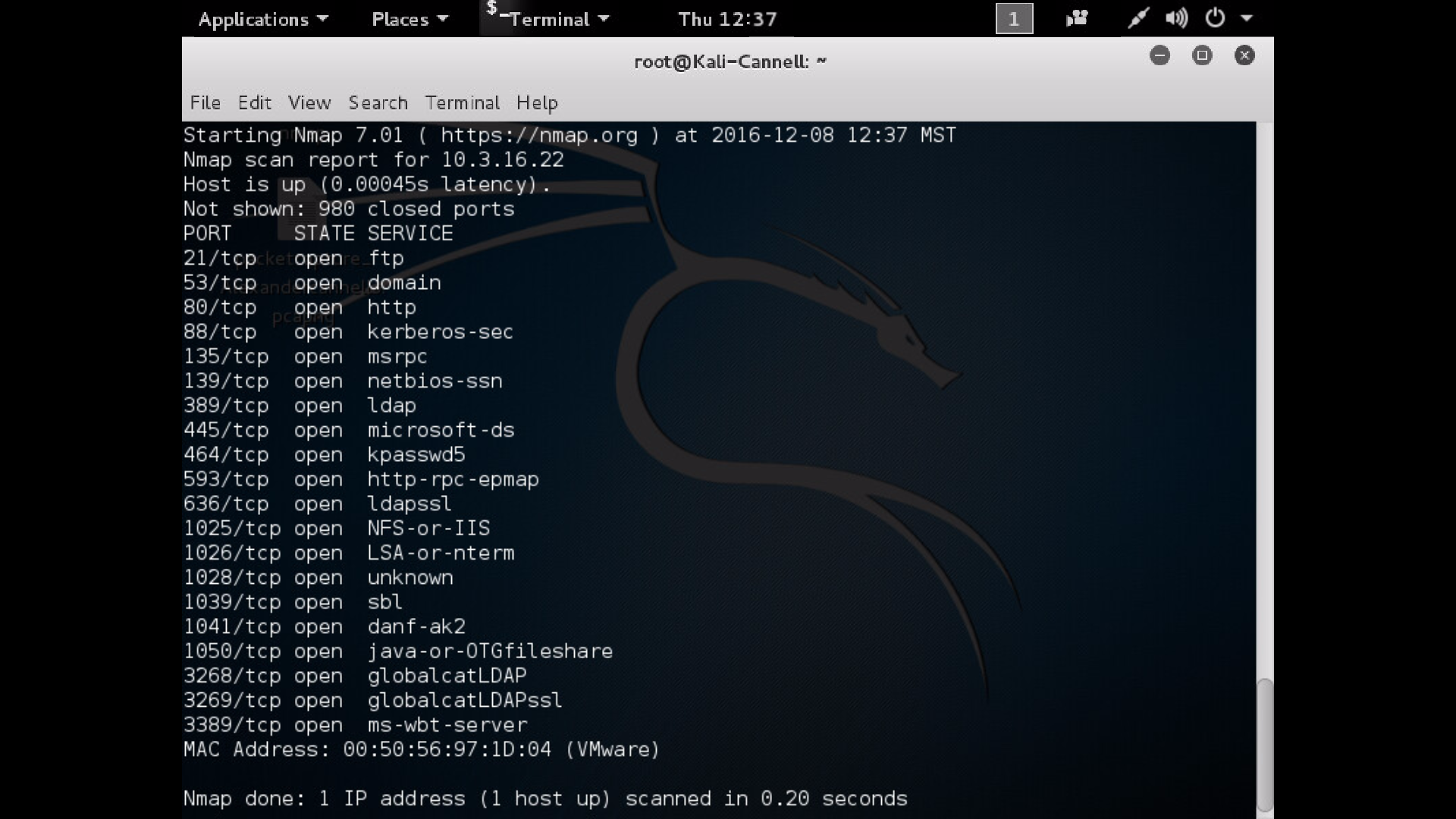
Alexander Cannell

CSIA 6010

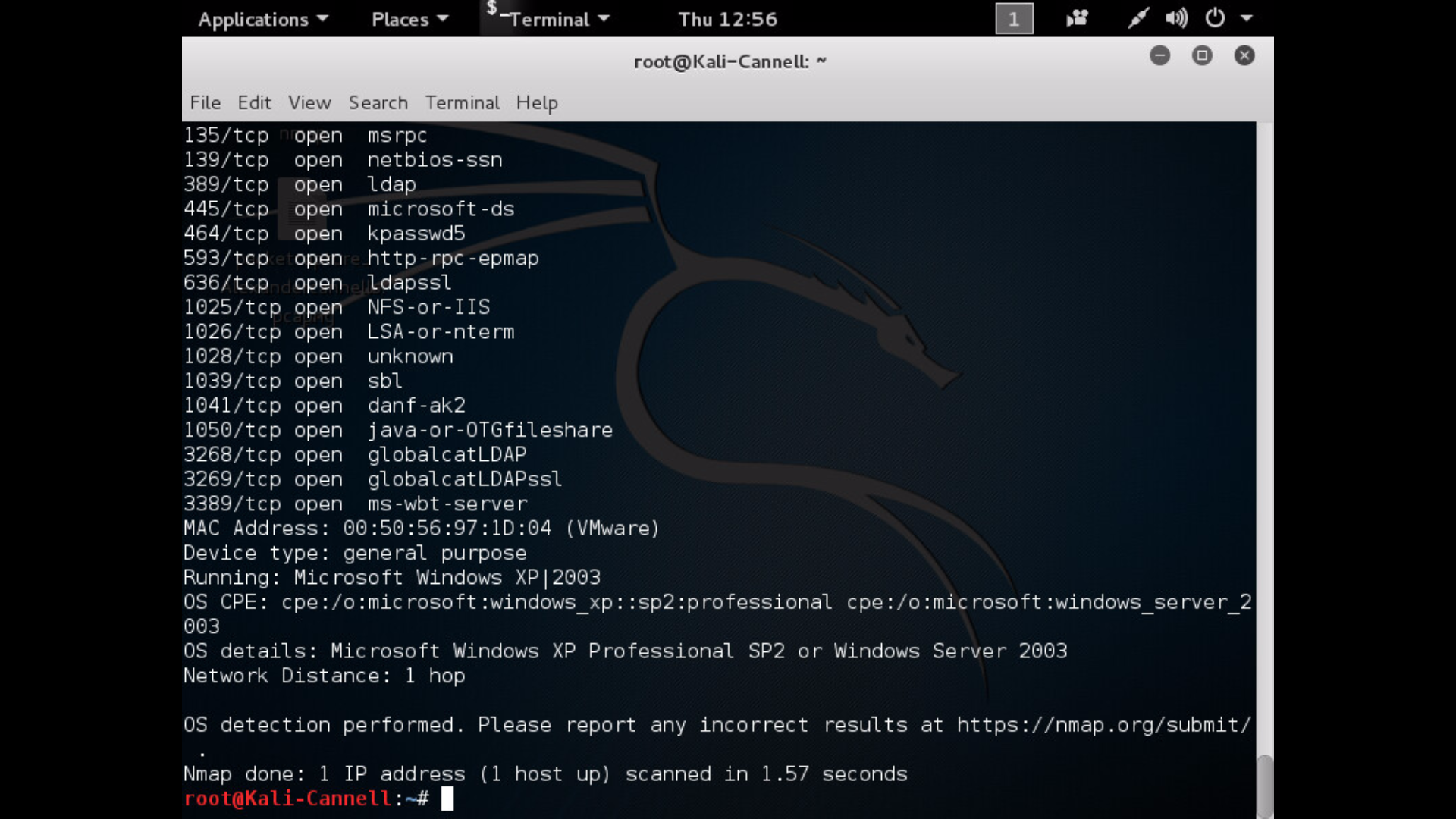
Network Security Tools

**NMAP SCAN:**

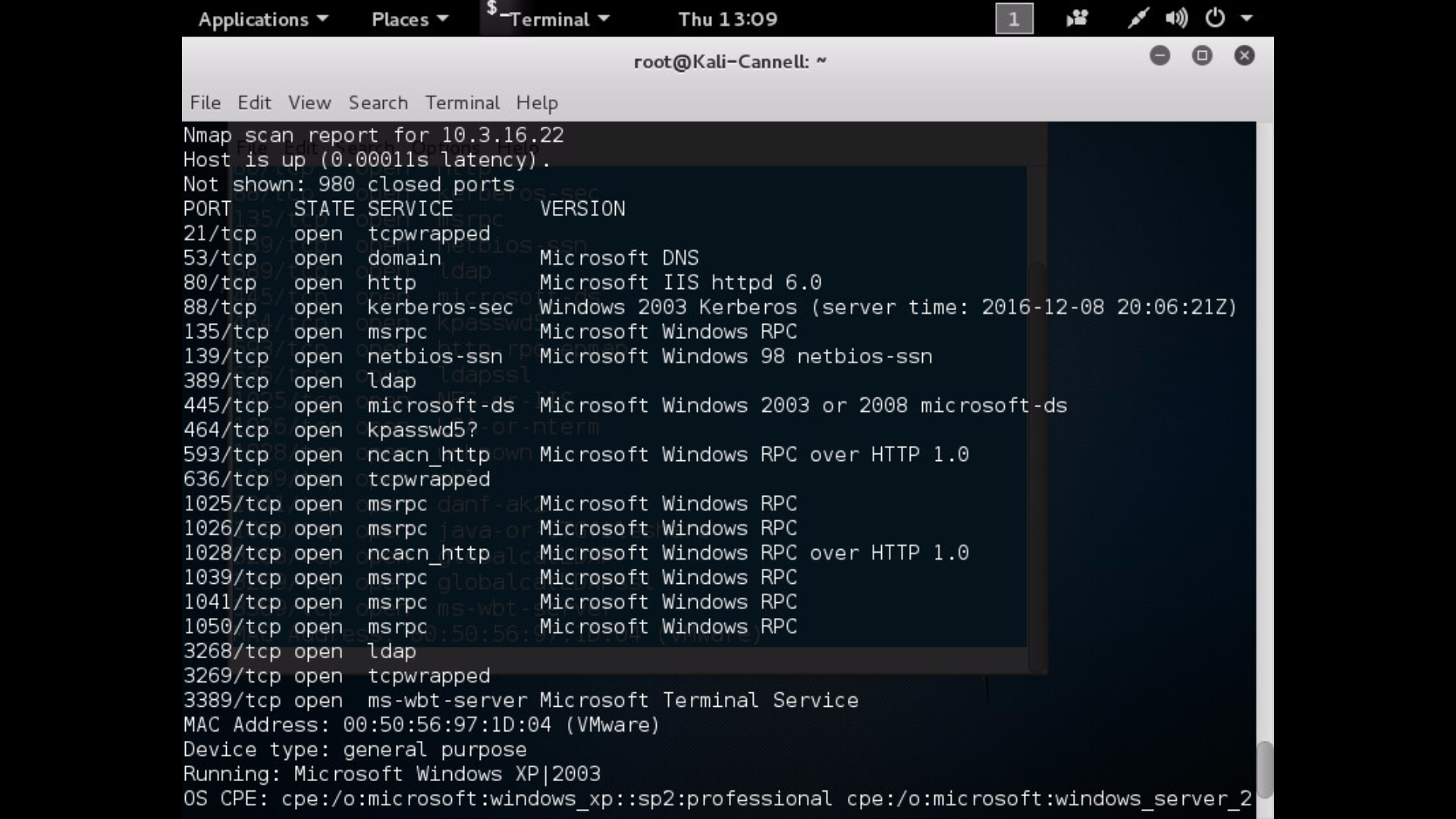
Running a NMAP Stealth Scan on 10.3.16.22; nmap -sS 10.3.16.22 to show the open ports, we can also see what is being run on those open ports.



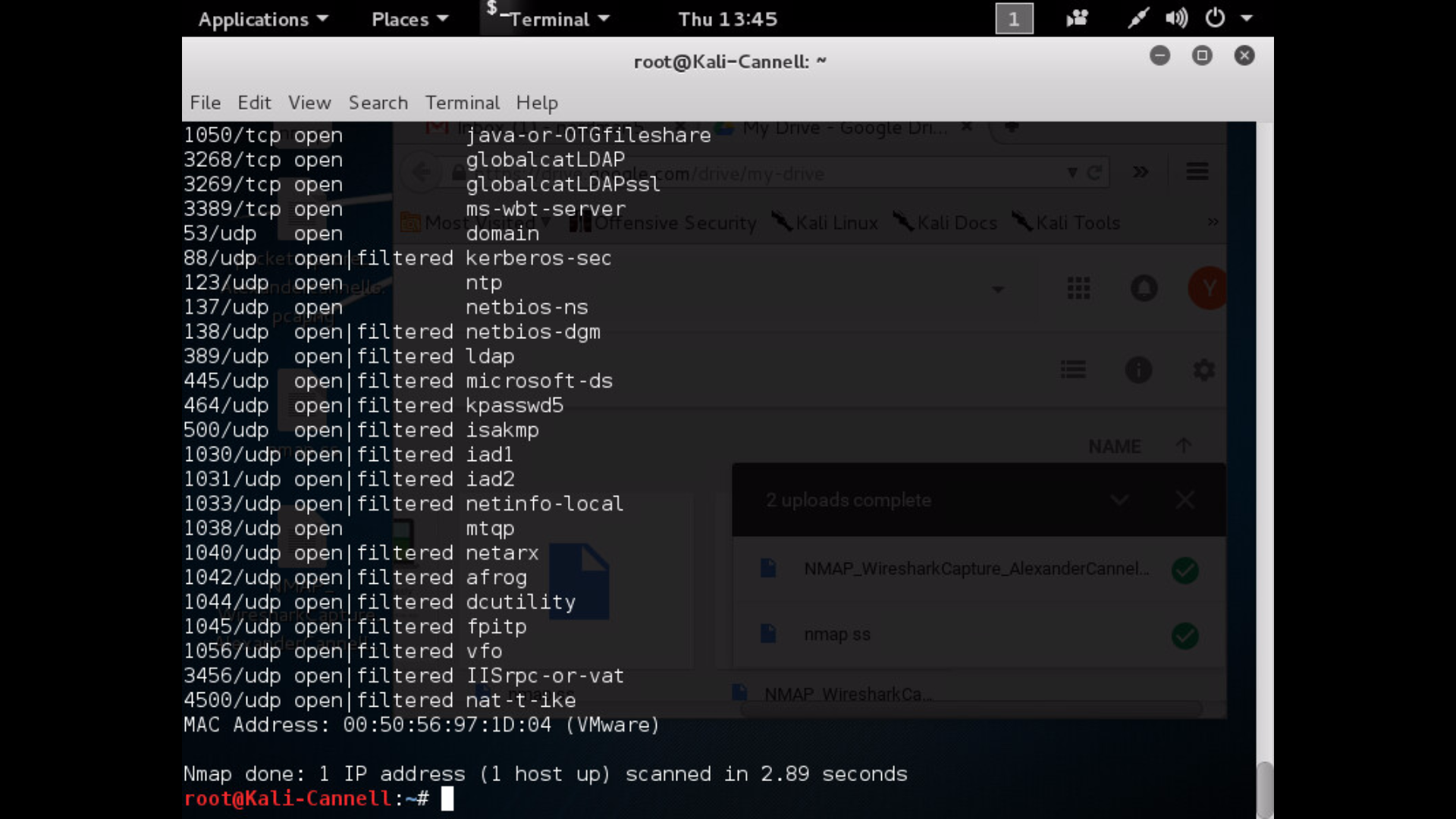
We can also use NMAP to find the Operating System by putting an -O at the end of our command. The OS that 10.3.16.22 is running is a Windows XP Professional:



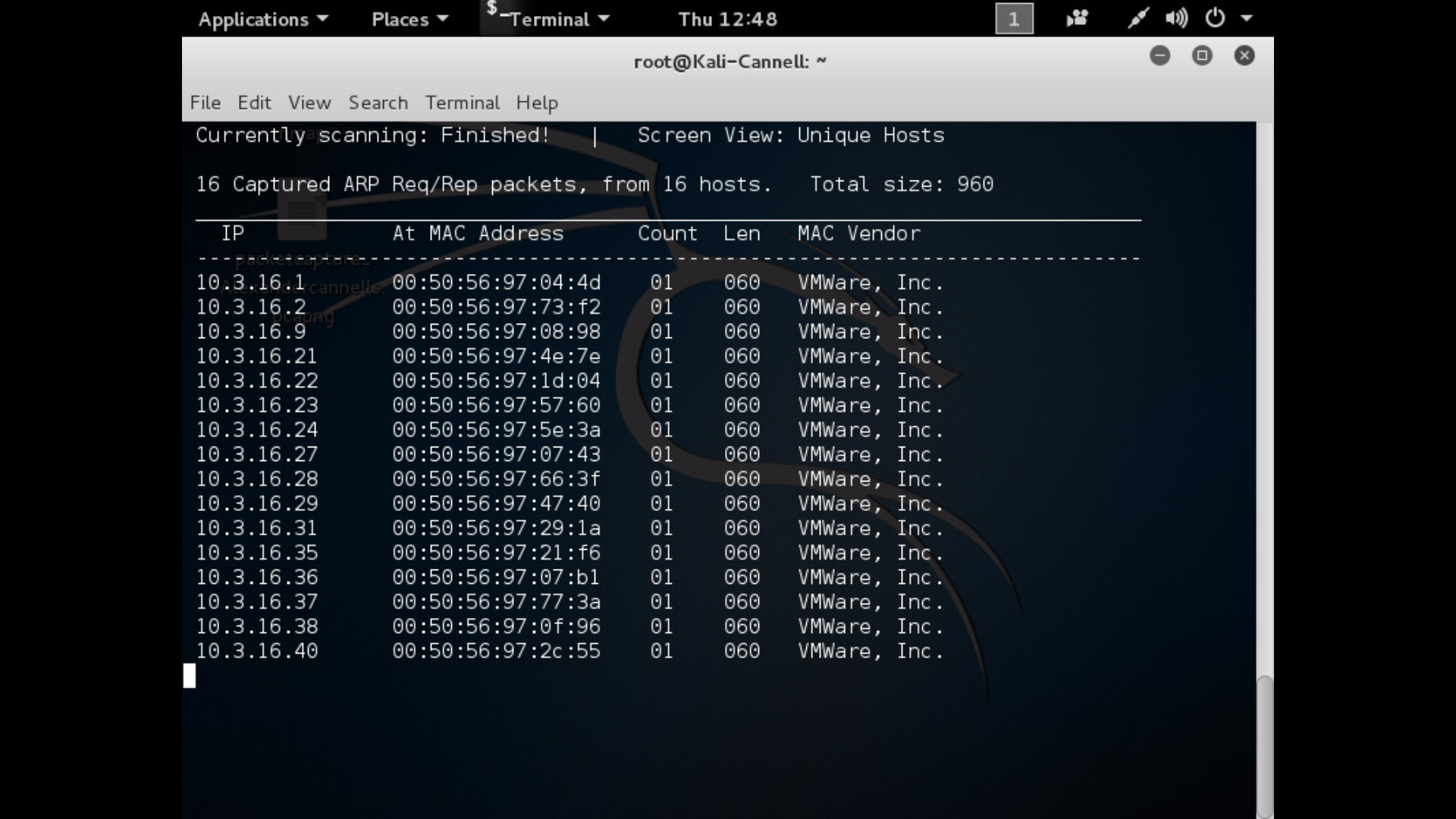
If you do a nmap -sV 10.3.16.22 it is a port prob that will tell you what service is being run on those open port, and what programs too.



If you do a nmap -sS -sU -PN 10.3.16.22 scan you can also see the open UDP ports and filtered ports.



Running a NETDISCOVER on 10.3.16.0/24 is another way we can see what 10.3.16.22’s MAC address is; Also another way of finding other devices on the network.



**What Ports are Open? What Services are running on the box based on the open ports?**

PORT STATE SERVICE

21/tcp open ftp

53/tcp open domain

80/tcp open http

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

1025/tcp open NFS-or-IIS

1026/tcp open LSA-or-nterm

1028/tcp open unknown

1039/tcp open sbl

1041/tcp open danf-ak2

1050/tcp open java-or-OTGfileshare

3268/tcp open globalcatLDAP

3269/tcp open globalcatLDAPssl

3389/tcp open ms-wbt-server

53/udp open domain

88/udp open|filtered kerberos-sec

123/udp open ntp

137/udp open netbios-ns

138/udp open|filtered netbios-dgm

389/udp open|filtered ldap

445/udp open|filtered microsoft-ds

464/udp open|filtered kpasswd5

500/udp open|filtered isakmp

1030/udp open|filtered iad1

1031/udp open|filtered iad2

1033/udp open|filtered netinfo-local

1038/udp open mtqp

1040/udp open|filtered netarx

1042/udp open|filtered afrog

1044/udp open|filtered dcutility

1045/udp open|filtered fpitp

1056/udp open|filtered vfo

3456/udp open|filtered IISrpc-or-vat

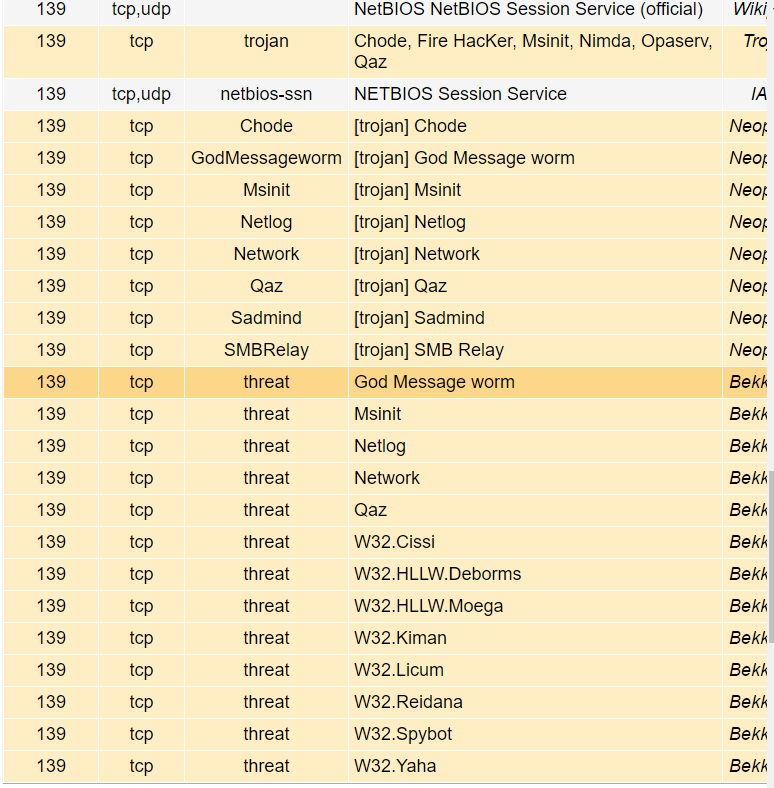
4500/udp open|filtered nat-t-ike

**What vulnerabilities can you identify in relation to any of the ports that are open? Are there actual exploits associated with those vulnerabilities?**

* 464/tcp open kpasswd5
  + “A vulnerability has been reported in Kerberos, which can be exploited by a DoS. The vulnerability is caused due to the kpasswd application not properly handling malformed UDP packets and can be exploited to exhaust CPU and network resources via the UDP “ping pong” attack on TCP port 464.” (Speedguide, 2016)
* 445/udp open|filtered microsoft-ds
  + “Port 445 should be blocked at the firewall level...leaving port 445 open will leave you vulnerable to some worms, such as W32.deloader and IraqiWorm...Critical RPC vulnerability that can be exploited via port 445 don't allow RPC over an unsecure network such as the internet. ” (Speedguide, 2016) There are a lot more vulnerabilities such as more worms, trojans, and other threats that can get in through port 445.” (Speedguide, 2016)



* 1050/tcp open java-or-OTGfileshare
  + “The MiniCommand Trojan is the primary exploit, which is a backdoor. Heartbeat listening port on the primary and backup routers in this load-balancing package for linux. Some windows server 2003 machines may use this port for DNS if other ports are being blocked by a firewall. ” (Speedguide, 2016)
* 593/tcp open http-rpc-epmap
  + “There is a critical buffer overrun RPC vulnerability that can be exploited this port should be filtered and can be exploited through ports 135, 139, 445, 593. ” (Speedguide, 2016)
* 139/tcp open netbios-ssn
  + There can be a number of vulnerabilities when leaving this port open…. The best protection is to block ports 135-139. But if you must enable it, you should have strong passwords, attach a $ at the end of your share names, and block at the router or firewall ports 135-139. You can leak out information about your system that can be used against you to the internet unless filtered by a firewall. Also Vulnerable to Critical Windows RPC vulnerabilities. Vulnerable to worms, trojans, and backdoors where worms can attempt to download and execute a remote file via FTP. Also Vulnerable to buffer overflow which allows remote attackers to execute code via SMB packets on TCP port Sessions. (Speedguide, 2016)



**References:**

* SpeedGuide Inc. "SpeedGuide.net - Broadband, Wireless, Network Security." *SpeedGuide*. N.p., n.d. Web. 08 Dec. 2016.
* @HackingTutors. "Nmap Open Port Scanning and OS Detection." *Hacking Tutorials*. N.p., 2016. Web. 08 Dec. 2016.