Xingyiquan is Simple and basic lkm r00tk1t for linux kernel 2.6.x and 3.x

Developed by Sw0rdm4n (@sw0rdm4n)
Official Website :
- www.ringlayer.net
- www.cr0security.com

DISCLAIMER

This kernel rootkit is just for educatinal purpose and shouldn't be used for any illegal activities, use this at your own risk.

INSTALLATION

To install, just type : ./install

CONFIGURATION FILES

- xingyiquan configuration file for userspace utility is at xingyi_userspace_src/xingyi_userspace_config.h
- xingyiquan configuration file for kernel space rootkit is at xingyi_kernel_src/xingyi_lkm_config.h

DEFAULT PORTS AND PASSWORDS

- default bindshell port : 7777
- default bindshell password : sw0rdm4n
- default netfilter hook port for reverse shell : 1337
- default port to get reverse shell : 7777
- default root shell binary: xingyi_rootshell
- default root shell password : sw0rdm4n (specified at argument)

FUNCTIONS

- escalate privilege

This rootkit has a binary utility named xingyi_rootshell, once this rootkit installed, you can get rootshell by type : ./xingyi_rootshell "sw0rdm4n". String "sw0rdm4n" is default password for root shell, This string is written in
userspace config file at xingyi_userspace_src/xingyi_userspace_config.h

- bindshell

This rootkit has a default bind shell on port 7777 using default password : "sw0rdm4n". String "sw0rdm4n" is default password for bind shell, This string is written in userspace config file at xingyi_userspace_src/xingyi_userspace_config.h

- reverse shell

This rootkit has reverse shell functionality which will be triggered by netfilter hook, in order to get reverse shell to your ip via port 7777, you must fire telnet on port 1337 to the box where you install this rootkit. Before that make sure you prepare a netcat listener on port 7777.

- another common functions

Another common functions : hide files/dirs, hide connections, hide module, hook kill process, hook open, hook open directory.

THANKS

Thanks to all people at:

http://www.cnhonkerarmy.com/forum.php
http://www.zoyzo.cn
http://www.bcwhy.com/
http://bbs.hack99.cn/forum.php
http://blog.yufeng.info/
http://www.kernelchina.org
http://www.cloud-sec.org
http://lengmo.net/
http://www.lenky.info/
https://www.freebsdchina.org/forum/
http://www.indonesianbacktrack.or.id
http://www.security-hooligan.com