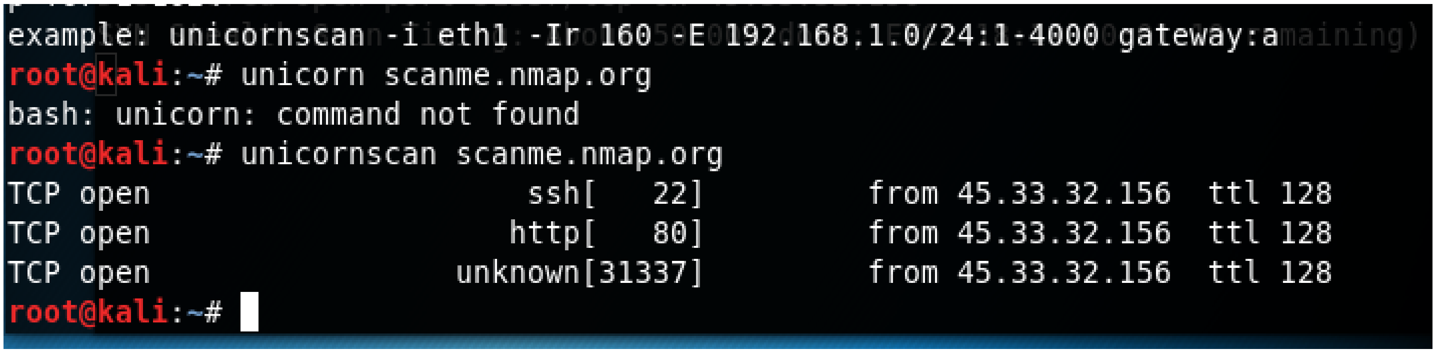
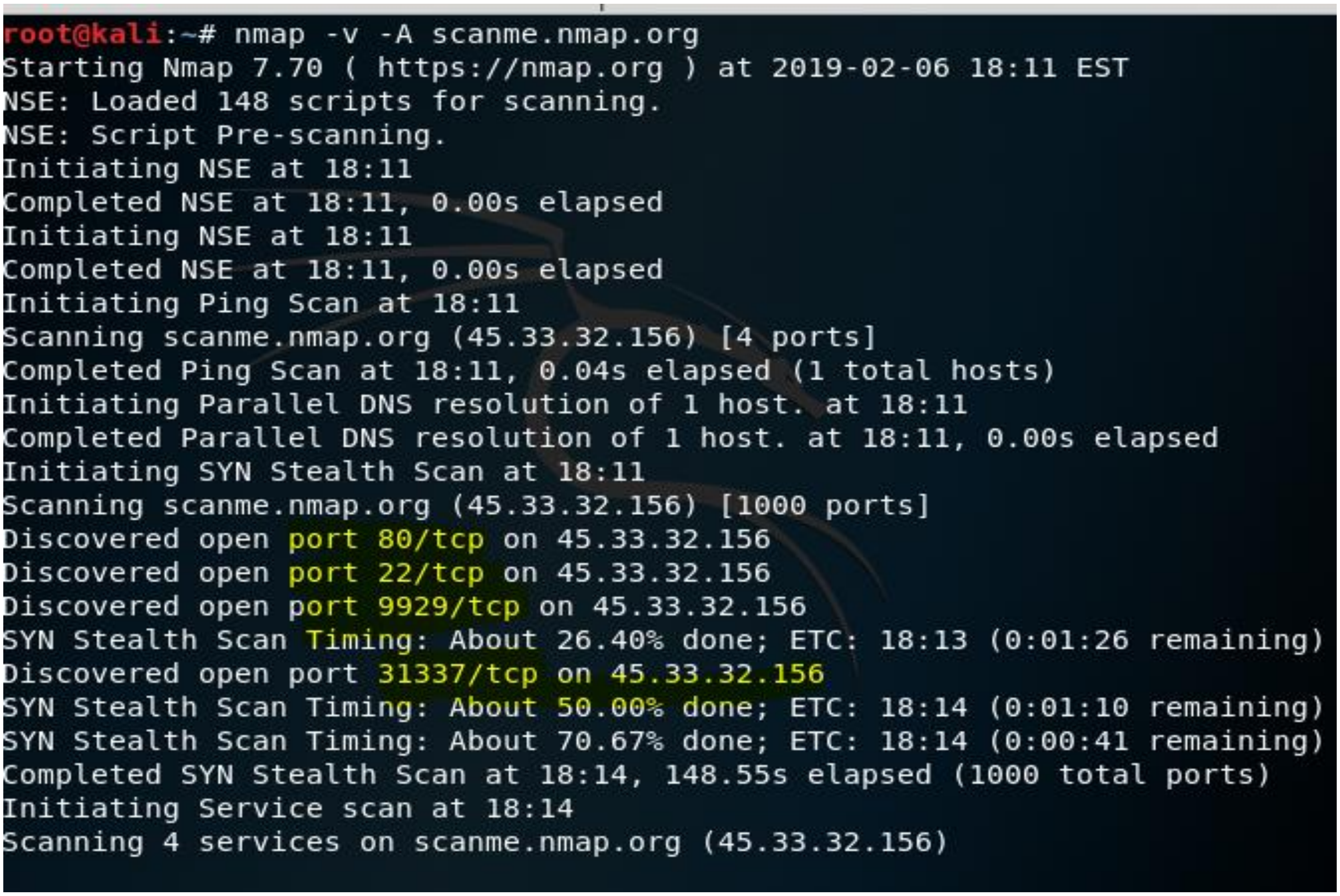
Task 1:

Below are the open ports on *scanme.nmap.org*. Unicorn was the port used to scan the website. Unicorn provides TTL of the operating system which can be further search online to identify the operating system.

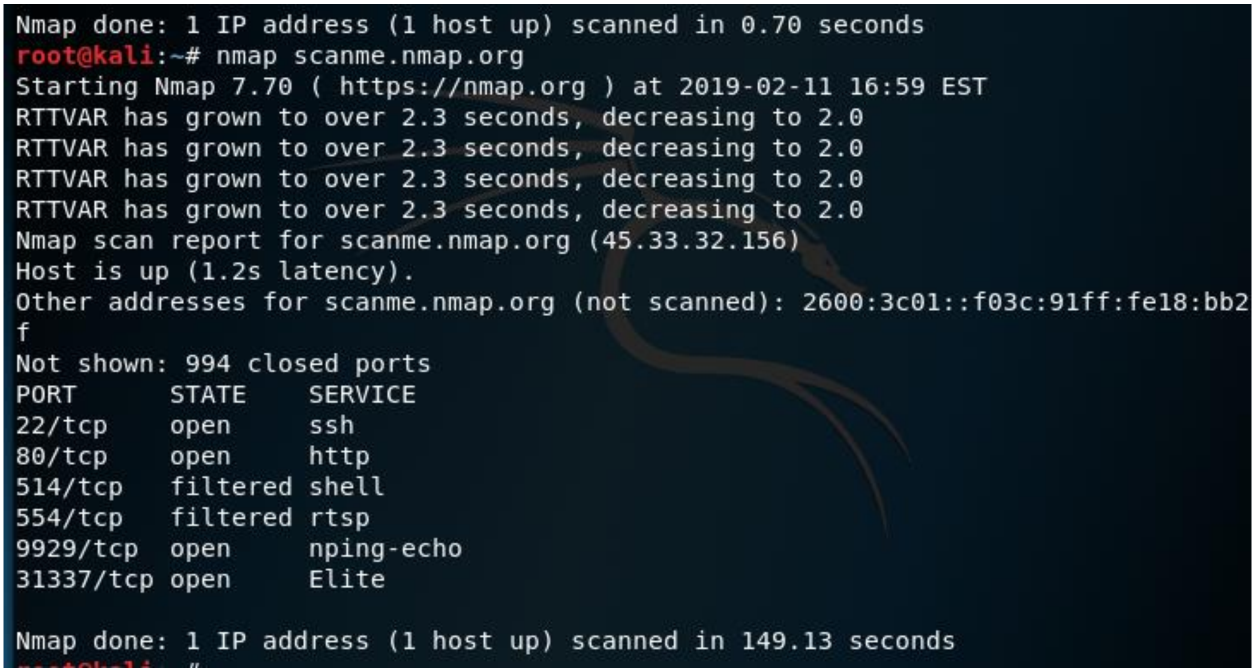


```
example: unicornscan -i eth1 -Ir 160 -E 192.168.1.0/24:1-4000 gateway:a
root@kali:~# unicorn scanme.nmap.org
bash: unicorn: command not found
root@kali:~# unicornscan scanme.nmap.org
TCP open                     ssh[   22]         from 45.33.32.156  ttl 128
TCP open                    http[   80]         from 45.33.32.156  ttl 128
TCP open                 unknown[31337]         from 45.33.32.156  ttl 128
root@kali:~#
```

Below is the scan output using NMAP scanner. It provides more details about the open port and services running on it. Moreover, advanced queries can confirm the name of operating system being used.



```
root@kali:~# nmap -v -A scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-06 18:11 EST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:11
Completed NSE at 18:11, 0.00s elapsed
Initiating NSE at 18:11
Completed NSE at 18:11, 0.00s elapsed
Initiating Ping Scan at 18:11
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 18:11, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:11
Completed Parallel DNS resolution of 1 host. at 18:11, 0.00s elapsed
Initiating SYN Stealth Scan at 18:11
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
SYN Stealth Scan Timing: About 26.40% done; ETC: 18:13 (0:01:26 remaining)
Discovered open port 31337/tcp on 45.33.32.156
SYN Stealth Scan Timing: About 50.00% done; ETC: 18:14 (0:01:10 remaining)
SYN Stealth Scan Timing: About 70.67% done; ETC: 18:14 (0:00:41 remaining)
Completed SYN Stealth Scan at 18:14, 148.55s elapsed (1000 total ports)
Initiating Service scan at 18:14
Scanning 4 services on scanme.nmap.org (45.33.32.156)
```



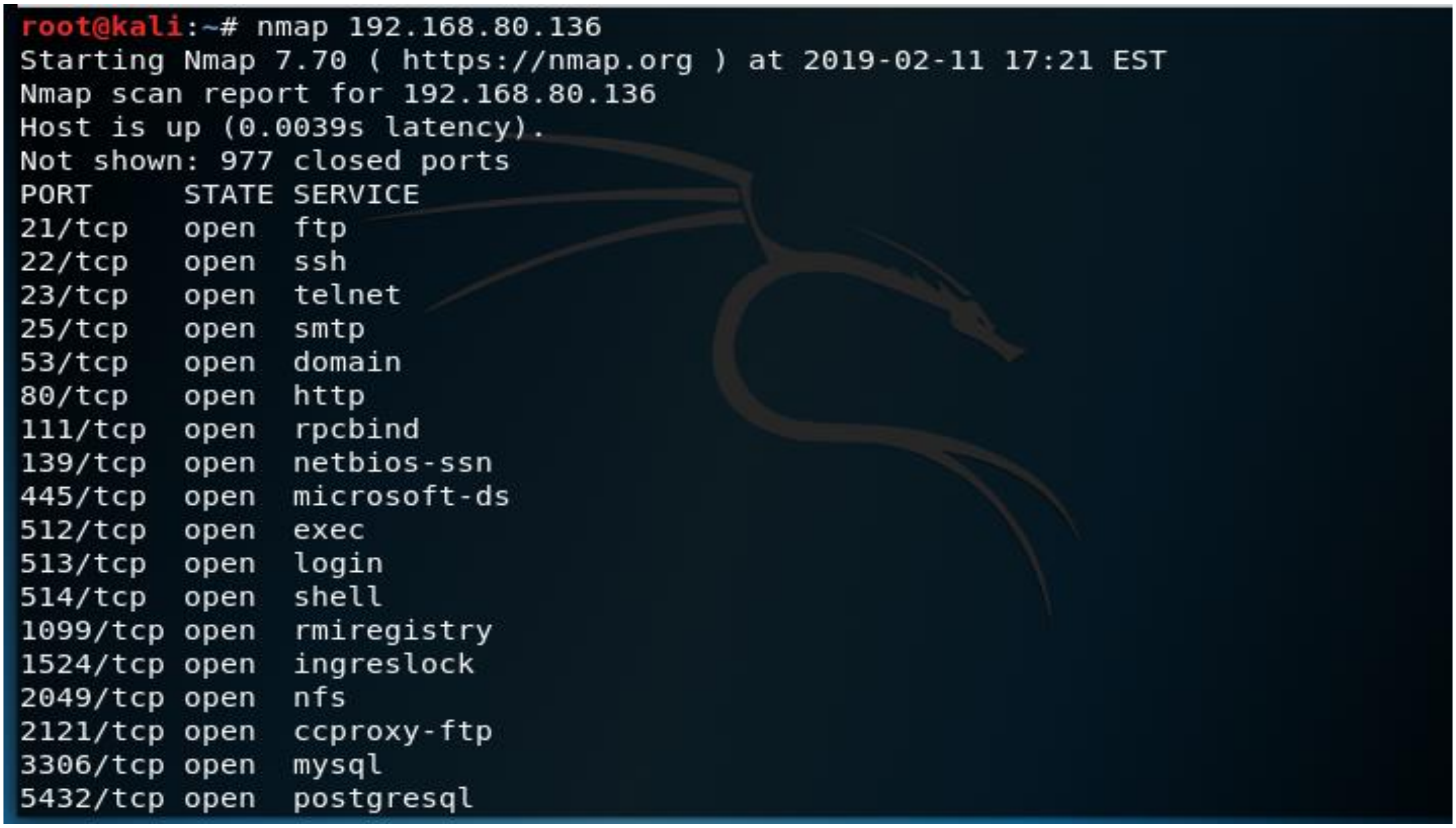
```
Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
root@kali:~# nmap scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-11 16:59 EST
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (1.2s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 994 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
514/tcp   filtered shell
554/tcp   filtered rtsp
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 149.13 seconds
```

Comparing both the scans, I find nmap better than unicorn as number of ports open found in nmap scan were more than the ports find in unicron scan. Further, former scan was able to determine operating system as well.

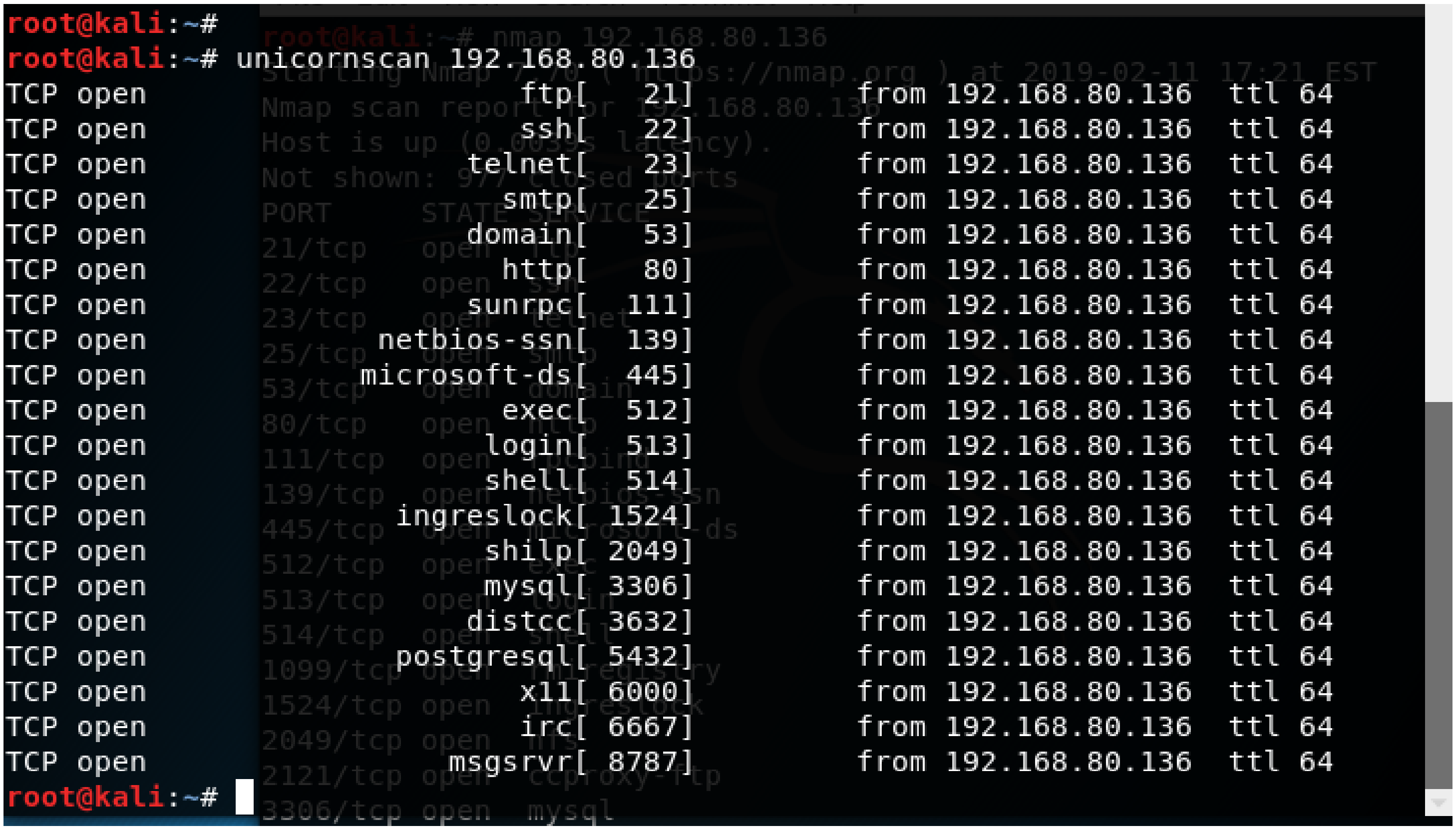
Task 2:

(a) Scanning open ports using NMAP:



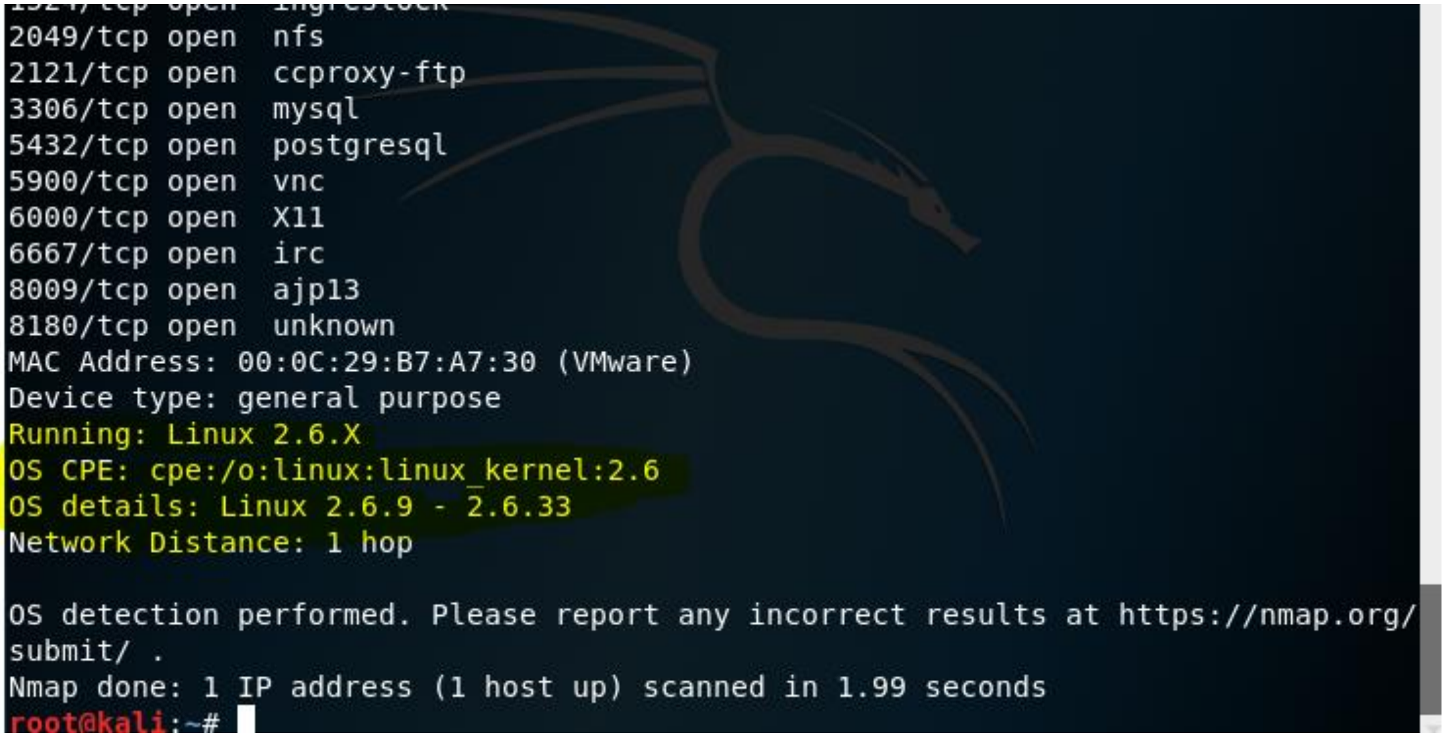
```
root@kali:~# nmap 192.168.80.136
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-11 17:21 EST
Nmap scan report for 192.168.80.136
Host is up (0.0039s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
```

Scanning open ports using unicorn:



```
root@kali:~#
root@kali:~# unicornscan 192.168.80.136
TCP open                     ftp[   21]         from 192.168.80.136  ttl 64
TCP open                     ssh[   22]         from 192.168.80.136  ttl 64
TCP open                  telnet[   23]         from 192.168.80.136  ttl 64
TCP open                    smtp[   25]         from 192.168.80.136  ttl 64
TCP open                  domain[   53]         from 192.168.80.136  ttl 64
TCP open                    http[   80]         from 192.168.80.136  ttl 64
TCP open                  sunrpc[  111]         from 192.168.80.136  ttl 64
TCP open             netbios-ssn[  139]         from 192.168.80.136  ttl 64
TCP open            microsoft-ds[  445]         from 192.168.80.136  ttl 64
TCP open                    exec[  512]         from 192.168.80.136  ttl 64
TCP open                   login[  513]         from 192.168.80.136  ttl 64
TCP open                   shell[  514]         from 192.168.80.136  ttl 64
TCP open              ingreslock[ 1524]         from 192.168.80.136  ttl 64
TCP open                   shilp[ 2049]         from 192.168.80.136  ttl 64
TCP open                   mysql[ 3306]         from 192.168.80.136  ttl 64
TCP open                 distcc[ 3632]         from 192.168.80.136  ttl 64
TCP open              postgresql[ 5432]         from 192.168.80.136  ttl 64
TCP open                     x11[ 6000]         from 192.168.80.136  ttl 64
TCP open                     irc[ 6667]         from 192.168.80.136  ttl 64
TCP open                 msgsrvr[ 8787]         from 192.168.80.136  ttl 64
root@kali:~#
```

(b) Operating System of Metasploitable2:

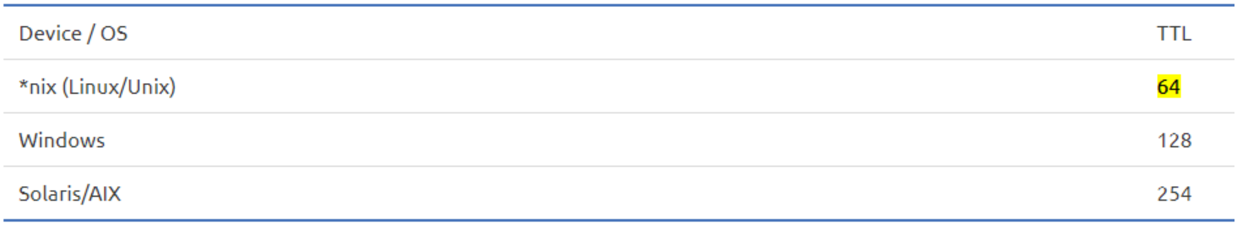


```
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:B7:A7:30 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.99 seconds
root@kali:~#
```

Unicorn: To find the possible operating system, TTL can be used. For given operating system, TTl was 64 making a prediction that operating system might be Linux/Unix

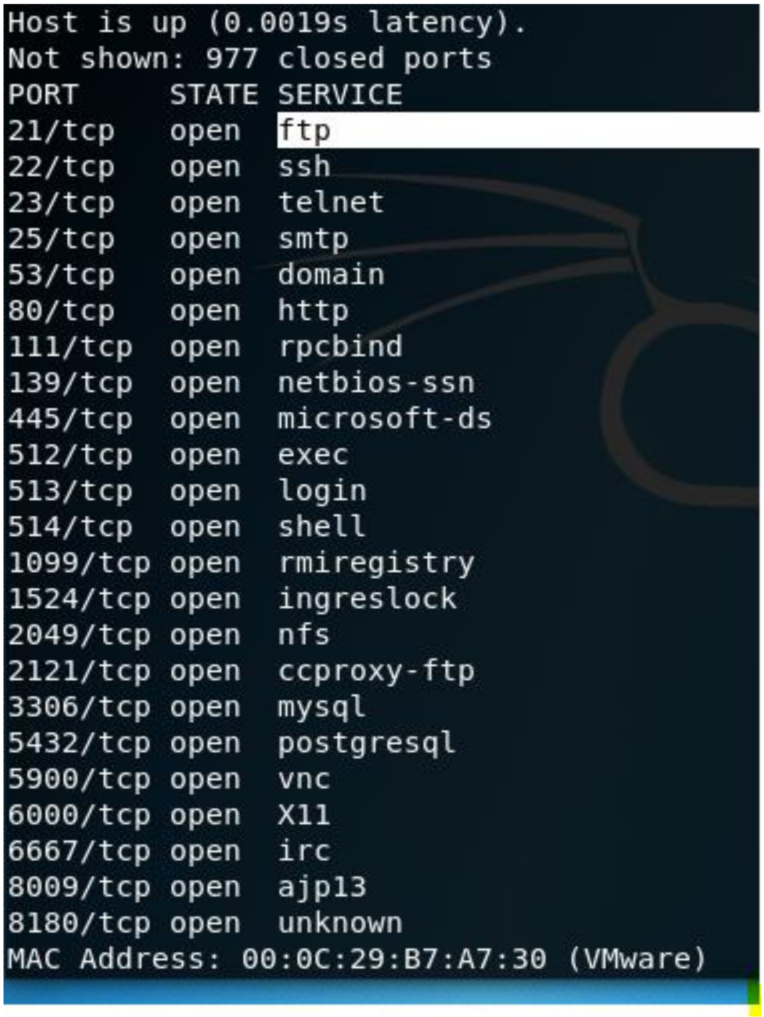
http://subinsb.com/default-device-ttl-values/



Device / OS	TTL
*nix (Linux/Unix)	64
Windows	128
Solaris/AIX	254

Task 3:

Below are the services running on open ports of Metasploitable2:



```
Host is up (0.0019s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:B7:A7:30 (VMware)
```

Below are the vunerablities on the service running on www.lkouniv.ac.in:

Service Name	**description**	**how it can be exploited**	**impact**	**how to deal with the vulnerability**	Reference
FTP	CVE-2018-13306	It can be exploited when TOTOLINK A3002RU is used. It is a wirless router with serious security lacking features. Hackers can execute command by atttaching script over post method	Allows unauthorized disclosure of information Allows unauthorized modification Allows disruption of service	Using a filter to check post request	1
	CVE-2018-18861	CVE-2018-18861 allows execution of code via APPE command remotely	Allows unauthorized disclosure of information Allows disruption of service	avoid standard library functions that are not bounds-checked, such as gets, scanf and strcpy.	2
	CVE-2018-17440	In D-link central wifi port 9000 runs FTP server which has hardcoded credentials. Attacker can execute PHP code in root directory and accessing data via request object	Allows unauthorized modification Allows disruption of service	Installing patch given by company	3
ssh	CVE-2019-3463	insufficient care of the arguements passed through rsync breached rssh	resulted in executing of ansurd commmands	rsync arguements have to be made compliant with rssh	4

	CVE-2019-6110	it displyed arbitary output for stderr from server	Ouput can be distorted	openssh 7.9 needs to be improved	4
	CVE-2018-5413	Escaltated user privilege	Allows unauthorized modification	imperva secure sphere needs to be upgraded above v13	4
telnet	CVE-2018-15390	FTP inspection engine of Cisco Firepower Threat Defense (FTD) allowed hacker to redirect high traffic resulting in in denial of service condition. Software failed to release spinlock in case of high traffic(low memory) affecting the availability of system.		Correcting the code so that thread waiting for resource can access other resource instead of waiting removing spinlock	5
	CVE-2018-20764	Buffer flow vunerability in HelpSystems tcpcrypt on Linux. Since setuid is being used, user privilage can be escalated by changing file permission.		replace the affected object with an alternative product.	6
	CVE-2018-19069	Some of Foscam C2 devices & Opticam i5 devices gets authorized by root user with a password of toor.	Allows unauthorized disclosure of information	Updating the username and password from default	4
smtp	CVE-2014-4782	remote users were allowed to identify server credentials via vector	Allows unauthorized disclosure of information	IBM Xforce needs to be upgraded	4
	CVE-2018-10814	cleartext password storage was used for SMTP credentials	unauthorised disclosure of information	Synametrics SynaMan 4.0 build 1488 has to be dispatched	4
	CVE-2018-6789	buffer overflow which made code to execute remotely	integrity was compromised	base64d function has to be improved through patch for SMTP listener	4
domain	CVE-2018-1340	on client side Apache guacamole used cookie without 'secure' flag	Can allow hacker to intercept user's session by accessing unencrypted http requrest	Enable secure flag in cookie	4
	CVE-2018-0678	in BN-SDWBP3 firmware version 1.0.9 buffer overflow can occur by user in the same network	Can allow hacker to run unauthorized code	Improving code that considers memory overflow exceptions	4
	CVE-2018-6173	URL formatter of Google chrome handled confusable characters incorrectly.	Attacker can pretend to be companies employee by using domain spoofing	Upgrading to a version greater than 68.0.3440.75	4
http	CVE-2018-20779	Traq 3.7.1 SQL injection. it affected some functionality of file tickets?search	Can compromise vailability and integrity	affected object needs to be replaced by alternative product	4
	CVE-2018-20780	fake admin accounts can be created through Traq3.7.1 for admin/users/new CSRF	hacker can control user actions	traq3.7.1 need to be patched	4
	CVE-2019-7700	wasm::WasmBinaryBuilder::visitCall : haepbased buffer overread lead to denial of services	Avaiablitiy might be effected	Binaryen 1.38.22 needed upgrades	4
rpcbind	CVE-2017-8779	For XDR strings, rpcbind through 0.2.4 don't consider memory allocation	hacker can cause denial of service by consuming all memory by sending XDR string via rpcBOMB	Creating services to detect unusual memory consumption	4
	CVE-1999-0190	Solaris rpcbind can be used to execute unauthorzied files by gaining root access	There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable	Add firewalld rules the server and restrict access to specific n/w	7

	CVE-2005-2132	System can fail by sending multiple post request to RPC portmapper in SCO unixware. he RPC portmapper (portmap(8)) is a server that converts RPC program numbers into TCP/IP (or UDP/IP) protocol port numbers.	Denial of service	Disabling portmapper in case of compromise. Enabling firewalld and iptables for ubuntu	8
netbois-ssn		folder sharing can be done on port 135 139 445	data compromise	applying filter on ports with firewall	9
microsoft-ds	CVE-2002-0597	Microsoft Windows 2000 allowed denial of service at port 445	denial of service	Microsoft Windows 2000 needs to be updated	4
	CVE-2002-0597	Lawman service on windows 2000 allowed attckers to cause denial of service at port 445	services got disrupted	Microsoft Windows 2000 needs to be updated	4
exec	CVE-2018-20773	Frog CMS 0.9.5 allows PHP code execution by visiting admin/?/page/edit/1 and inserting additional <?php lines	Availability and integrity was compromised	Frog CMS 0.9.5 needs to be patched	4
	CVE-2018-1352	Fortinet FortiOS 5.6.0 allowed hackers to execute unauthorised code through ssh	unauthorised modification	Fortinet FortiOS 5.6.0 needs to be patched	4
	CVE-2018-7814	Stack-based Buffer Overflow (CWE-121) vulnerability in Eurotherm which caused remote code execution	unauthorised modification	Gold Build 683.0 needs revision	4
login	CVE-2019-3825	in gdm before 3.31.4, lock screen could be bypassed by enabling timed login and waiting for timer to expire	Hacker can access to logged in user's session	Disable timed login, or using 2FA	4
	CVE-2018-4056	in the administrator web portal function of coTURN prior to version 4.5.0.9, specially crafted username can cause SQL injection	Can give access to admin web protal by bypassing authentication	Don't create dynamic SQL query directly with user inputted fields	4
	CVE-2018-16201	Toshiba Home gateway HEM-GW16A 1.2.9 uses hard coded credentials	Attacker on same network can login to admin screen	Never harcode username and password	4
shell	CVE-2019-7731	MyWebSQL 3.7 has a remote code execution (RCE) vulnerability after an attacker writes shell code into the database, and executes the Backup Database function with a .php filename for the backup's archive file.	data compromise	Checking for unauthrozied php file execution	4
	CVE-2019-7692	install/install.php in CIM 0.9.3 allows remote attackers to execute arbitrary PHP code via a crafted prefix value because of configuration file mishandling in the N=83 case	creates public php folder	Check for the bug	4
	CVE-2019-7632	Networker 220 devices allow Authenticated Remote OS Command Injection, as demonstrated by shell metacharacters in the support/mtusize.php mtu_size parameter.	unauthorized access to device	Enabling hash and salt	4
ingreslock		payment is transmitted unencrypted	hacking during transmission	Disable rlogin service and use ssh instead	10
		Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.	data compromise	Disable rlogin service and use ssh instead	11
		A backdoor is installed on the remote host	data compromise	Disable rlogin service and use ssh instead	12
nfs	CVE-2018-5498	Clustered Data ONTAP versions 9.0 through 9.4 are susceptible to a vulnerability which allows remote authenticated attackers to cause a Denial of Service (DoS) in NFS and SMB environments.	Denial of service		4
	CVE-2018-16884	A flaw was found in the Linux kernel's NFS41+ subsystem. NFS41+ shares mounted in different network namespaces at the same time can make bc_svc_process() use wrong back-channel IDs and cause a use-after-free vulnerability.	kernel memory consumption		4

	CVE-2018-20029	uninitialized memory can be read in The nxfs.sys driver in the DokanFS library 0.6.0 in NoMachine before 6.4.6 on Windows 10	Denial of service	Required windows path	4
ccproxy-ftp	CVE-2008-6415	Buffer overflow in YoungZSoft CCProxy 6.5 might allow remote attackers to execute arbitrary code via a CONNECTION request with a long hostname	System integrity loss	Additional condition to consider long hostname	4
	CVE-2004-2416	Buffer overflow in the logging component of CCProxy allows remote attackers to execute arbitrary code via a long HTTP GET request.		additional condition to check long http get request	4
	CVE-2004-2685	Buffer overflow in YoungZSoft CCProxy 6.2 and earlier allows remote attackers to execute arbitrary code via a long address in a ping (p) command to the Telnet proxy service	Unauthrozied data access	addressing long ping command	4
mysql	CVE-2019-6799	An attacker can read files on the server that the web user's can access with the use of a malicious MySQL Server, when the AllowArbitraryServer Configuration is set true	Confidential information might leak	Filters to determin SQLinjection	4
	CVE-2019-2539	Allowed high privileged attacker with network access to compromise the SQL Server using easily exploitable vulnerabilities.	Can lead to ahng or crash of the server.	Filters to determin SQLinjection	4
	CVE-2019-2535	Allowed high privileged attackers with access to SQL Server to compromise SQL Server using exploitable vulnerabilities.	Lead to hang or crash of SQL Server.	Filters to determin SQLinjection	4
distcc	CVE-2005-1461	Attackers can cause denial of service and execution of random codes using buffer overflow	denial of service	use fuction that consider overflow	4
	CVE-2004-2687	Allowe attackers to run commands on restricted server port without legit checks	Lead to hang or crash of SQL Server.	Configuring security	4
	CVE-2004-0601	Allow attackers to bypass IP restrictions , when they are not interpreted correctly on 64 bit system	Data loss	Additional functionality to check 64 bit	4
postgresql	CVE-2017-18359	It allows attacker to create a denial of service error due to abnormal termination of the server caused by query	denial of service	System to filter unusal query/data fetching	4
	CVE-2018-16203	Unspecified vectors could be used by attackers to get the administrative privileges of the database by bypassing the login	System might be compromised	Tracking unsecified vector	4
	CVE-2018-16850	Were vulnerable to SQL injection which can allow random SQL statements to run that had superuser privileges	System might be compromised	No sql query with data directly coming from user	4
x11	CVE-2018-14665	It allowed users to escalate their priveliges using a physical console and allow them to add codes with root privileges	Confidential information might leak	Securing root privileges	4
	CVE-2018-14600	It leads to a wrong interpretation of a variable thus resulting in out-of-bounds error causing remote code execution	denial of service	Adding condition to consider wrong variable	4
	CVE-2018-14599	Server responses can cause off-by-one error leading to DOS or unspecified other impact.	Impact not measurable	Adding required conditions	4
irc	CVE-2019-1660	A vulnerability in the SOAP of TMS can provide unauthorized access to a remote attacker. Vulnerability is due to the lack of proper access and authentication controls on the TMS software.The attacker can get access to the system management tools	services got disrupted	Fixing SOAP message	4
	CVE-2018-18363	This can lead to a bypass exploit in Norton Lock App which wil allow the user to circumvent the app and prevent it from locking ,thereby allowing him/her an access into the device	Data loss	Lock releasing on time	4
	CVE-2019-0243	Sometimes it will not perform the required authentication checks for a legit user there by giving away privileges	denial of service	Checking user privileges	4
ajp	CVE-2018-1048	Allowed the slash characters in the url to cause path traversal and disclosure of random files	Data leak	correcting controller to consider /	4
	CVE-2016-1555	Allowed attackets to execute random commands.	unauthrozied command execution		4
	CVE-2016-6652	When we have a repository with @Query annotation , and we do an SQL injection, it allowed attackers to execute random JPQL commands.	Data compromise	Filters to determin SQLinjection	4

References:

1 https://blog.securityevaluators.com/new-vulnerabilities-in-totolink-a3002ru-d6f42a081154

2https://www.veracode.com/security/buffer-overflow

3 https://securityadvisories.dlink.com/announcement/publication.aspx?name=SAP10092

4 https://nvd.nist.gov

5 https://www.tenable.com/plugins/nessus/117917

6 https://www.mag-securs.com/alertes/artmid/1894/articleid/28168/helpsystems-tcpcrypt-up-to-671-on-linux-memory-corruption-cve-2018-20764.aspx

7 https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-securing_services#sec-Securing_rpcbind

8 https://www.transip.eu/knowledgebase/entry/334-securing-the-rpc-portmapper-service/

9 https://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/

10 https://pentest-tools.com/public/sample-reports/openvas-scan-sample-report.pdf

11 https://pentest-tools.com/public/sample-reports/openvas-scan-sample-report.pdf

12 https://pentest-tools.com/public/sample-reports/openvas-scan-sample-report.pdf

Task 4:

IP Address of www.lkouniv.ac.in: 182.18.166.206
Administrative Contact:

inetnum: 182.18.128.0 - 182.18.191.255 netname: PEL-IN descr: Pioneer Elabs Ltd. country: IN admin-c: PSR1-AP tech-c: II45-AP mnt-by: MAINT-IN-IRINN mnt-lower: MAINT-IN-IPAPELABS mnt-routes: MAINT-IN-IPAPELABS mnt-irt: IRT-PEL-IN status: ALLOCATED PORTABLE last-modified: 2013-07-04T23:00:30Z source: APNIC	irt: IRT-PEL-IN address: Pioneer Elabs Ltd. address: #3D, Samrat Commercial Complex, address: Saifabad, hyderabad - 500004 address: Andra Pradesh, India e-mail: abuse{!}ctrls.in abuse-mailbox: abuse{!}ctrls.in admin-c: PSR1-AP tech-c: II45-AP auth: # Filtered mnt-by: MAINT-IN-IPAPELABS last-modified: 2013-08-19T06:18:30Z source: APNIC
person: IP Administrator IP Administrator Pioneer Elabs nic-hdl: II45-AP e-mail: ip.admin{!}pioneerelabs.com address: Ground Floor, Pioneer Towers, Plot No.16, address: APIIC Software Units Layout, address: Madhapur, address: Hyderabad - 500081 phone: +91-404-2030700 fax-no: +91-402-3116055 country: IN mnt-by: MAINT-IN-IPAPELABS last-modified: 2012-11-30T05:10:56Z source: APNIC	person: Pinnapureddy Sridhar Reddy address: CtrlS Datacenters Ltd. address: 7th Floor, Pioneer Towers, address: Plot No.16, APIIC Software Units Layout, address: Madhapur, address: Hyderabad - 500081 country: IN phone: +91-40-42030700 fax-no: +91-40-23116055 e-mail: admin{!}ctrls.in nic-hdl: PSR1-AP mnt-by: MAINT-IN-PSREDDY last-modified: 2011-11-29T04:13:23Z source: APNIC

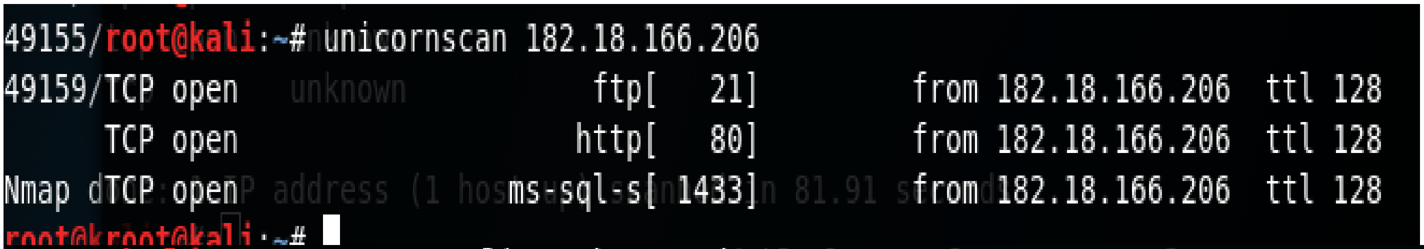
Source: https://www.abuseipdb.com/whois/202.65.154.101

Website used to find IP: https://ipinfo.info/html/ip_checker.php

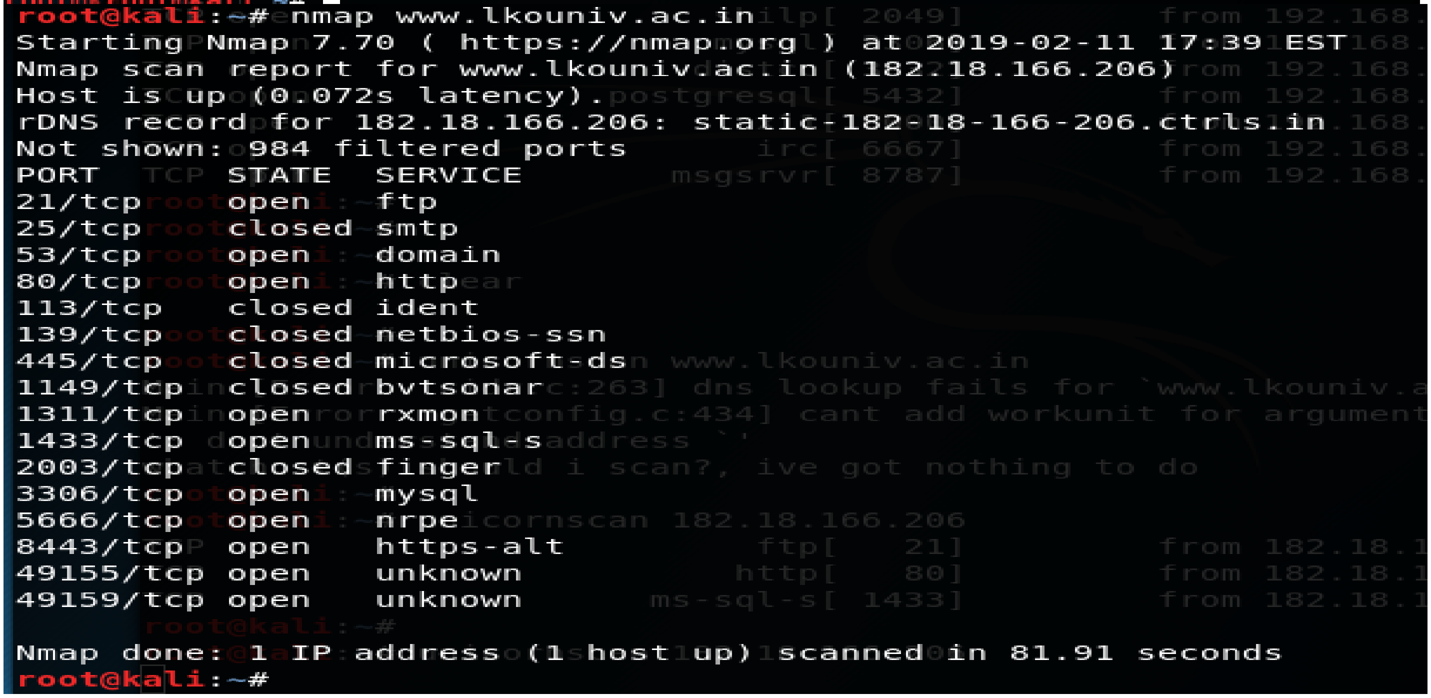
Hacker might use this information for phishing attack. Hackers can bring down the system for small time by sending high traffic and then calling the University to fetch important sensitive information.
Other type of attack can be on the website provider. Hackers can scan the port, get relevant services and come up with a story that makes IT team to believe the call/mail is from university

Task 5:

Open ports were scanned using unicornscan and nmap. Below are the open ports. Since TTL is 128, operating system can be windows server which is further strengthened by namp scan.

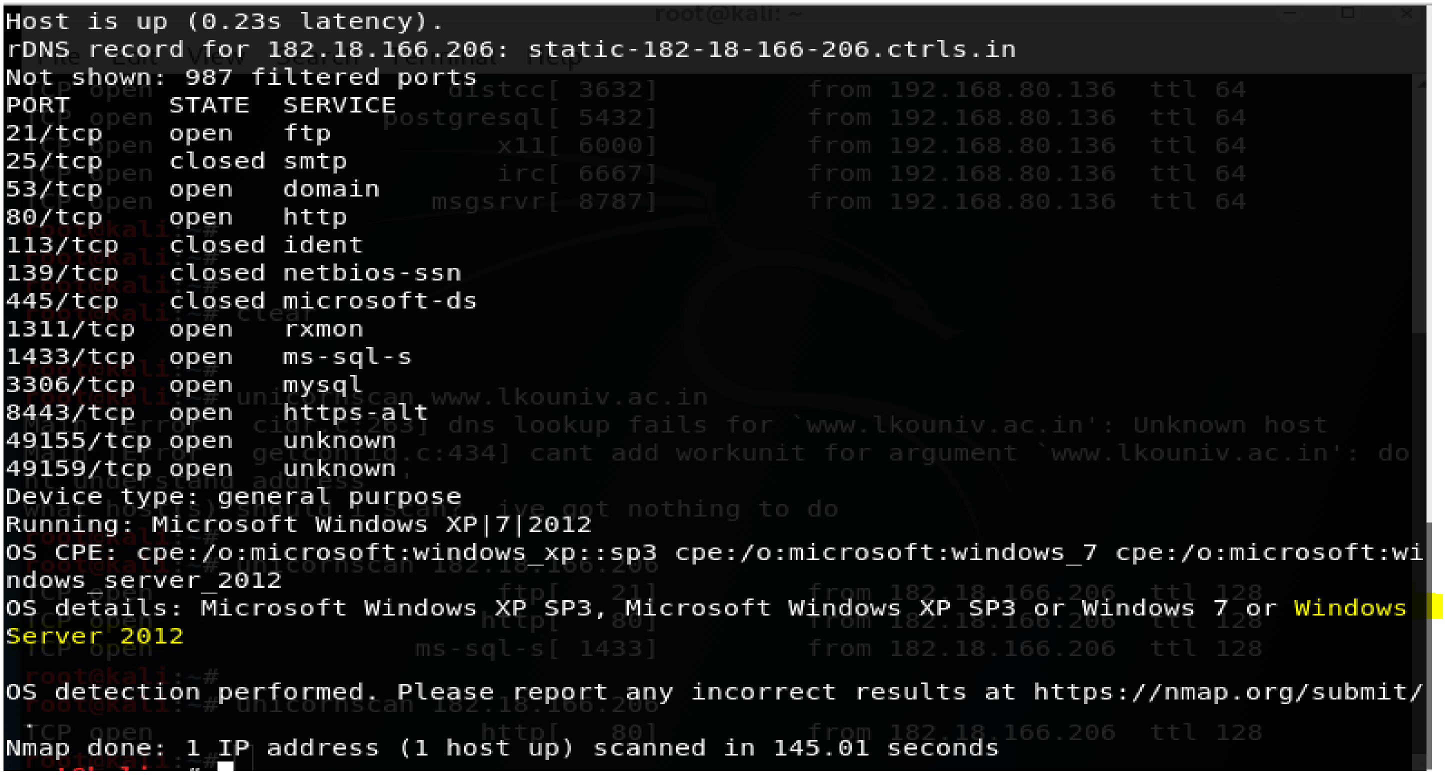


```
root@kali:~# unicornscan 182.18.166.206
TCP open                    ftp[   21]         from 182.18.166.206  ttl 128
TCP open                   http[   80]         from 182.18.166.206  ttl 128
TCP open               ms-sql-s[ 1433]         from 182.18.166.206  ttl 128
root@kali:~#
```



```
root@kali:~# nmap www.lkouniv.ac.in
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-11 17:39 EST
Nmap scan report for www.lkouniv.ac.in (182.18.166.206)
Host is up (0.072s latency).
rDNS record for 182.18.166.206: static-182-18-166-206.ctrls.in
Not shown: 984 filtered ports
PORT      STATE  SERVICE
21/tcp    open   ftp
25/tcp    closed smtp
53/tcp    open   domain
80/tcp    open   http
113/tcp   closed ident
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds
1149/tcp  closed bvtsonar
1311/tcp  open   rxmon
1433/tcp  open   ms-sql-s
2003/tcp  closed finger
3306/tcp  open   mysql
5666/tcp  open   nrpe
8443/tcp  open   https-alt
49155/tcp open   unknown
49159/tcp open   unknown

Nmap done: 1 IP address (1 host up) scanned in 81.91 seconds
root@kali:~#
```



```
Host is up (0.23s latency).
rDNS record for 182.18.166.206: static-182-18-166-206.ctrls.in
Not shown: 987 filtered ports
PORT      STATE  SERVICE
21/tcp    open   ftp
25/tcp    closed smtp
53/tcp    open   domain
80/tcp    open   http
113/tcp   closed ident
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds
1311/tcp  open   rxmon
1433/tcp  open   ms-sql-s
3306/tcp  open   mysql
8443/tcp  open   https-alt
49155/tcp open   unknown
49159/tcp open   unknown
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:wi
ndows_server_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows
Server 2012

OS detection performed. Please report any incorrect results at https://nmap.org/submit/

Nmap done: 1 IP address (1 host up) scanned in 145.01 seconds
```

Task 6:

One of the possible vulnerability on www.lkouniv.ac.in is service ‘FTP’. It is a service which transfers file in and out of the target server. If this service is intercepted then any piece of code can be put into the server enabling hackers to fetch sensitive information using response object. It can be intercepted in many ways. For example, if the wifi router (or any other network device) is known then recent defects on the product can be found in google easily. If university hasn’t upgraded the device software, device can be exploited to collect data from FTP service.

First step towards security is to use standardized network devices. Standard device makers provide patches time to time so that any new anomaly found is corrected asap.

Secondly including a system which checks any unusual activity in the system. Even after getting into the system, hackers need to send data outside of servers. Unusual data transfer can be checked and further alerted to relevant IT support team.