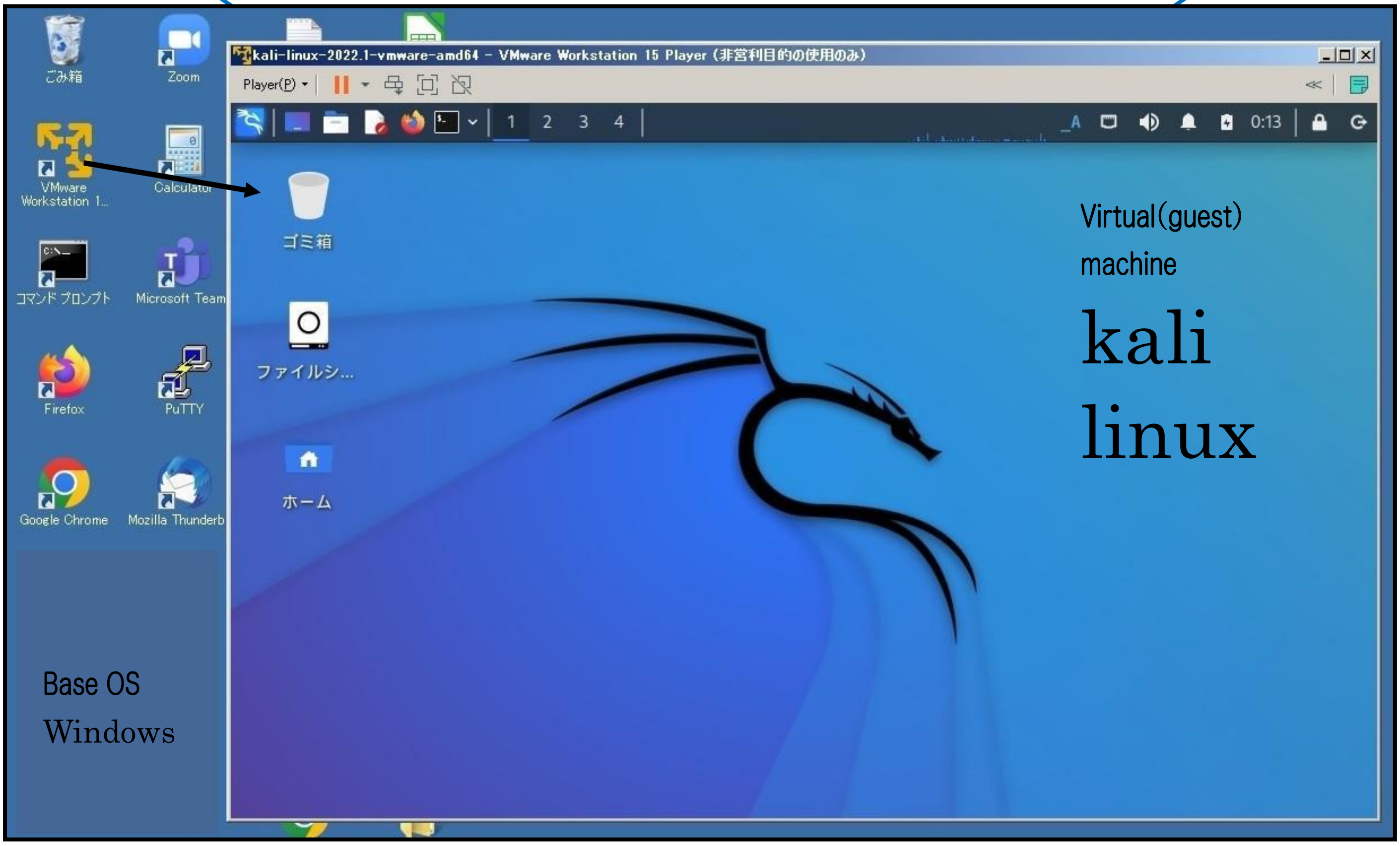
You can practice hacking effectively by using the virtual machine we talked about in episodes 8 to 12. We will use "kali linux" as a virtual machine.

Think of "kali linux" as a server to be hacked and the base OS Windows as a terminal to be attacked. In this way, you can study hacking anywhere with a single laptop. Furthermore, "kali linux" has many tools (aircrack−ng, burpsuit, hyda, john, nmap, sqlmap, wireshark, etc.) for hacking practice installed as standard.

As I said before, you can't target real servers on the Internet for learning to hack. You've got to protect this.

So, virtual environment is very important to learn the technology. If you even have a virtual environment, download "kali−linux−2022.1−vmware−amd64.7z", extract it with "7z2107−x64", save it in an appropriate folder, specify the destination, and click the button "Open Virtual Machine". Then you will see the following image and you can use it.

In other words, the extracted "kali−linux−2022.1−／−" itself is a virtual machine.



Kitsune! I also tried booting "kali linux" in the VMware virtual environment I had created in episodes 8 through 12. It was easy to start, but it was hard to make Japanese language available. Of course, I was able to do it by referring to the Internet.

But "kali linux" is so cool! I feel like I could become a white hacker just by looking at this.

It's true that "kali linux" is cool.

However, "kali linux" is a Debian (Ubuntu) Linux system, so it is easy to operate if you are familiar with Ubuntu's command usage.

Now, network hacking is an attack on a server on a network. In the case of white hat hackers, they need to have a good reason why they are attacking the server or why they have to.

Only with a good cause, the purpose of the attack becomes clear. Examples are as follows.

(1) Obtain the root authority of the server and control the entire server.

(2) Obtain only specific information in the server.

(3) Prevent other users from accessing a specific server.

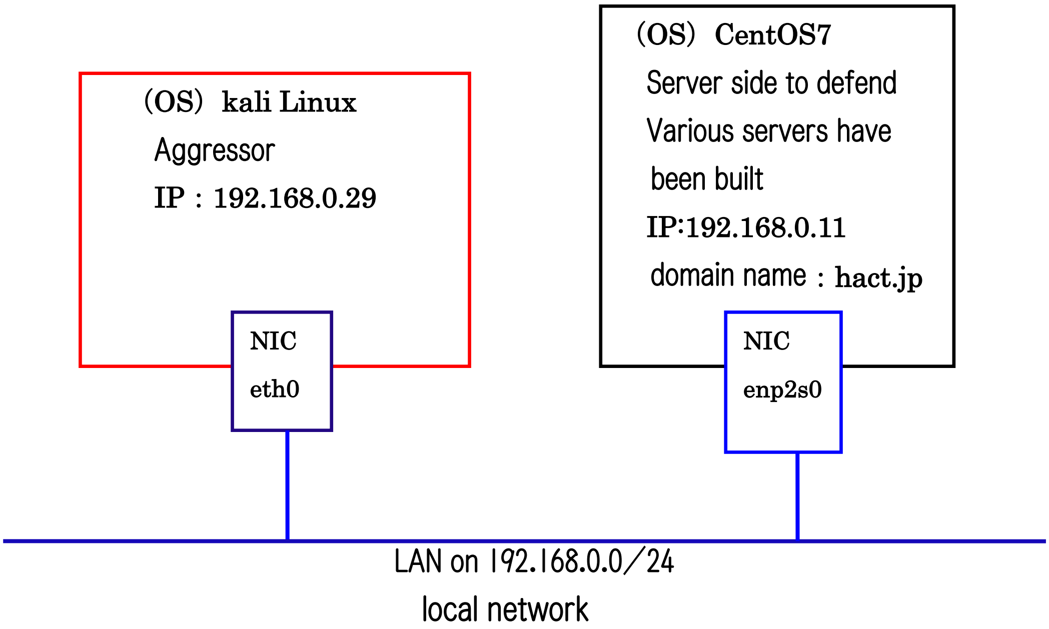
The methods differ depending on the purpose. The method differs depending on the purpose.

I see. So hacking without a cause in the dark makes you a criminal or a black hacker.

I'll have to be careful too.

In order to practice hacking, you need a good learning environment. This is shown below. As mentioned before, you really need a server to hack. You also need a terminal on the attacker's side. We chose "kali Linux" as the terminal, which is equipped with a wealth of tools for attacks.

[Learning environment for network hacking practice.]

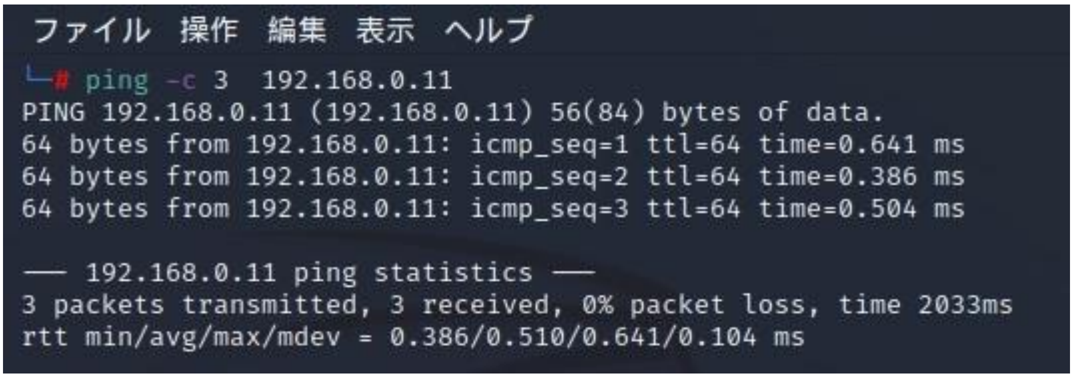


Surely, students who can't build this level of hands−on training environment can't learn network hacking. I'll do my best to build it.

Anyway, to do network hacking, you need basic knowledge about networks.

First of all, ”ifconfig (ipconfig: for windows), ping, traceroute (tracert: for windows), nslookup” to check the connection of PCs on the network are basic commands, so you should try using them.

Let’s start the test with a ping command to determine if the target server exists on the network.The attacker is ”kali linux” and the target is a CentOS7 server.Let’s send a ping from the ”kali linux” side.Ping has multiple options, such as ”−a −c −f −i −j −k −l −n −r −s −t −v −w,” so use them as needed.On the CentOS7 side, it is possible to configure filtering settings so that pings are not accepted. The following screen shows the screen when a ping is accepted.

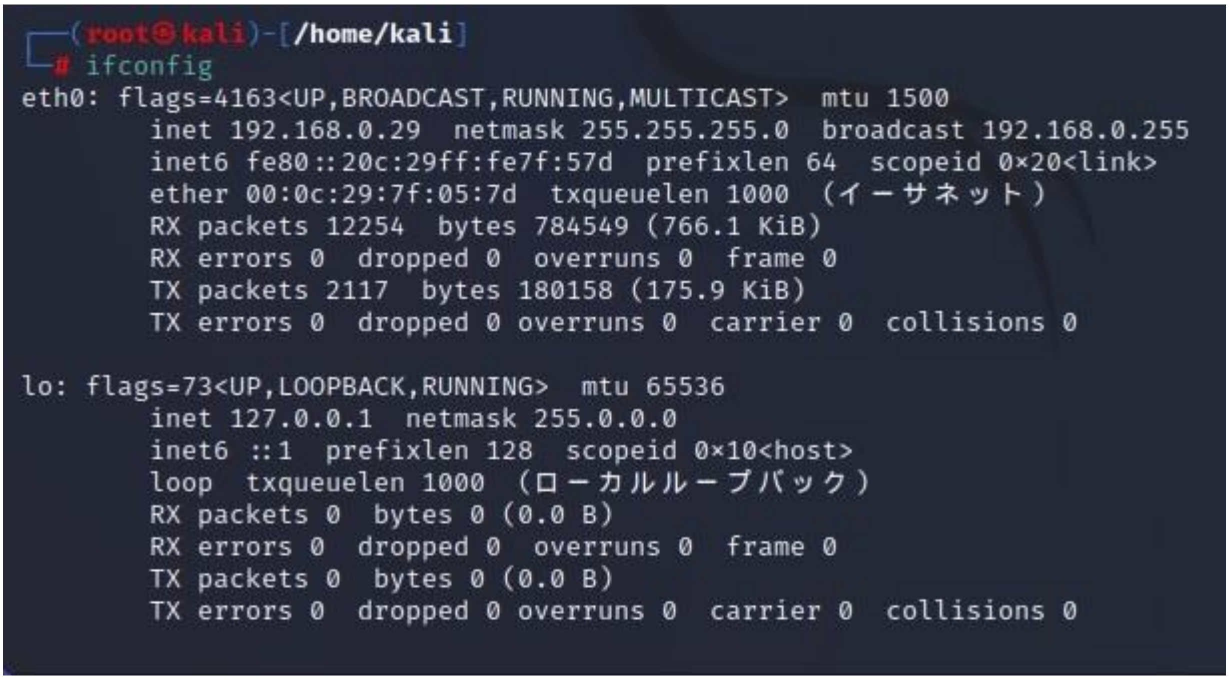


```
└─# ping -c 3  192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=64 time=0.641 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=64 time=0.386 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=64 time=0.504 ms

── 192.168.0.11 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2033ms
rtt min/avg/max/mdev = 0.386/0.510/0.641/0.104 ms
```

You have confirmed that the CentOS7 server exists. The option ”−c 3” means to try to send out three times, right?
What’s the next command?

I also need to know my network environment (NIC status), so let's use ifconfig as well.
The following is its display screen.

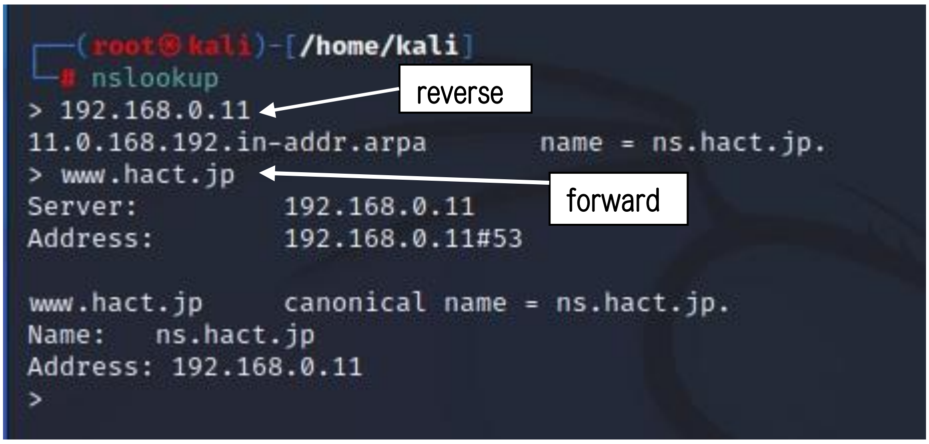


```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.29  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::20c:29ff:fe7f:57d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7f:05:7d  txqueuelen 1000  (イーサネット)
        RX packets 12254  bytes 784549 (766.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2117  bytes 180158 (175.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (ローカルループバック)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

If I use ifconfig, I can also find out the device name (eth0) assigned to the NIC. There are many other things we can find out.
Is the device name (lo) a local area network?
Fox, next..

The next step is an nslookup, which checks for the existence of DNS servers.
There's a forward lookup and a reverse lookup.

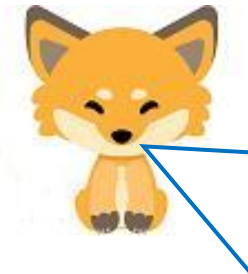


```
┌──(root㉿kali)-[/home/kali]
└─# nslookup
> 192.168.0.11
11.0.168.192.in-addr.arpa       name = ns.hact.jp.
> www.hact.jp
Server:         192.168.0.11
Address:        192.168.0.11#53

www.hact.jp     canonical name = ns.hact.jp.
Name:   ns.hact.jp
Address: 192.168.0.11
>
```

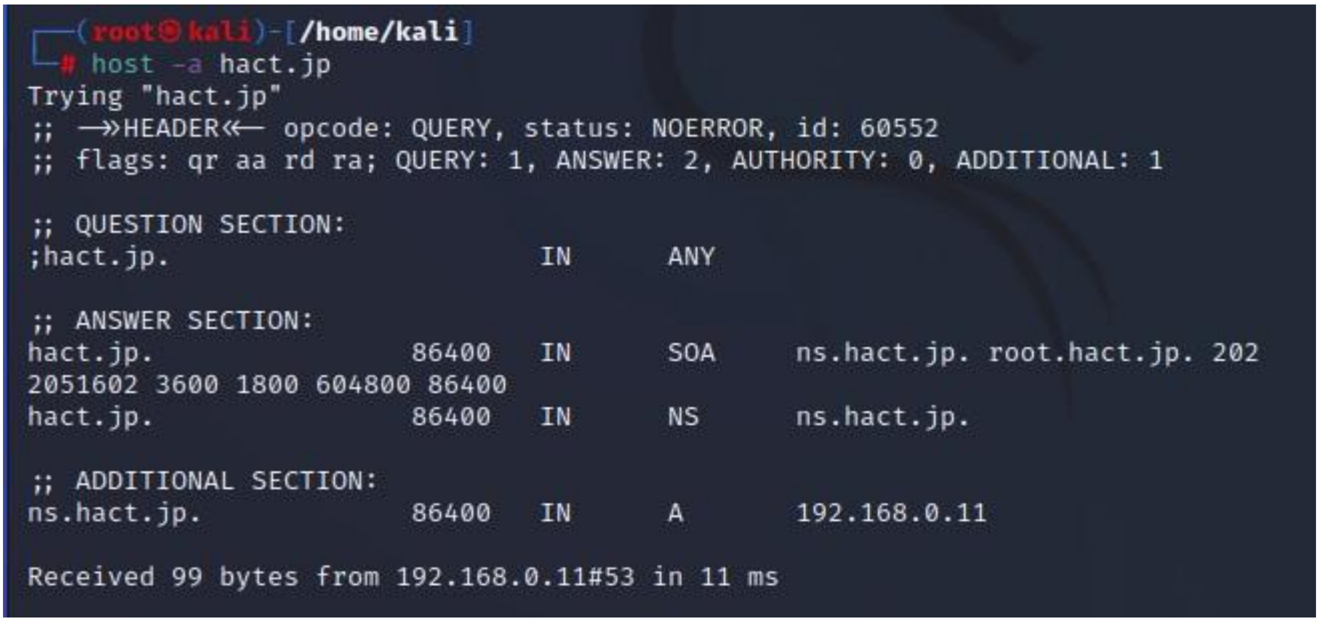
reverse

forward



If you know the domain name (hact.jp) by reverse lookup and use the host command, you can see the contents of the DNS server's forward lookup zone database file.

How to use this depends on your hacking knowledge and your own creativity. You can learn the hacking tools and learn how to use them, but only a moderate hacker knows how to use them. The challenge is to find ways to use those tools that other hackers haven't thought of. The individual hacker's originality will determine his or her superiority.



```
┌──(root㉿kali)-[/home/kali]
└─# host -a hact.jp
Trying "hact.jp"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60552
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;hact.jp.                       IN      ANY

;; ANSWER SECTION:
hact.jp.                86400   IN      SOA     ns.hact.jp. root.hact.jp. 202
2051602 3600 1800 604800 86400
hact.jp.                86400   IN      NS      ns.hact.jp.

;; ADDITIONAL SECTION:
ns.hact.jp.             86400   IN      A       192.168.0.11

Received 99 bytes from 192.168.0.11#53 in 11 ms
```

I see, sure, it's a DNS server zone database file, but I wonder how to use it to look at this. After all, we want to have ROOT privileges, don't we?

Yes, it is how to get ROOT authority. I'll leave the further discussion to the next episode, Episode 25, as it will include packet analysis and so on.
Stay tuned to see how it all unfolds!

Translated at DeepL