



Breaking Windows

Feb - PenTest



PenTest Methodology



Enumerate



Exploit



Escalate

Enumeration

OSINT

NMAP

SERVICES

Initial Access

01

- What Services are running?

02

- Do you know the credentials?

03

- What can you exploit?

Enumeration

PERMISSIONS

FILES

USERS

Escalate Privileges

01

- What permissions do you now have?

02

- What files can you exploit?

03

- What can you do with that knowledge?

Enumeration

APPLICATIONS

CREDENTIALS

ENCRYPTION

Gain Root Access

01

- What permissions do you now have?

02

- What files can you exploit?

03

- What processes can you hijack?



What did we learn?

Enumerate - Exploit - Escalate

