IoT Security -Workshop

Hacking Activities and its countermeasure

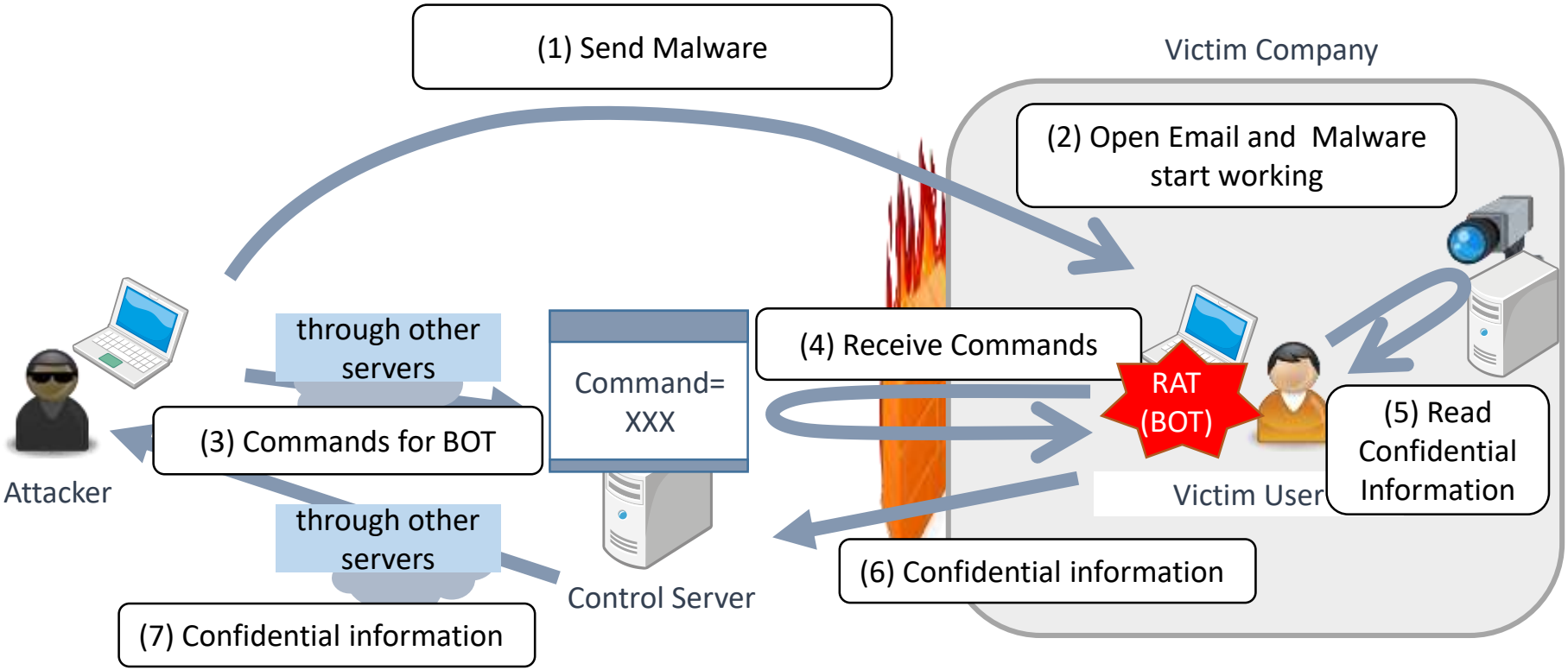
Mirai (malware)

- A malware targets IoT devices with Linux operating system, such as IP cameras and home routers.
  - Mirai uses factory default usernames and passwords to get into IoT devices.
- Infected devices are used for DDoS attacks.
  - On September 19, 2016, attack against French host OVH
  - On October 12, 2016, attack against DNS services provider Dyn
    - More than 100,000 Infected IoT devices are used for the attack.

Examples of user ID and passwords used by Mirai Malware

User ID	Password
root	admin
root	888888
root	default
admin	password
admin	admin1234
guest	guest
(Total of 62 combinations)	

Remote Control Mechanism



出典 IPA　http://www.ipa.go.jp/security/txt/2012/11outline.html

Goal of the workshop

- Intrude to a system and steal photo from the camera connected to the system.
  - Experience the process of "hacking"
  - Learn how to protect the system

- This workshop is performed by groups (Max 10 groups)
  - Each group consists of
    - Hacking operator (1 person)
    - Reporter (1 person)
    - Researcher (all other persons)

Before we start workshop

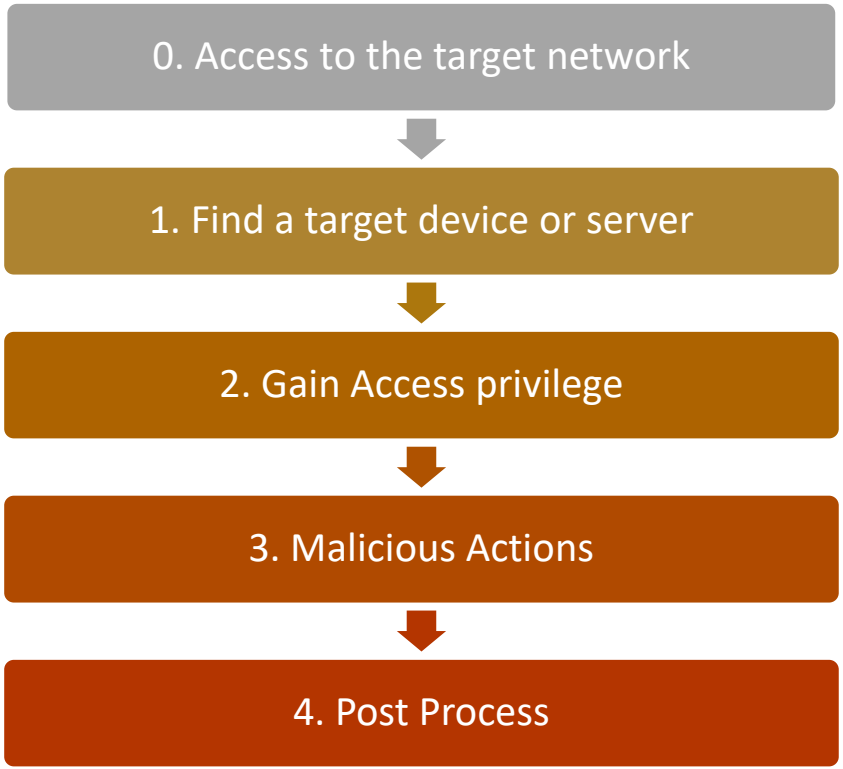
- It is illegal to try to get into system without permission to do so.
  - Act on Prohibition of Unauthorized Computer Access (Japan)

- Do not try what you learn here on any network except those prepared for experiments

出典：http://www.japaneselawtranslation.go.jp/law/detail/?id=2250&vm=04&re=01

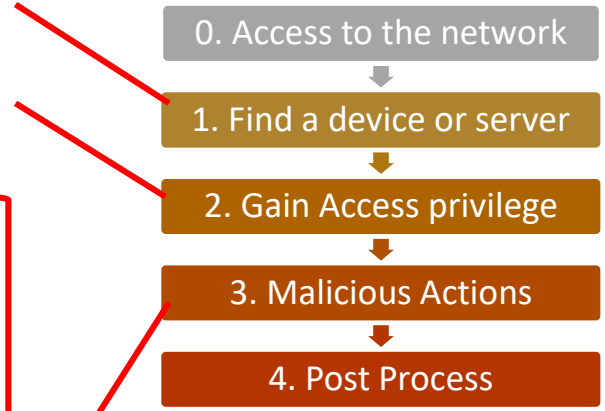
不正アクセスの手順
Typical process of Hacking

Process of Hacking



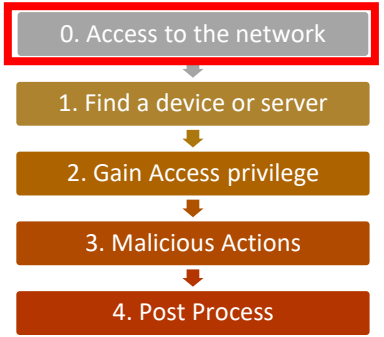
How Mirai works

- Find another device to infect Mirai
  - Try to set up an TCP connection with a random IP address
  - If the device respond, try to login with popular UserID and Password
- Spreading Mirai (Infect the device with Mirai)
  - If succeeded, copy the source code of Mirai malware itself.
  - Compile it on the target machine.
  - Mirai start working on the machine.
- DDos attack
  - Mirai communicate with C&C server and receive commands.
  - Perform DDos attack to a server



User ID	Password
root	admin
root	888888
root	default
admin	password
admin	admin1234
guest	guest
(Total of 62 combinations)	

0. Access to the target network

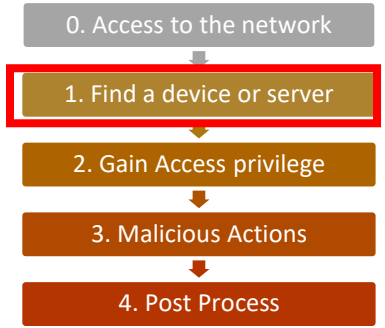


- To attack a Device connect to the Internet (A device with global address)
  - Can be attacked from anywhere in the Internet

- To attack a Device connect to local network
  - Protected by a router and/or firewall

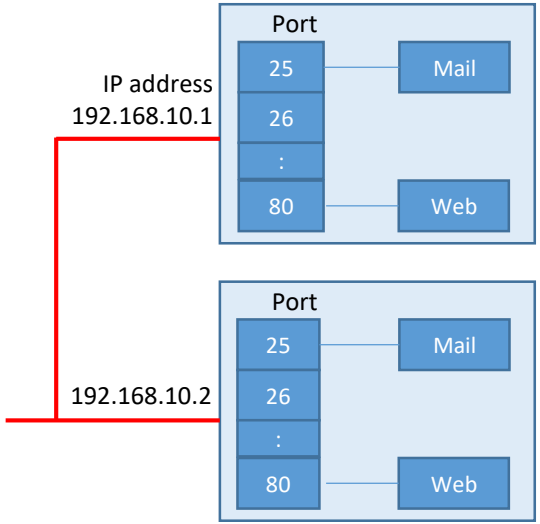
  - Infect a computer virus to the computer on the local network
  - Get in to the Wi-Fi (by getting the Wi-Fi password)

1. Find a target device or server

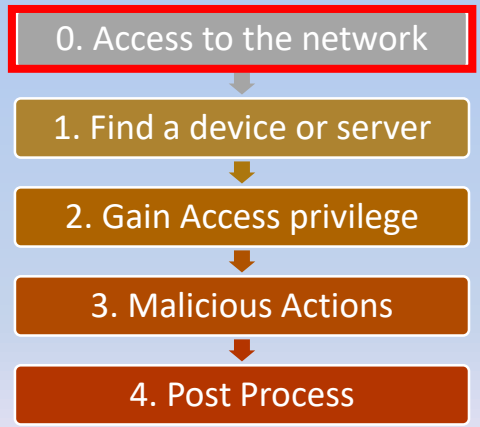


- Address Scan
  - Look for devices connected to the target network
  - Send “ping” command or other packets to all possible addresses. => If responded, that address is used
- Port Scan
  - Look for used port of the server
  - Nmap command
- Banner Check
  - Check OS and software versions

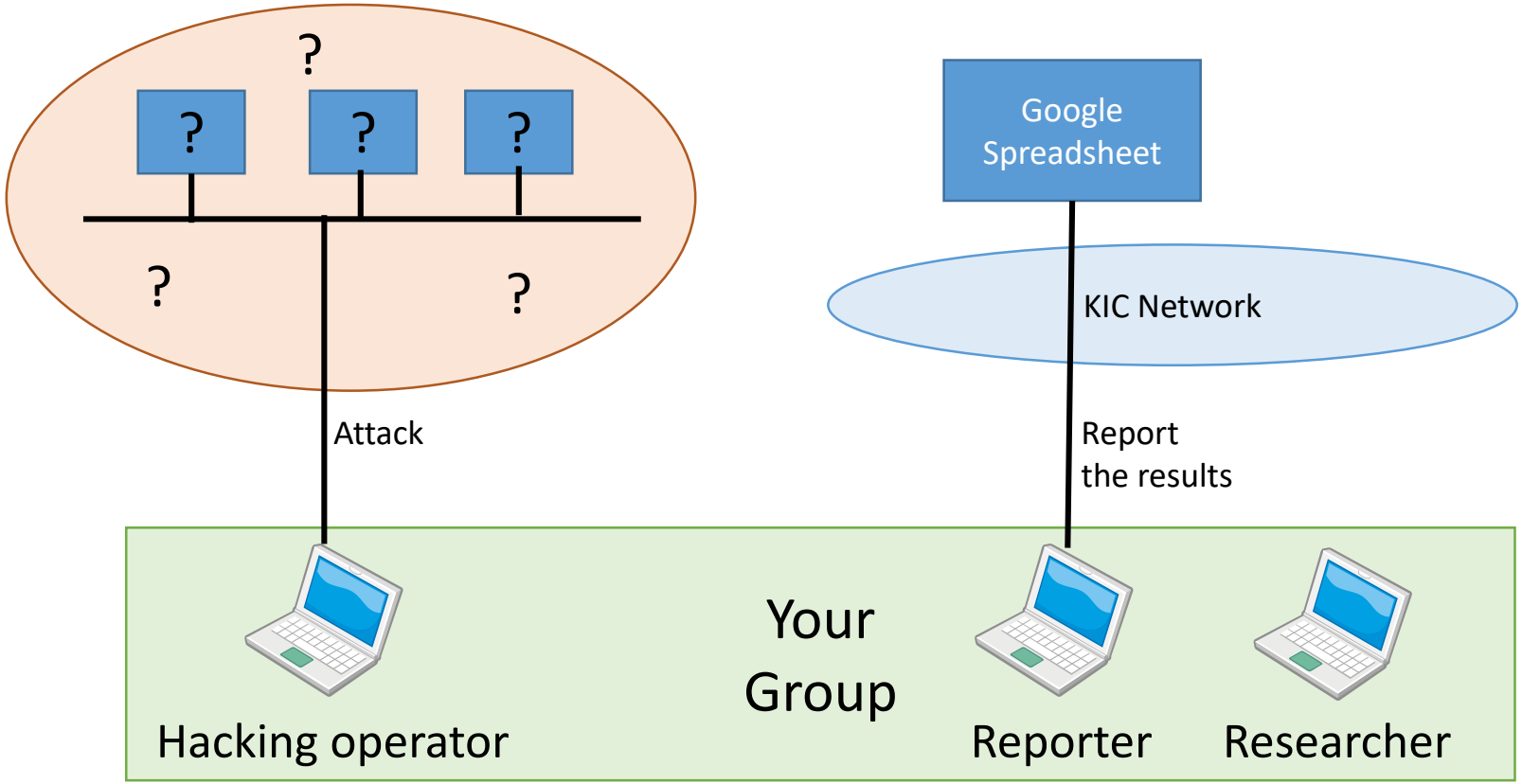
Caution: These actions can be considered illegal attack



Mission 1
試してみよう: ネットワークに接続
Let's Try: Access to the network



Workshop Configuration



Network Scan Tools

- Nmap
  - An open source tool scan IP address and Ports
  - Available for Windows, Linux, Mac

- Caution
  - Do not “scan” servers which you do not own.
    - It is considered preparation of attacking
  - Prepare attackers will scan your servers

Mission1 : Access to the network

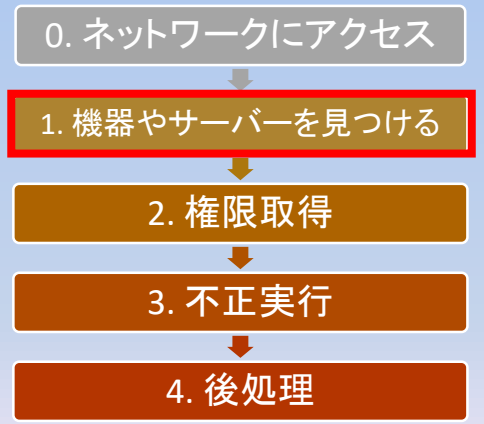
Hacking operator :

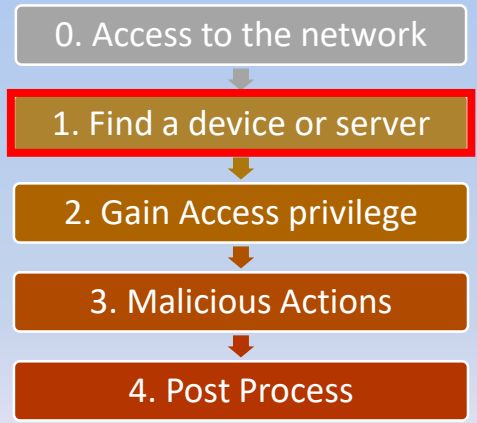
1. Connect to the Hacking environment (Network)
   - Open "Settings" and Connect "Wi-Fi"
     - SSID: Security-WS
     - Password: KICKICKIC
   - Turn Off Ethernet connection (Disconnect from other networks)
2. Check the IP address of Wi-Fi interface of your machine
   - Hint: Use following command on "terminal"
     - "ipconfig" Command (Windows)
     - "ifconfig" command (Linux)

Reporter

1. Do not connect to the Hacking environment.
2. Open chrome browser.
3. Open the workshop Spread Sheet https://shorturl.at/atKNR
4. Follow the link to the page of your group
5. Enter data for Mission 1
   - Name and Student ID
   - IP address and subnet mask of Hacking Machine

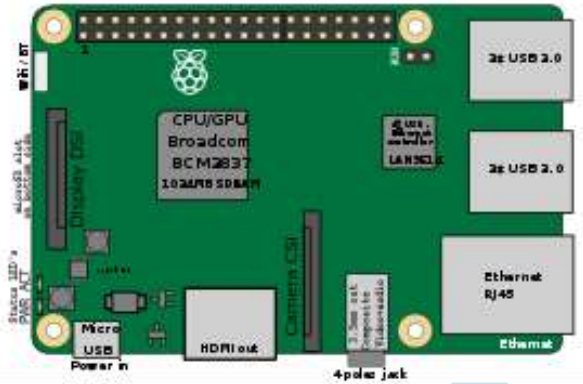
Mission 2
機器やサーバーを見つける
Find a target device or server





Raspberry Pi

- A small single-board computers with ARM CPU
- Developed by the Raspberry Pi Foundation (UK)
- Widely used for education, IoT experiments and prototypes
- In many cases, Debian-based Linux distribution (Raspbian) is used as OS



Mission2 ：Find a target device or server

Hacking operator：

1. Use Nmap and perform "Quick scan" on the network

```
nmap 192.168.220.0/24
```

2. For all the devices you found recode the information of the device
   - IP Address
   - Manufacture
   - Opened Ports（Network Function）

- Identifying OS type and Services

```
nmap -A 192.168.220.0/24
```

Researcher

1. Research on the Internet

Reporter

1. Report the information found to the Report page

Transport layer address

- TCP / UDP port number
  - Address within host (a computer)
  - Port number identifies the application
  - 16 bits, a number from 0 to 65535

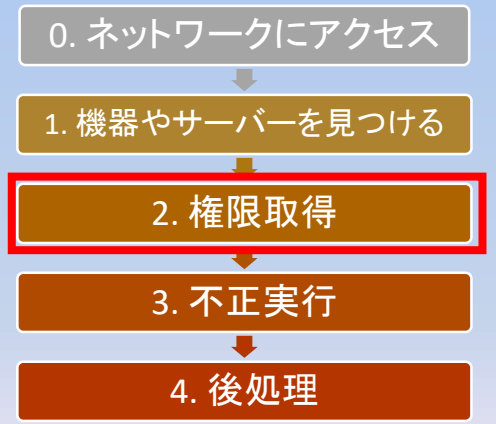
review
What is the data link layer address?
What is the network layer address?

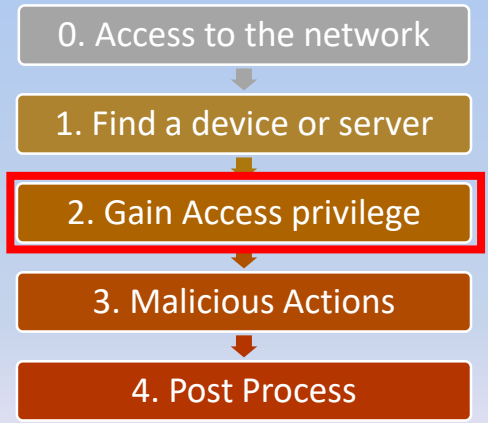
well known Port numbers (Examples)

http://www.iana.org/assignments/port-numbers

Port Number	Description
0/TCP,UDP	Reserved
20/TCP	FTP – Data transfer port
21/TCP	FTP – Control port
22/TCP,UDP	Secure Shell (SSH)
23/TCP	Telnet
25/TCP,UDP	Simple Mail Transfer Protocol (SMTP)
53/TCP,UDP	Domain Name System (DNS)
67/UDP	Dynamic Host Configuration Protocol Server (DHCP)
68/UDP	Dynamic Host Configuration Protocol Client(DHCP)
80/TCP,UDP	Hypertext Transfer Protocol (HTTP)
110/TCP	Post Office Protocol 3 (POP3)
123/UDP	Network Time Protocol (NTP)
143/TCP,UDP	Internet Message Access Protocol (IMAP)
443/TCP,UDP	Hypertext Transfer Protocol over TLS/SSL (HTTPS)

Mission 3
権限取得 (機器にログインする)
Gain Access privilege (Log in the device)





Gain Access privilege

- ID
  - root, administrator, pi, (name of user) etc.
- Passwords
  - “Default” password ("raspberry" for Raspberry Pi)
  - Popular passwords
  - Dictionary attack (Next page)
  - Brute Force attack
  - Keyboard logger
- Utilize the Vulnerability of the System

Use of “popular” password

- Many peoples use popular passwords
  - 4.7% of users have the password password;
  - 8.5% have the passwords password or 123456;
  - 14% have a password from the top 10 passwords
  - 40% have a password from the top 100 passwords
  - 79% have a password from the top 500 passwords
  - 91% have a password from the top 1000 passwords
  - Source: https://xato.net/passwords/more-top-worst-passwords/#.VG7UaousVlw (2011)
- Many people use same password for different services
  - Once your ID and password are stolen from a service, that ID and password may be used to attack other services
  - Check: http://haveibeenpwned.com/

Order	Password
1	password
2	123456
3	12345678
4	1234
5	qwerty
6	12345
7	dragon
8	pussy
9	baseball
10	football

Mission3 : Log in to the device

Hacking operator :

1. Find a Raspberry Pi on the network and log in to it. (You can log-in only one of the two Raspberry Pis)
   - Use ssh command on the Windows command prompt (or Linux shell)

   ssh userID@ip-address

   - User ID
     - Your Group name (all small characters) (group-a, group-b etc.)
   - IP address is that of the raspberry pi you found. (The one with smaller number)
   - Password
     - Hint
       - One of the popular password

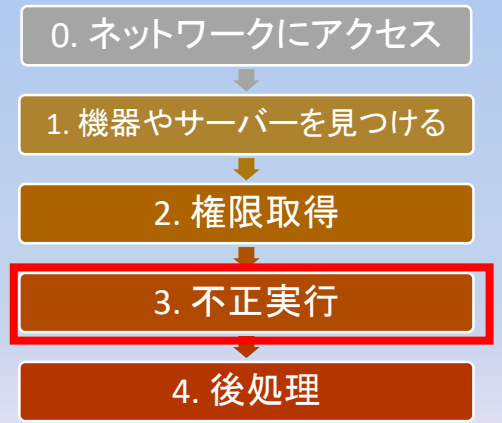
Researcher

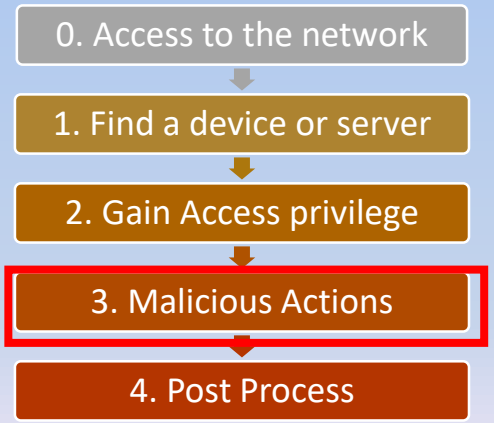
1. Research on the Wikipedia for "the most common passwords"

Reporter

1. Report the found password to the Report sheet

Mission 4
不正実行
Malicious Actions





Investigate Raspberry Pi you just logged in

- Check devices connected to USB
  - lsusb command

```
lsusb
```

Mission 4 : Take a photo using USB camera and download it

Hacking operator :

1. Take a photo using USB Camera
   - use "fswebcam" command

```
fswebcam image.jpg
```

   - "image.jpg" is the file name to save the photo image

2. Download the phono
   - Open a new terminal window on your PC and use "scp" command to copy the image file to your PC

```
scp userID@ip-address:~/image.jpg   .
```

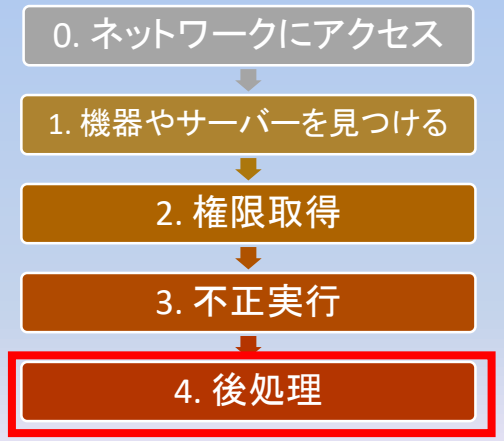
Researcher

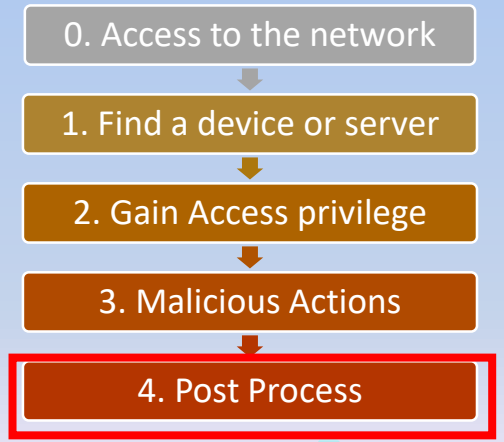
1. Research on the Internet

Reporter

1. Report the success of downloading the photo

Mission 5
後処理
Post Process





Possible post process activities

- Prepare for future login
  - Create another user account
  - Create a back door

- Log data
  - Your IP address and log-in activities are recorded on the syslog
  - To Erase traces of your log-in, you need to erase logs.

Mission 5 : Post Process

Hacking operator :

1. Read the Log file. Identify the IP address of the machine which is used to log-in to the account.

   - Read the Log file

```
cat /var/log/auth.log
```

   - You can use grep command

```
cat /var/log/auth.log | grep group-a
```

Researcher

1. Research on the Internet

Reporter

1. Report the IP address of intruder

まとめ：守るためには
Summary: How to Protect

How to protect your servers

- Set strong password
  - Do not leave the default password
  - Avoid popular password, popular words, person's name, birthday etc.
  - Use a random string with alphabet and numbers
  - Use public key password if possible.
- Update OS and software to the most recent version
- Store and Check system log
  - Store the log on a separate log server
  - Detect suspicious log-in
  - Detect log-in failures (wrong password)
- Network Monitoring (IPS, IDS, UTM)
  - Detect Repeated login trial
  - Detect Address scan and port scan

Questions and Comments

- Sent Questions and comments to

shima@kic.ac.jp

- This material is available at

https://github.com/kic-shima/UTYCC2020/