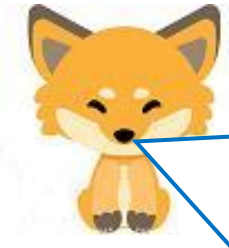
Episode 25 (Security IV: Contraptions)　Port Scanning

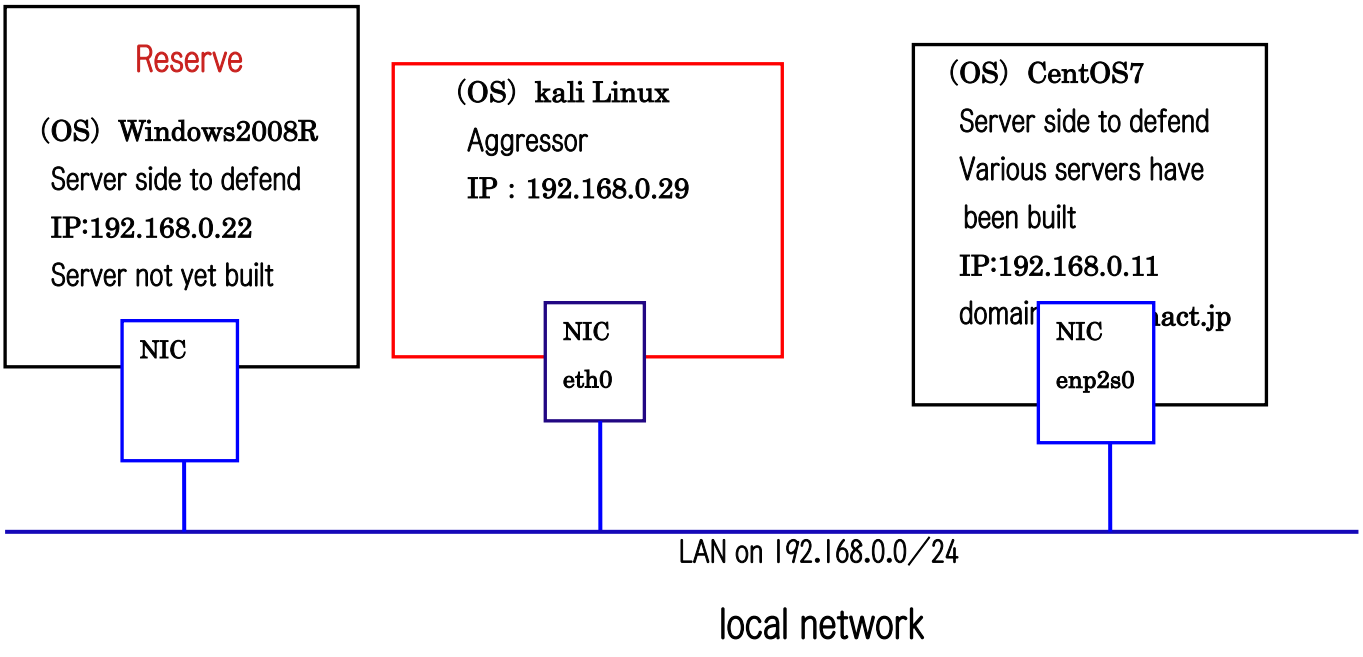


Tanuki, in Episode 25, we will try to see how much open port information we can get from the target server using nmap, a port scanning tool.

Since nmap has many options, it is important to learn how to use it.

In addition, we'll join a spare Windows 2008R server to the target server. But note that the Windows2008R server is being used as a base machine for a virtual machine (kali Linux), so we are not building various servers.

[Learning environment for network hacking practice.]



Various servers on the Internet are assigned a fixed number. That is the port number. The nmap tool can check whether the target port is open or closed, and if it is open, TCP connections and UDP packets can be sent. The purpose of the nmap tool is to check if the port is OPEN or CLOSE.
The first step is a list scan (option -sL). The following is a list scan.

```
root@kali: /home/kali
ファイル  操作  編集  表示  ヘルプ
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] kali のパスワード:
┌──(root㉿kali)-[/home/kali]
└─# nmap  -sL www.hact.jp
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:15 JST
Nmap scan report for www.hact.jp (192.168.0.11)
rDNS record for 192.168.0.11: ns.hact.jp
Nmap done: 1 IP address (0 hosts up) scanned in 0.04 seconds
```

You see that in this local network, the IP address assigned to the URL (www.hact.jp) is one 192.168.0.11 and ns.hact.jp is the DNS server name.
Next ?.

I'll also show you when an error occurs with the Internet port scan. (The -sP option is an instruction to ping scan. (The (-pO) option is an instruction not to ping. Obviously, this is a contradiction. You cannot use these two options at the same time. The following error message will be returned.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap  -sP -p0 192.168.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:16 JST
You cannot use -F (fast scan) or -p (explicit port selection) when not doing a port scan
QUITTING!
```

I see, it's hard to use options.
Next?

I'll try to find out if the ftp server is open or closed, specifying the port number (the port number of the ftp server is 21). First of all, the basic execution without stealth scan is as follows. In this case, a log will be written to /var/log/secure on CentOS7, stating that a port scan from 192.168.0.29 was performed.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap  192.168.0.11 -p21
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:18 JST
Nmap scan report for ns.hact.jp (192.168.0.11)
Host is up (0.00029s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:1A:A0:38:18:F7 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

I can read that the ftp server is open. Next ?.

Next is a port scan to the ftp server, but the (−sS) option is a stealth scan. This means that no log of the port scan from 192.168.0.29 will be logged in /var/log/secure on CentOS7. It's important to note that it won't be logged.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap  -sS 192.168.0.11 -p21
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:20 JST
Nmap scan report for ns.hact.jp (192.168.0.11)
Host is up (0.00032s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:1A:A0:38:18:F7 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds
```

I see. But to check if it is really stealth, I need to log in to CentOS7 and open the secure file. Next?

Next is a TCPconnect() scan. (-sT) option. In this case, the port scan from 192.168.0.29 will be logged in /var/log/secure on CentOS7.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap  -sT 192.168.0.11 -p21
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:22 JST
Nmap scan report for ns.hact.jp (192.168.0.11)
Host is up (0.00069s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:1A:A0:38:18:F7 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

I'd like to see how the server logs port scans, Kitsune,
to present.

OK! I'll show you the secure file in /var/log,
which can only be opened with Root privileges.

```
May 25 16:09:06 cent64 polkitd[740]: Registered Authentication Agent for unix-session:1 (system bus name
bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ja_JP.UTF-8)
May 25 16:24:26 cent64 sshd[3271]: Did not receive identification string from 192.168.0.29 port 36180
May 25 17:00:47 cent64 gdm-password]: gkr-pam: unlocked login keyring
```

This record shows that there was an access
from "kali Linux" (192.168.0.29).
We'll have to learn how to read the log, right?
Next is the (-sV) option.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap  -sV 192.168.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:24 JST
Nmap scan report for ns.hact.jp (192.168.0.11)
Host is up (0.00061s latency).
Not shown: 983 filtered tcp ports (no-response), 10 filtered tcp ports (host-prohibited)
PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      vsftpd 3.0.2
22/tcp  open  ssh      OpenSSH 7.4 (protocol 2.0)
25/tcp  open  smtp     Postfix smtpd
53/tcp  open  domain   ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp  open  http     Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips)
110/tcp open  pop3     Dovecot pop3d
443/tcp open  ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips)
MAC Address: 00:1A:A0:38:18:F7 (Dell)
Service Info: Host:  hact.jp; OSs: Unix, Linux; CPE: cpe:/o:redhat:enterprise_linux:7

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 18.79 seconds
```

You can see that all the servers Kitsune has built are open.

That's right. I didn't apply any filters. Also, all servers are set to start automatically when CentOS7 starts up, so they will be marked as open.
Note that even if no filter is applied, the ports of servers that have not been started will show "close".
The following figure shows the results of a port scan on a spare Windows 2008R server. This one is the default, with no other servers configured.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap  -sV 192.168.0.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:26 JST
Nmap scan report for 192.168.0.22
Host is up (0.00020s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1027/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:A0:B0:55:CA:E6 (I-O Data Device)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 11.41 seconds
```

Next is the IP protocol scan.
The option is (−sO). Instead of the port number, the IP protocol number in use is displayed. Note that (1) is the ICMP protocol number and (6) is the TCP protocol number. The [open | filtered] in the figure indicates a protocol that has not responded even after retransmitting several times.
The above figure shows CentOS7 and the following figure shows the result of IP protocol scan on spare Windows 2008R.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap  -sO 192.168.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:29 JST
Warning: 192.168.0.11 giving up on port because retransmission cap hit (10).
Nmap scan report for ns.hact.jp (192.168.0.11)
Host is up (0.00044s latency).
Not shown: 251 filtered n/a protocols (host-prohibited)
PROTOCOL STATE         SERVICE
1        open          icmp
6        open          tcp
33       open|filtered dccp
47       open|filtered gre
136      open|filtered udplite
MAC Address: 00:1A:A0:38:18:F7 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 274.24 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap  -sO 192.168.0.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:34 JST
Nmap scan report for 192.168.0.22
Host is up (0.00014s latency).
Not shown: 255 open|filtered n/a protocols (no-response)
PROTOCOL STATE SERVICE
1        open  icmp
MAC Address: 00:A0:B0:55:CA:E6 (I-O Data Device)

Nmap done: 1 IP address (1 host up) scanned in 6.37 seconds
```

CentOS 7

Windows2008R

Fox, one question, if I may.
ICMP comes up a lot, what kind of protocol is it?

It is a protocol to check whether the other host (PC) exists or not. If the other host's power is turned off, it also notifies the user that it is turned off (closed).
Ping and Traceroute commands also use the ICMP protocol.
The following figure shows the (−r) option. The top figure shows CentOS7 and the bottom figure shows Windows 2008R. This option randomly scans the ports in use.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap  -r 192.168.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:37 JST
Nmap scan report for ns.hact.jp (192.168.0.11)
Host is up (0.00090s latency).
Not shown: 983 filtered tcp ports (no-response), 10 filtered tcp ports (host-prohibited)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
443/tcp open  https
MAC Address: 00:1A:A0:38:18:F7 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 5.45 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap  -r 192.168.0.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:39 JST
Nmap scan report for 192.168.0.22
Host is up (0.00062s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1027/tcp open  IIS
MAC Address: 00:A0:B0:55:CA:E6 (I-O Data Device)

Nmap done: 1 IP address (1 host up) scanned in 8.81 seconds
```

CentOS7's support https with SSL as well as http.
IIS on Windows 2008R is a web server or this is available by default as well.

Yes, CentOS7's can be accessed at "https://www.hact.jp/".
The next step is to detect the OS used on the target host.
nmap has a ffingerprinting function that can be used by simply adding the (-O) option.
The first one is CentOS7.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap  -O 192.168.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:45 JST
Nmap scan report for ns.hact.jp (192.168.0.11)
Host is up (0.00042s latency).
Not shown: 983 filtered tcp ports (no-response), 10 filtered tcp ports (host-prohibited)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
443/tcp open  https
MAC Address: 00:1A:A0:38:18:F7 (Dell)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
losed port
Device type: general purpose
Running: Linux 3.X|4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
.1
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9, Linux 5.1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.68 seconds
```

I see that CentOS7 shows the Linux kernel version information.

Windows 2008R is next.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap  -O 192.168.0.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:47 JST
Nmap scan report for 192.168.0.22
Host is up (0.00029s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1027/tcp open  IIS
MAC Address: 00:A0:B0:55:CA:E6 (I-O Data Device)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
losed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microso
ft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:m
icrosoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Profession
al or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0,
 Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windo
ws Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.95 seconds
```

I see that this one detects the name of the OS itself, Windows 2008R.
By the way, can you explain a little more about the ffingerprinting feature?

OK! Actually, nmap records data on more than 1,500 operating systems in a database called nmap-os-fingerprints.
nmap collects target host data via TCP and UDP and checks it against the nmap-os-fingerprints database to find the matching OS.
That's called fingerprinting.
In this age of spam, it is important to know how much of your PC environment is readable by the recipient.
Finally, I describe how to check for Heartbleed, which checks for vulnerabilities in OpenSSL. The above figure shows how to investigate CentOS7 and the below figure shows how to investigate Windows 2008R.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap  -sV -p443 --script=ssl-heartbleed 192.168.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:54 JST
Nmap scan report for ns.hact.jp (192.168.0.11)
Host is up (0.00031s latency).

PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
MAC Address: 00:1A:A0:38:18:F7 (Dell)

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 28.52 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap  -sV -p443 --script=ssl-heartbleed 192.168.0.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 16:57 JST
Nmap scan report for 192.168.0.22
Host is up (0.00019s latency).

PORT    STATE    SERVICE VERSION
443/tcp filtered https
MAC Address: 00:A0:B0:55:CA:E6 (I-O Data Device)

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
```

If the white oval shows [State: VULNERABLE], it means that the SSL is vulnerable.
On CentOS7, SSL is open, which means there is no vulnerability.
Windows2008R is not vulnerable because SSL is not used in the fileter display in the first place.

By the way, what is Heartbleed?

I'll include the following article about Heartbleed in the magazine.

Column OpenSSL Heartbleed

OpenSSL 1.0.1 was released on March 14, 2012 without the Heartbleed Bug being noticed. This bug allows a malicious person to send inappropriate heartbeats to the server and receive an arbitrary amount of information from the server's memory as a reply. This means that a malicious person can steal the OpenSSL server's private key. Once the private key is obtained, it would be possible to create a website that is exactly the same as a website for commercial transactions (including online banking) that uses digital signatures. The "https:／／￣" website, which was previously thought to be mostly secure, will no longer be secure.

Since the domain names used in URLs are not allowed to be registered twice, the best way to protect yourself is to check the domain name more than before when accessing the site.

OpenSSL 1.0.1g with bug fixes was released on Monday, April 7, 2014.

OpenSSL installed on Ubuntu 12.04 is 1.0.1.

It is best to assume that the heartbleed bug exists until you upgrade to OpenSSL1.0.1g.

Well, that's enough about how to use nmap. In the next episode (26), we will finally cover packet analysis. Packet analysis is a laborious task.
Stay tuned to see how it all unfolds!

Translated at DeepL