Josh Ruppe

Security Researcher, Speaker, & Penetration Tester

user@site:/# locate

Subscribe via RSS

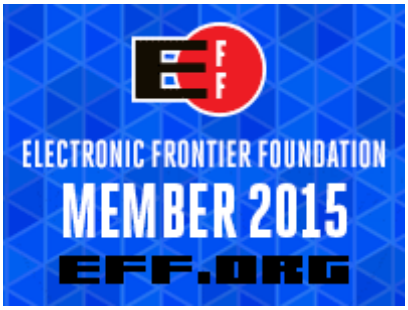
Projects

LinkedIn

Twitter

Github

Contact



Basic Windows Privilege Escalation

10 months ago

As I have been working through my OSCP course I have had to reference several cheat sheets and blog posts for windows enumeration, and while its not a **major** inconvenience, I figured I would put what I already knew and what I have found in one location for everyone's benefit. This list is by no means complete and I will update it as I come across more information and from what is contributed in the comments. **Note:** this is heavily influenced by g0tmilk's Linux Privilege

Josh Ruppe

Security Researcher, Speaker, & Penetration Tester

user@site:/# locate

Subscribe via RSS

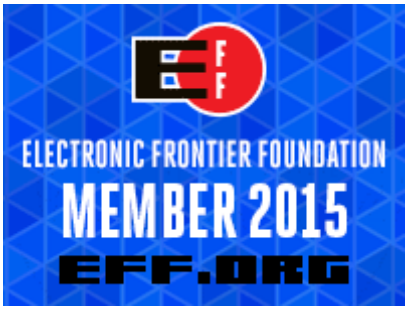
Projects

LinkedIn

Twitter

Github

Contact



Escalation post, so the overall layout credit goes to him.

Operating System

What version of windows is running? Is it 32 or 64-bit?

```
ver
systeminfo
more c:\boot.in
wmic os get osa
```

Hostname?

```
set computernam
hostname
```

What drives are there? Are any being shared?

```
wmic logicaldis
net share
wmic share
net use
```

Josh Ruppe

Security Researcher, Speaker, & Penetration Tester

user@site:/# locate

Subscribe via RSS

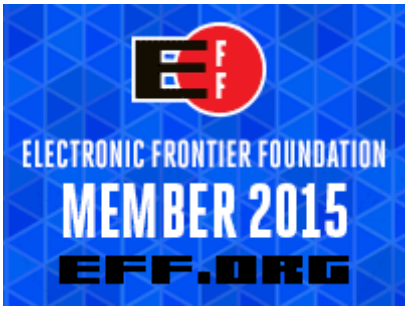
Projects

LinkedIn

Twitter

Github

Contact



What can the OS variables tell you?

```
more C:\WINDOWS
more C:\WINDOWS
more C:\Users\u
path
echo %path%
set
tree (massive o
wmic context
wmic bootconfig
wmic environmen
wmic loadorder
wmic startup
```

What patches are installed?

```
wmic qfe
```

What services are installed/running?

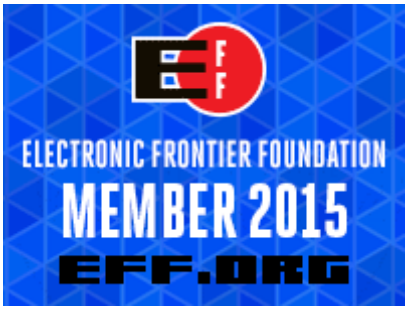
```
wmic service
net start
sc query
```

Network

What is the current network config? What

Josh Ruppe

Security Researcher, Speaker, & Penetration Tester



is this machine talking to?

```
ipconfig /allco
getmac
wmic nicconfig
route PRINT
netstat -ano
arp -a
nbtstat
wmic nicconfig
```

What is the firewall configuration?

```
netsh dump
netsh firewall
netsh firewall
netsh advfirewa
netsh advfirewa
```

Is the machine on a domain?

```
set userdomain
net view /domai
```

Installed Software

What software is currently running?

Josh Ruppe

Security Researcher, Speaker, & Penetration Tester

user@site:/# locate

Subscribe via RSS

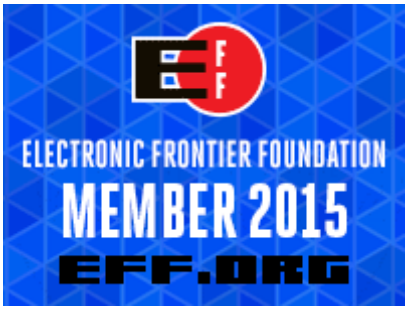
Projects

LinkedIn

Twitter

Github

Contact



What is installed?

```
tasklist
tasklist /svc
tasklist /fi “p
tasklist /fi “u
qprocess
driverquery /v
assoc
wmic sysdriver
wmic product
```

User Info

Who is logged in? Who is an administrator? Who belongs to what group/domain?

```
set username
whoami
echo %username%
net users
wmic group
net localgroup
net localgroup
qusers
qwinsta
wmic useraccoun
```

Registry

What is in the registry?

```
1 reg query
2 reg query "HKLM
```

Hardware Information

What is installed in this PC?

```
1 wmic bios
2 wmic baseboard
3 wmic cdrom
4 wmic cpu list f
5 wmic csproduct
```

Josh Ruppe

Security Researcher, Speaker, & Penetration Tester

user@site:/# locate

Subscribe via RSS

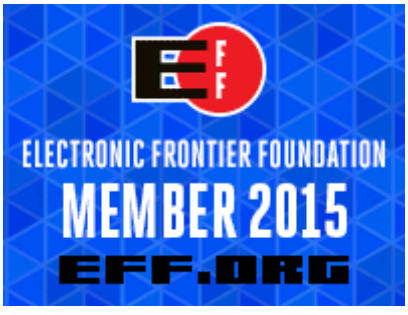
Projects

LinkedIn

Twitter

Github

Contact



Josh Ruppe

Security Researcher, Speaker,

Josh Ruppe

Security Researcher, Speaker, & Penetration Tester

user@site:/# locate

Subscribe via RSS

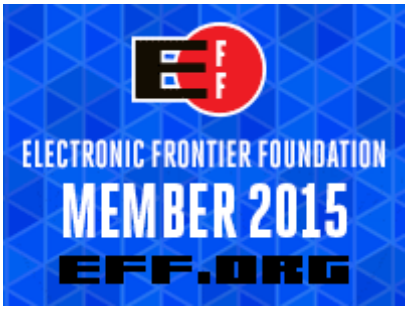
Projects

LinkedIn

Twitter

Github

Contact



Penetration Tester, Eater of Delicious Burgers, Avid Runner.

Atlanta, GA

Josh Ruppe

Security Researcher, Speaker, & Penetration Tester

user@site:/# locate

Subscribe via RSS

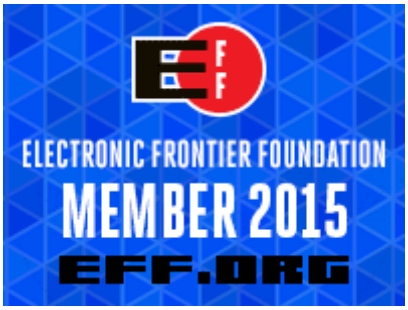
Projects

LinkedIn

Twitter

Github

Contact



Opinions expressed are solely my own and do not express the views or opinions of my employer.

Comments

Community Login

1

Recommend Share

Sort by Best

Start the discussion…

Be the first to comment.