**Kali Linux Tutorial for Beginners**

* ls options

-l : long listing

-a : show hidden files

-t : arrange new files first

-r : arrange in reverse name

-rt : older first

-h : show file size at human readable(eg. 1M, 1.5G)

* cp options

-i : When you copying the existing file name, Microsoft ask to you overwrite or rename but linux is doesn’t it. So you set the -i options, cp is working interactively like Microsoft.

* mv options

-i : mv is also apply the default linux rule like cp. -i options is enable interactively mv.

* rm options

-i : rm is have same options like cp, mv.

* Apt

apt is package management software on debian distribution. When you use install a package, remove, update etc.

apt-get install [package\_name] : install the package

apt-get remove [package\_name] : remove package but config file is leave on the machine.

apt-get purge [package\_name] : remove package with config files

apt-get update : update a repository

apt-cache search : search for package

apt-cache show [package\_name] : display information of package

apt have more than option excluded above command.

* Dpkg

Not only apt, but you can download use dpkg. Sometimes you need to download from internet some package extensions like deb. It is debian package file and for installed on the local machine, open the terminal and typing this.

Dpkg -i [file\_name].deb

When remove for package, change the options i to r.

* Archive & Compression

Archive is use for backup size isn’t changed. But compression is can reduce the file size.

Tar is archive tool in Linux.

Tar c : Create archive

tar r : Append to archive

tar t : List contents of archive

tar x : Extract archive

tar v : Verbose

tar f [file] : File to use

Compression tool is have two choice. Gzip is classic compression tool in linux, bzip2 is more compression than gzip but need more time to compress. Whatever their look similar how to use. For decompress file, add the d option.

Tar also can compress the file when archiving. If you want to gz type, add the z option. Or bzip2 type, add the j option. File extension is must set the tar.gz or tar.bz2.

* Netstat

Netstat is show on your terminal about what would you use the service like http, ftp etc.

-a : all

-n : show numerical address

-t : tcp

-p : show the name of the program

-u : udp

* User

adduser is create user with home directory but useradd is don’t create home directory when create new user. Userdel is delete just user, the other hand deluser --remove-home is delete user with them home directory.

Process

Process is minimum unit of service on system. In linux, we can managed with “ps” command them. And they have an unique ID each other.

Ps : List of processes of current session

ps -f : List processes with full formatting

ps -e : List all processes

ps -u [username] : List processes of [username]

ps -p [pid] : Display information PID

* nohup

For run in the background, we add the end of command &. But & is affected the terminal connectivity. If you want to running background not relying on terminal connectivity, use the nohup. Syntax is easy.

“nohup [command] &”

* cut

문자열을 자를 때 사용할 수 있는 명령어로 다양한 옵션과 결합하여 사용이 가능하다.

* apropos

문자열의 내용을 포함하고 있는 명령어를 출력해준다. 사용법의 경우 apropos [String] 이다.

Target System에서 무언가 스크립트를 다운받아 실행하고 싶다면 tmp directory에 설치하는 편이 좋다. Tmp directory의 경우 어떤 user든 다운로드와 파일을 실행할 수 있다.(아마도 기본적으로)

* Shell

bind shell : netcat과 같은 도구를 이용하여 target 서버에서 shell 접속이 가능하도록 bind를 지정한다. 그 후 attacker가 해당 주소로 접속해 shell을 획득한다.

Reverse shell : bind shell과 같이 netcat 툴을 이용하여 shell을 취득하는 방법이다. 그러나 이 경우 attacker에서 bind를 하고 target 서버에서 attacker로 접속하는 방법이다. 그러나 shell 취득의 경우 attacker에서 target 서버의 shell을 취득할 수 있다.

Bind shell과 Reverse shell의 가장 큰 동작에서의 차이점은 bind shell의 경우 설명에서 알 수 있듯이 target에서 -e option을 통해 쉘 접속이 가능케 함과 동시에 port를 열어주는 반면, reverse shell의 경우 attacker에서 port를 열지만 -e option을 통해 쉘 사용을 지정하는 것은 target에서 attacker로 연결할 때 사용해준다.

Reverse shell의 주요 목적은 방화벽 우회이다. 만약 방화벽에서 service port 이외의 port를 차단할 경우 target에 port를 열어도 접근할 수 없는데 대부분의 방화벽은 내부에서 외부로 나가는 패킷에 대해서는 차단하지 않는 점을 이용하여 attacker로의 연결을 유도하는 것이다.

* MSFPC

Metasploit을 사용할 때 자신이 사용하고 싶은 payload를 custom 할 수 있는 툴이다. CLI 환경으로 구성되어 있다.