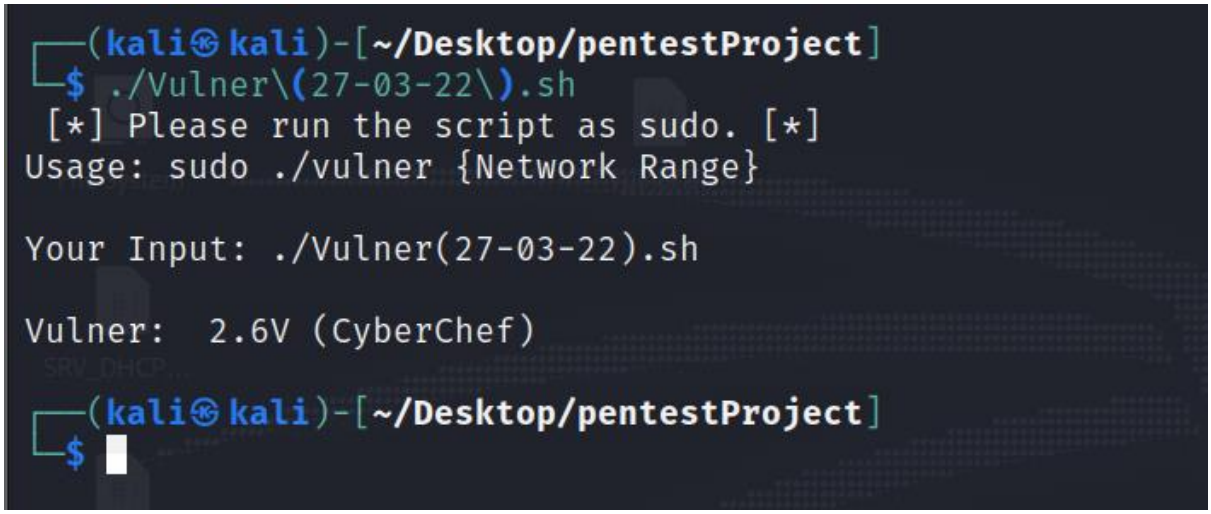
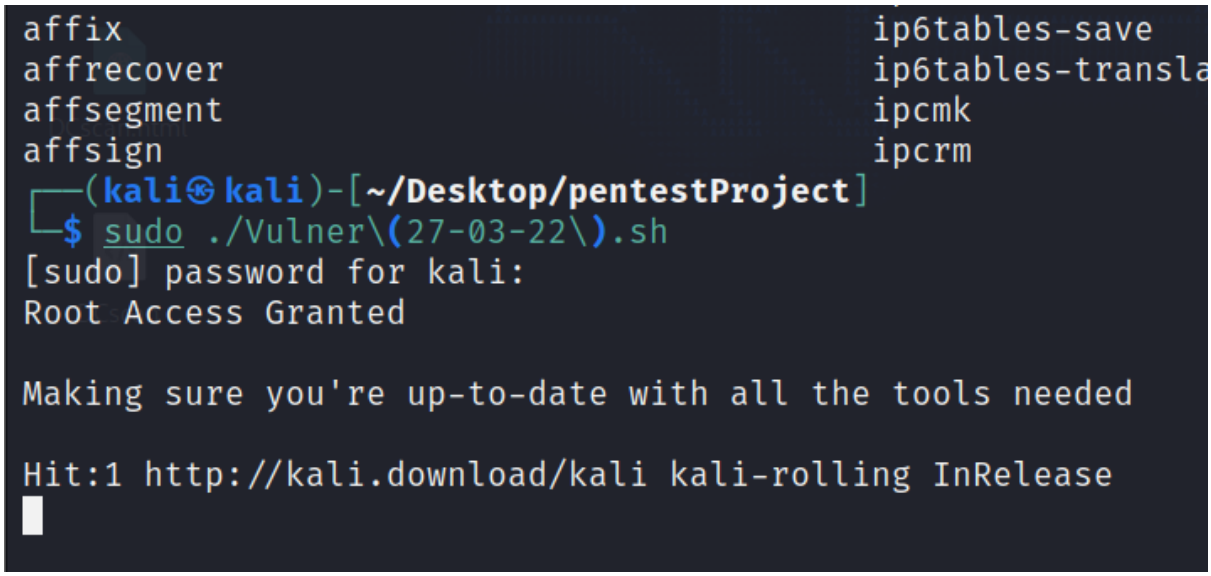
hello, this is a proof of concept for my script, network mapping for open ports, services, vulnerabilities, and weak passwords + usernames

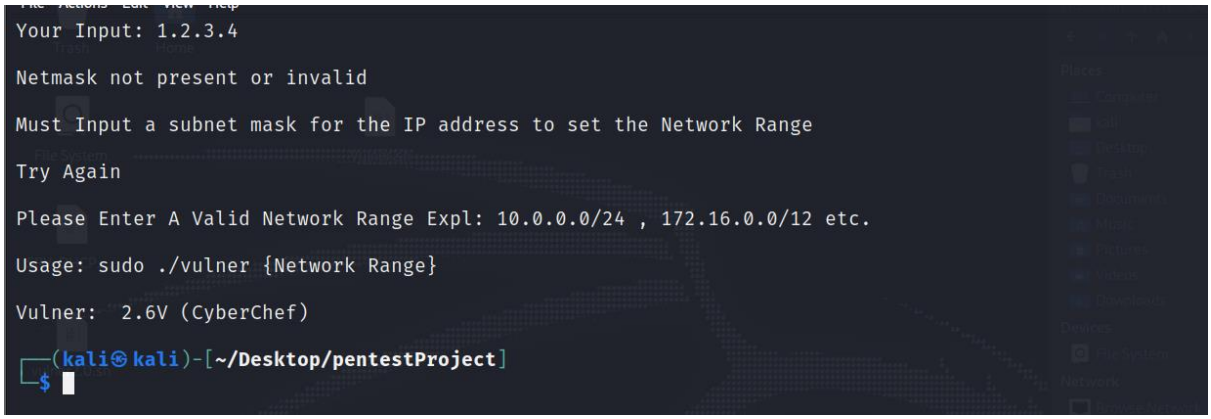
1.Starting the tool as regular user , aka not root:



2. now that you've ran the script as root ,you'll get an update, and couple of tools installed (nmap ,masscan)

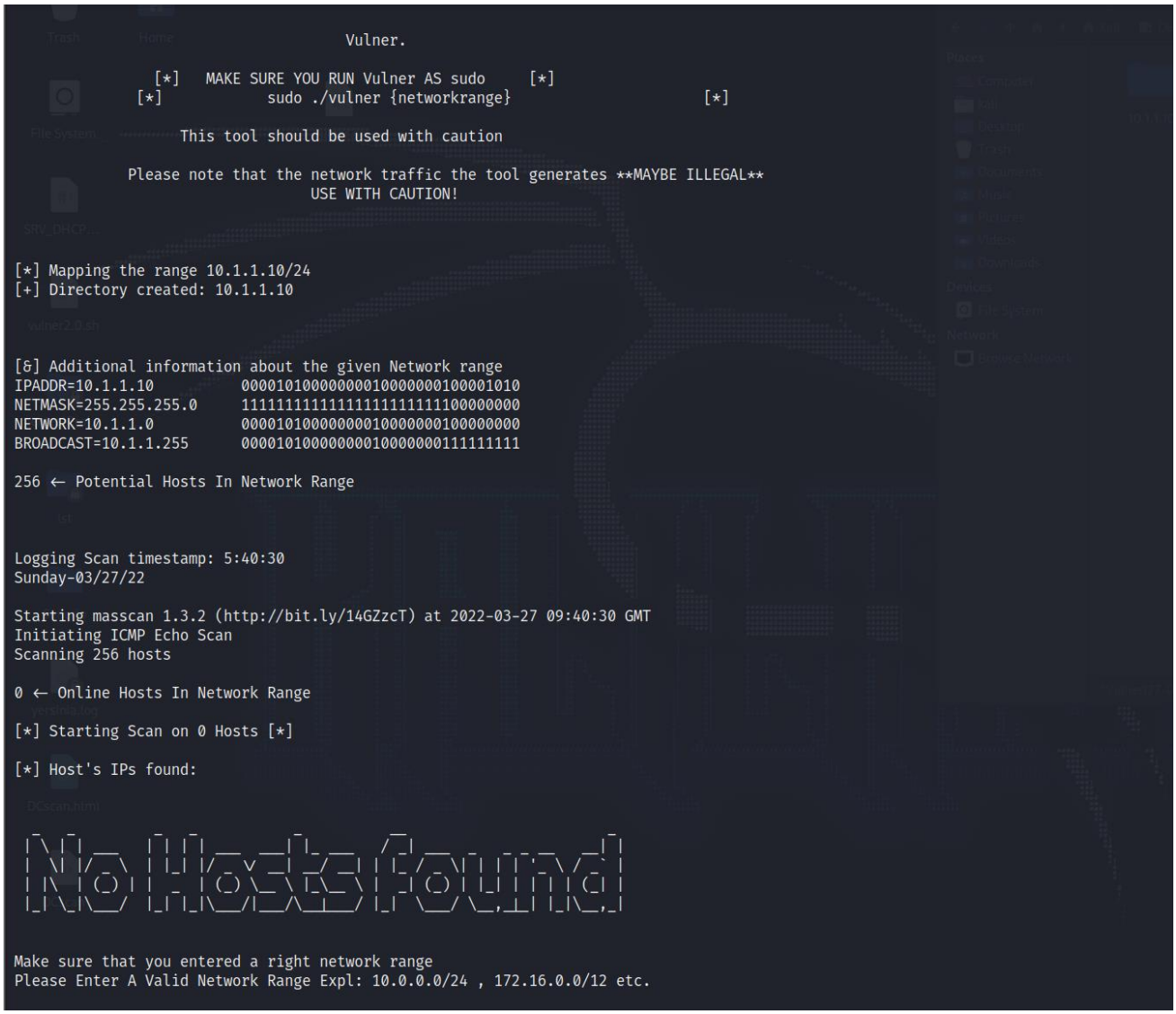


3. if the user, didn’t give the script a input of ip address , the script will show the following massage

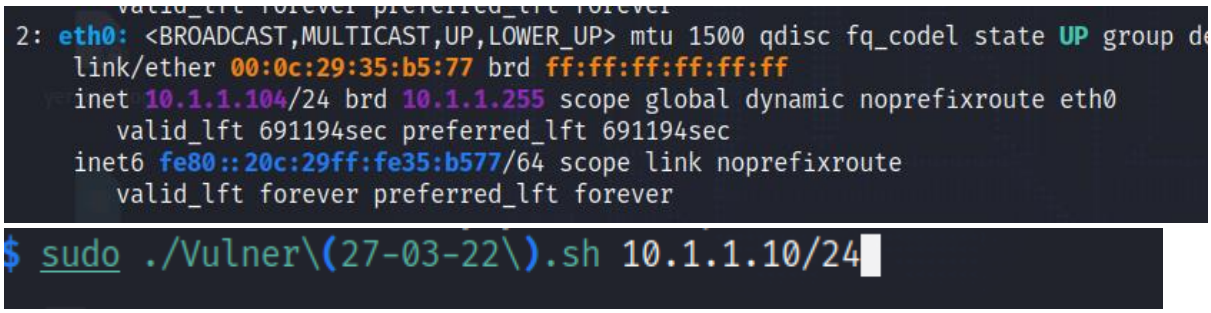


4.now we will run the script on a LAN network range.

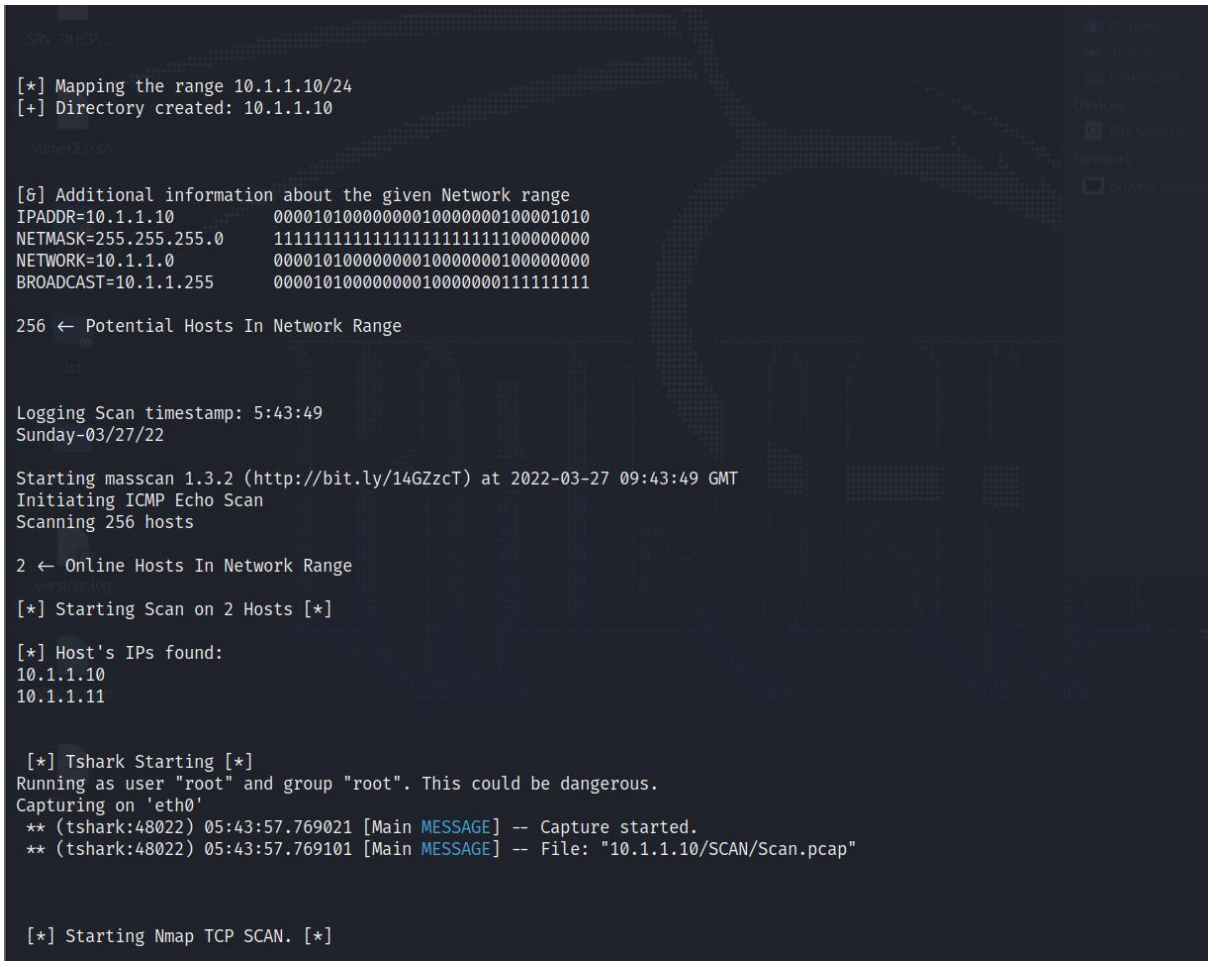
5.the script didn’t find any IP address that responded to him thouse for it didn’t follow trough with the scan.



6.now we will enter a valid ip address that we are connected to.



7.the script then run's automatically scanning the network range you input .



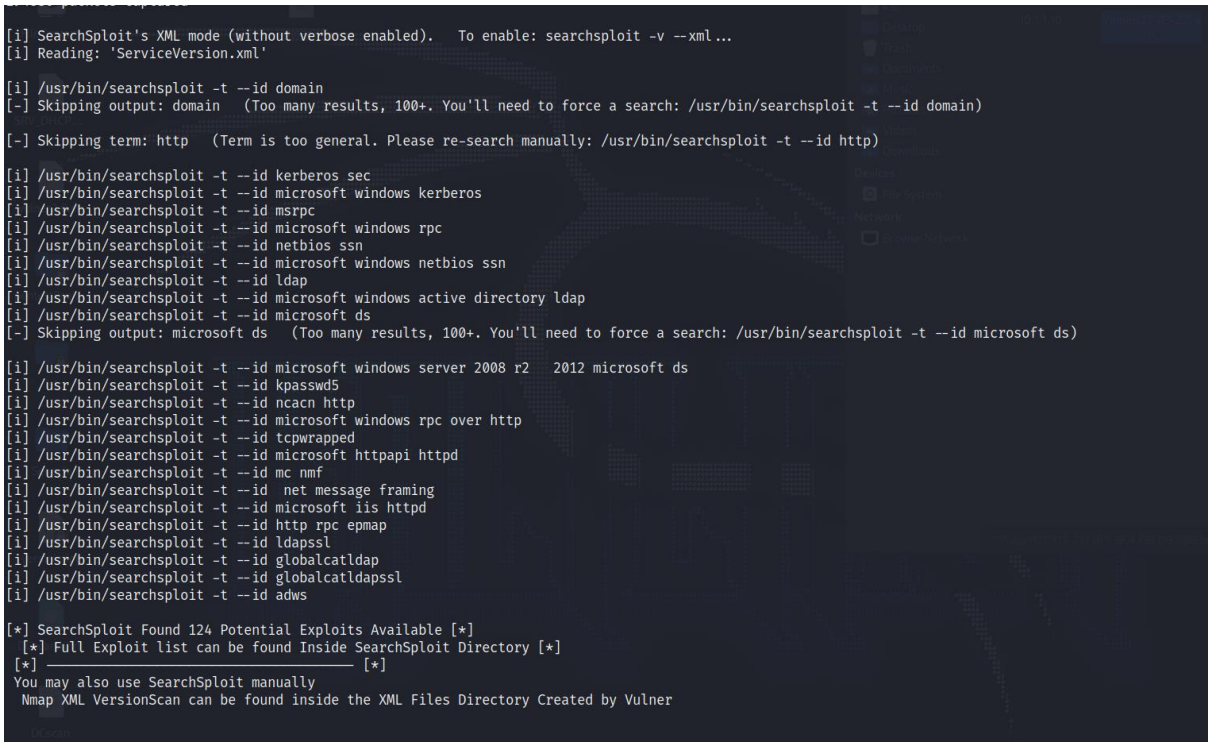
7.

```
 [*] Starting Nmap TCP SCAN. [*]

Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-27 05:44 EDT
Nmap scan report for 10.1.1.10
Host is up (0.00089s latency).
Not shown: 8337 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
MAC Address: 00:0C:29:35:DE:A1 (VMware)

Nmap scan report for 10.1.1.11
Host is up (0.00067s latency).
Not shown: 8345 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
47001/tcp open  winrm
MAC Address: 00:0C:29:CC:BD:4D (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 5.08 seconds

 [*] Starting Masscan UDP SCAN. [*]

Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-03-27 09:44:07 GMT
Initiating SYN Stealth Scan
Scanning 2 hosts [50001 ports/host]

 Open Ports Found.  Starting Nmap VersionScanner For Open Ports Found, Sit Tight
 [*] ──────────────────────────────────── [*]

  NOTICE:Nmap Version Scan is an aggressive scan which can take time to perform well.
```

8.open ports are being scanned for Versionb of the service running on that port . plus additional info such as OS , etc'

```
 Open Ports Found.  Starting Nmap VersionScanner For Open Ports Found, Sit Tight
 [*] ──────────────────────────────────── [*]

  NOTICE:Nmap Version Scan is an aggressive scan which can take time to perform well.


              Fetching OS info
 [*] ──────────────────────────────────── [*]



     NSE Is Scanning For Vulnerabilities
 [*] ──────────────────────────────────── [*]
```

9.searchsploit will that the output and suggest the user with a list of available vulnerabilities.



10. Brute force stage.

(please note that Tshark is running in the background at the ending giving the user two pcap files , one for the scanning stage and another for the brute force stage *only*

11.Lastly the user gets a log of all the info the tool gathered

```
[*]IP Addresses SCANNED [*]
_____________________________

10.1.1.10
10.1.1.11


[*] Services Found [*]
_____________________________

Nmap scan report for 10.1.1.10
53/tcp    ← PORT   SERVICE→   domain?
88/tcp    ← PORT   SERVICE→   kerberos-sec Microsoft Windows Kerberos (server time: 2022-03-27 09:44:49Z)
135/tcp   ← PORT   SERVICE→   msrpc        Microsoft Windows RPC
139/tcp   ← PORT   SERVICE→   netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   ← PORT   SERVICE→   ldap         Microsoft Windows Active Directory LDAP (Domain: tc.local, Site: Default-First-Site-Name)
445/tcp   ← PORT   SERVICE→   microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: TC)
464/tcp   ← PORT   SERVICE→   kpasswd5?
593/tcp   ← PORT   SERVICE→   ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   ← PORT   SERVICE→   tcpwrapped
3268/tcp  ← PORT   SERVICE→   ldap         Microsoft Windows Active Directory LDAP (Domain: tc.local, Site: Default-First-Site-Name)
3269/tcp  ← PORT   SERVICE→   tcpwrapped
5985/tcp  ← PORT   SERVICE→   http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  ← PORT   SERVICE→   mc-nmf       .NET Message Framing
47001/tcp ← PORT   SERVICE→   http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Nmap scan report for 10.1.1.11
80/tcp    ← PORT   SERVICE→   http             Microsoft IIS httpd 10.0
135/tcp   ← PORT   SERVICE→   msrpc            Microsoft Windows RPC
139/tcp   ← PORT   SERVICE→   netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   ← PORT   SERVICE→   microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp  ← PORT   SERVICE→   http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp ← PORT   SERVICE→   http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)



[*]PC Names.[*]
_____________________________

WINSRV-DC

[*]Operating system Found.[*]
_____________________________

 Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
[*]Vulnerabilities Nmap Found.[*]
_____________________________

# Nmap 7.92 scan initiated Sun Mar 27 05:47:10 2022 as: nmap -sT -sU -sC -T4 -iL IP_Hosts -pT:135,139,3268,3269,389,445,464,47001,53,593,5985,636,80,88,9389,U:137,53 -o
X NmapVulneFound.xml -oN NmapVulneFound.nmap
Nmap scan report
⟶10.1.1.10
Host is up (0.00024s latency).

PORT      STATE  SERVICE
53/tcp    open   domain
80/tcp    closed http
88/tcp    open   kerberos-sec
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
|   hostname: WINSRV-DC
|   interfaces:
|_    10.1.1.10
MAC Address: 00:0C:29:35:DE:A1 (VMware)

Host script results:
|_clock-skew: mean: -59m59s, deviation: 1h43m55s, median: 0s
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
|   Computer name: WINSRV-DC
|   NetBIOS computer name: WINSRV-DC\x00
|   Domain name: tc.local
|   Forest name: tc.local
|   FQDN: WINSRV-DC.tc.local
|_  System time: 2022-03-27T12:47:13+03:00
|_nbstat: NetBIOS name: WINSRV-DC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:35:de:a1 (VMware)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-03-27T09:47:13
|_  start_date: 2022-03-27T06:25:43
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required

Nmap scan report
⟶10.1.1.11
Host is up (0.00042s latency).

PORT      STATE         SERVICE
53/tcp    closed        domain
80/tcp    open          http
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp    closed        kerberos-sec
135/tcp   open          msrpc
139/tcp   open          netbios-ssn
389/tcp   closed        ldap
445/tcp   open          microsoft-ds
464/tcp   closed        kpasswd5
593/tcp   closed        http-rpc-epmap
636/tcp   closed        ldapssl
3268/tcp  closed        globalcatLDAP
3269/tcp  closed        globalcatLDAPssl
5985/tcp  open          wsman
9389/tcp  closed        adws
47001/tcp open          winrm
53/udp    open|filtered domain
137/udp   open          netbios-ns
| nbns-interfaces:
|   hostname: WINSRV-RTR
|   interfaces:
|     10.10.250.136
|_    10.1.1.11
MAC Address: 00:0C:29:CC:BD:4D (VMware)

Host script results:
```

```
 [*] OSs Found in the Network Range[*]
 ──────────────────────────────────────

↓Nmap scan report for 10.1.1.10
MAC Address: 00:0C:29:35:DE:A1 (VMware)
OS details: Microsoft Windows Server 2016 build 10586 - 14393

↓Nmap scan report for 10.1.1.11
MAC Address: 00:0C:29:CC:BD:4D (VMware)

[*]Valid credentials Found [*]
 ──────────────────────────────────────
Nmap scan report for 10.1.1.10
--
47001/tcp open   winrm
|_  guest:<blank> ⇒ Valid credentials, account disabled
Nmap scan report for 10.1.1.11
--
47001/tcp open   winrm
|_  guest:<blank> ⇒ Valid credentials, account disabled


[*] TOP 3 Backdoor Exploits Available [*]
 ──────────────────────────────────────

[*] TOP 3 Command Execution Exploits Available [*]
 ──────────────────────────────────────
  Exploit: PineApp Mail-SeCure - 'ldapsyncnow.php' Arbitrary Command Execution (Metasploit)

[*] TOP 3 Remote Code Execution Exploits Available [*]
 ──────────────────────────────────────
  Exploit: IBM Lotus Domino LDAP - Bind Request Remote Code Execution
  Exploit: Novell NetIQ Privileged User Manager 2.3.1 - 'ldapagnt.dll' ldapagnt_eval() Perl Code Evaluation Remote Code Execution
  Exploit: NetIQ Privileged User Manager 2.3.1 - 'ldapagnt_eval()' Perl Remote Code Execution (Metasploit)

scan ended at:  5:43:49
Sunday-03/27/22

 Making Seder  hehe
  organizing log directories'
  Converting XML Files to HTML Readable format
 [*] ──────────────────────────────────────── [*]


DONE!! Thanks :)
```