MATSUURA LAB.

[Cryptography and Information Security]

Department of Informatics and Electronics

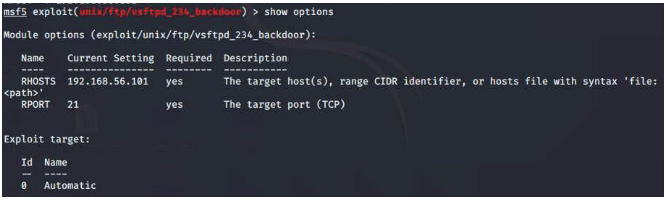
Information Security

Information and Communication
Engineering Department,

http://kmlab.iis.u-tokyo.ac.jp/

- Penetration Test
  - In order to prevent attacks due to exploitation of vulnerabilities in advance, a pseudo attack is performed by a security engineer with excellent technology.
  - Very useful, but requires good engineers and high costs.

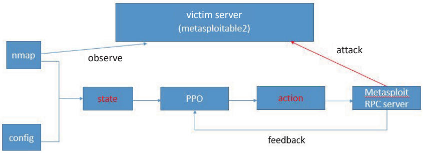
  → Use deep reinforcement learning to explore the possibility of efficient automation.
- metasploit
  - A penetration testing framework that brings together a large number of attack programs.
  - It can be called as an API from within the program via the RPC server, and deep reinforcement learning and cooperation can be performed.



```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.101   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:
<path>'
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

(Top) metasploit screen

(Right) Conceptual diagram of Metasploit automation based on an open source program called Deep exploit


victim server
(metasploitable2)
nmap
observe
attack
state
PPO
action
Metasploit
RPC server
config
feedback