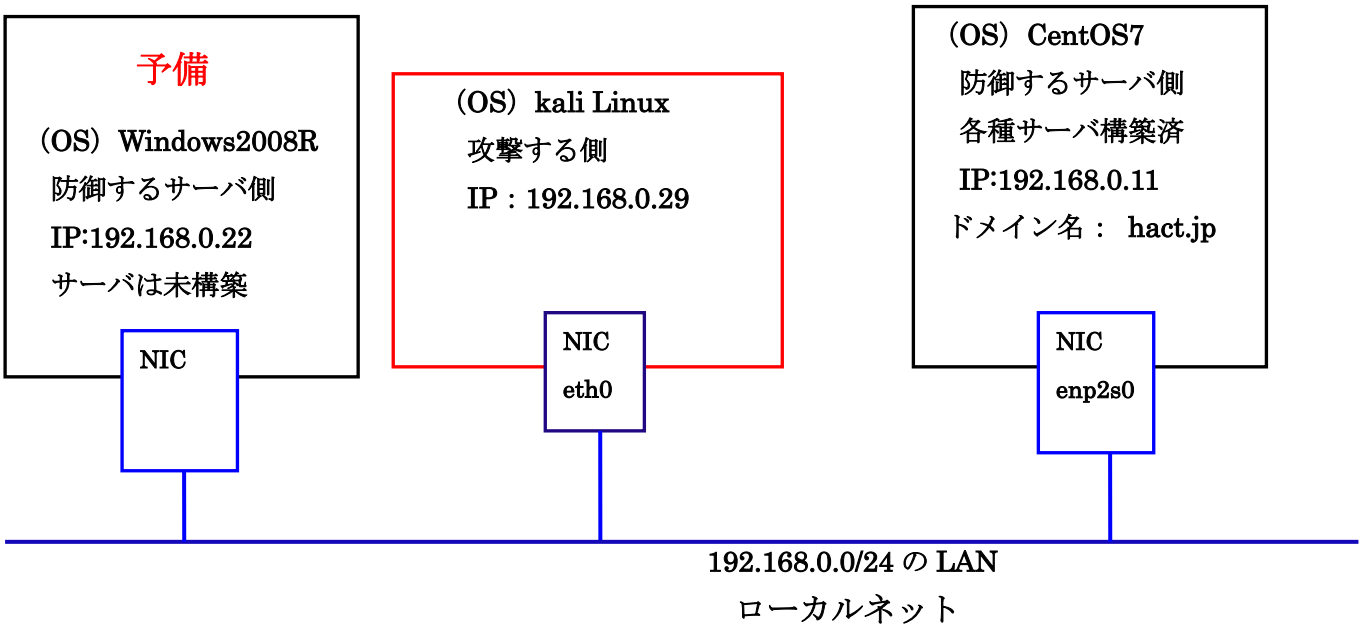
第２５話（セキュリティⅣ：矛）　ポートスキャン

タヌキ、第２５話ではポートスキャンツールのｎｍａｐを使ってターゲットサーバのオープンされているポート情報をどれだけ取得できるか試してみるぞ。

ｎｍａｐには多くのオプションがあるので、その使い方を学ぶのも大切なことだ。
ついでに、ターゲットサーバに予備として Windows2008R サーバも参加させることにする。ただ、Windows2008R サーバは仮想マシン（kali Linux）のベースマシンとして使っているので、各種サーバは構築していないから注意してくれ。

［ネットワーク・ハッキング実習の為の学習環境］



インターネット上の各種サーバには固定の番号が割り振られている。それがポート番号だ。ターゲットとするポートがＯＰＥＮになっているか、ＣＬＯＳＥされているか調べることができるのがｎｍａｐツールだ。ＯＰＥＮ になっていれば、ＴＣＰコネクションやＵＤＰパケットを送りこむことができるのだ。それを調べるのが目的だ。
先ずは、リストスキャン（オプション　–sL）だ。以下のようになる。

```
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
```

このローカルネットワークでは、ＵＲＬ（www.hact.jp）に割り振られているＩＰアドレスは 192.168.0.11 の１個で、ns.hact.jp がＤＮＳサーバ名ということがわかるな。
次は？

インターネットポートスキャンでエラーになる場合も示しておくね。（-sP）オプションは、Ping スキャンの指示です。（-pO）オプションは、Ping を実行しない指示です。明らかに矛盾です。この２つのオプションを同時に使うことができません。以下のようなエラーメッセージが返ってきます。

```
┌──(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!
```

なるほど、オプションの使い方も難しいんだ。
次は？

ftp サーバがオープン状態にあるか、クローズ状態にあるか、ポート番号（ftp サーバのポート番号は 21）を指定して探ることにするね。先ずは基本となるステルシスキャン無しの実行は以下のようになる。
この場合、CentOS7 の/var/log/secure に 192.168.0.29 からのポートスキャンがなされた、というログが記録されるよ。

```
┌──(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
```

ftp サーバは、オープン状態にあることが読み取れるね。次は？

次は、ftp サーバへのポートスキャンだが、（- s S）オプションをステルススキャンになる。つまり、CentOS7 の/var/log/secure に 192.168.0.29 からのポートスキャンのログが記録されない。記録されない、ということは重要だよね。

```
┌──(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
```

なるほどね。でも本当にステルスかどうか確認するためには、CentOS7 にログインして secure ファイルを開く必要があるね。次は？

次は、TCPconnect()スキャンだ。（- s T）オプションを付けた場合だ。この場合、CentOS7 の/var/log/secure に 192.168.0.29 からのポートスキャンのログがしっかり記録されるからね。

```
┌──(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
```

サーバにポートスキャンしたログがどのように記録されるか見てみたいんだが、キツネ、提示してくれる。

OK！/var/log 内の secure ファイルを提示するけれども、これは Root 権限でないと開けないからね。

```
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
```

この記録は、「kali Linux」（192.168.0.29）からアクセスがあったことを示している。
ログの見方も学習しなければならないよね。
次は、（-sV）オプションだ。

```
┌──(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
```

キツネが構築した全てのサーバがオープンになっているのがわかるね。

そうだよ。フィルタはかけていないからね。また、CentOS7 の起動と同時に全てのサーバを自動起動に設定してあるから、open と表示されるよ。
フィルターをかけていなくても、起動されていないサーバのポートは、close と表示されるから注意してね。
以下の図は、予備の Windows2008R サーバに対してポートスキャンしてみた結果だ。此方は、特に他のサーバ類を構築していない、デフォルトのままだ。

```
┌──(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
```

次は IP プロトコルスキャンだ。
オプションは（- s O）だ。ポート番号では無く、使用されている IP プロトコル番号が表示される。ちなみに（1）は ICMP、（6）は TCP プロトコル番号だ。
図に表示されている［open｜filtered］数回再送しても応答が無いプロトコルを指しているのだ。
上図が CentOS7 の状態で、下図が予備の Windows2008R に対して IP プロトコルスキャンした結果だ。

```
┌──(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

キツネ、質問を１つ、良いか。
ICMP って良く出てくるけど、どんなプロトコルだ？

相手のホスト（PC）が存在しているかどうか調べるプロトコルだ。相手のホストの電源が OFF になっている場合も、OFF（close）されていることを知らせてくれる。Ping や Traceroute コマンドも ICMP プロトコルを使っているよ。

次図は、（-r）オプションだ。上図が CentOS7、下図が Windows2008R だ。このオプションは、使用されているポートをランダムにスキャンするのだ。

```
┌──(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 の方は、http だけでなく、SSL を使った https もサポートしているんだ。
Windows2008R の IIS は Web サーバか、これはデフォルトでも使用できるようになっているんだ。

そうだよ、CentOS7 の方は、「https://www.hact.jp/」でアクセスできるよ。
次は、ターゲットホストで使用されている OS の検出だ。
ｎｍａｐには、フインガープリンティング機能というものがあって（-O）オプションを付けるだけで利用できるのだ。
最初は CentOS7 だ。

```
┌──(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
```

CentOS7 の方は、Linux のカーネルの
バージョン情報が表示されているね

次は Windows2008R の方だ。

```
┌──(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
```

此方は、Windows2008R という OS そのものの名称が検出されているね。
ところで、フインガープリンティング機能についてもう少し詳しく説明してくれないか。

OK！実は、ｎｍａｐは、nmap-os-fingerprints というデータベースに 1500 以上のＯＳについてのデータを記録しているのだ。nmap の TCP や UDP でターゲットホストのデータを集め、nmap-os-fingerprints データベースと照合して一致する OS を見つけだしているのさ。そのことをフインガープリンティングというのだ。
いろいろ迷惑メールが来る時代だから、自分の PC 環境のどこまでが相手に読み取り可能なのか知っておくことも、不安解消の為に必要なことだよ。
最後に Heartbleed の調査の仕方を記述しておく。Heartbleed は OpenSSL の脆弱性を調査するものだ。SSL のポート番号は 443 だから、それを指定する。上図が CentOS7 の調査、下図が Windows2008R の調査の仕方だ。

```
┌──(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
```

白の楕円で示した部分に[State：VULNERABLE（脆弱）]と表示されたら SSL に脆弱性があるということだ。CentOS7 の方は SSL がオープンになっており、脆弱性が無いということだ。Windows2008R の方は、そもそも fileter 表示で SSL が使われていないので評価のしようが無いようだ。

ところで、Heartbleed って何だ？

Heartbleed（ハートブレード）については、雑誌に次のような記事が掲載されたので、それを載せておくよ。

コラム　　OpenSSL のハートブリード（心臓出血）

２０１２年３月１４日にハートブリード･バグに気づかないまま OpenSSL1.0.1 が公開されました。このバグは、悪意ある者がサーバに対して不適切なハートビート（生存確認信号）を送信することによってサーバのメモリーから任意の容量の情報を返信として受信することが可能になっているというものです。つまり、悪意ある者が OpenSSL のサーバの秘密鍵を盗むことができるということです。秘密鍵を得ることができれば、電子署名を使用した商取引（ネットバンキングも含む）の Web サイトと完全に同じサイトを作ることができることになります。これまで、ほぼ安全と思われていた「https://～」のサイトも安全でなくなります。URL で使用されているドメイン名は、二重登録が認められていませんので、アクセスする時に、これまで以上にドメイン名を確認することが、さしあたっての防御方法だと思います。２０１４年４月７日（月）にバグを修正した OpenSSL1.0.1 g が公開されています。

Ubuntu12.04 にインストールされている OpenSSL は、1.0.1 です。OpenSSL1.0.1 g にアップグレードされるまでハートブリード・バグは存在している、と考えた方が良いでしょう。

では、ｎｍａｐの使い方についてはこの程度にするよ。

次回の**第２６話**ではいよいよパケット解析を取り上げるよ。パケット解析は根気のいる作業なのだ。

どのように展開されるか、後、御期待だ！