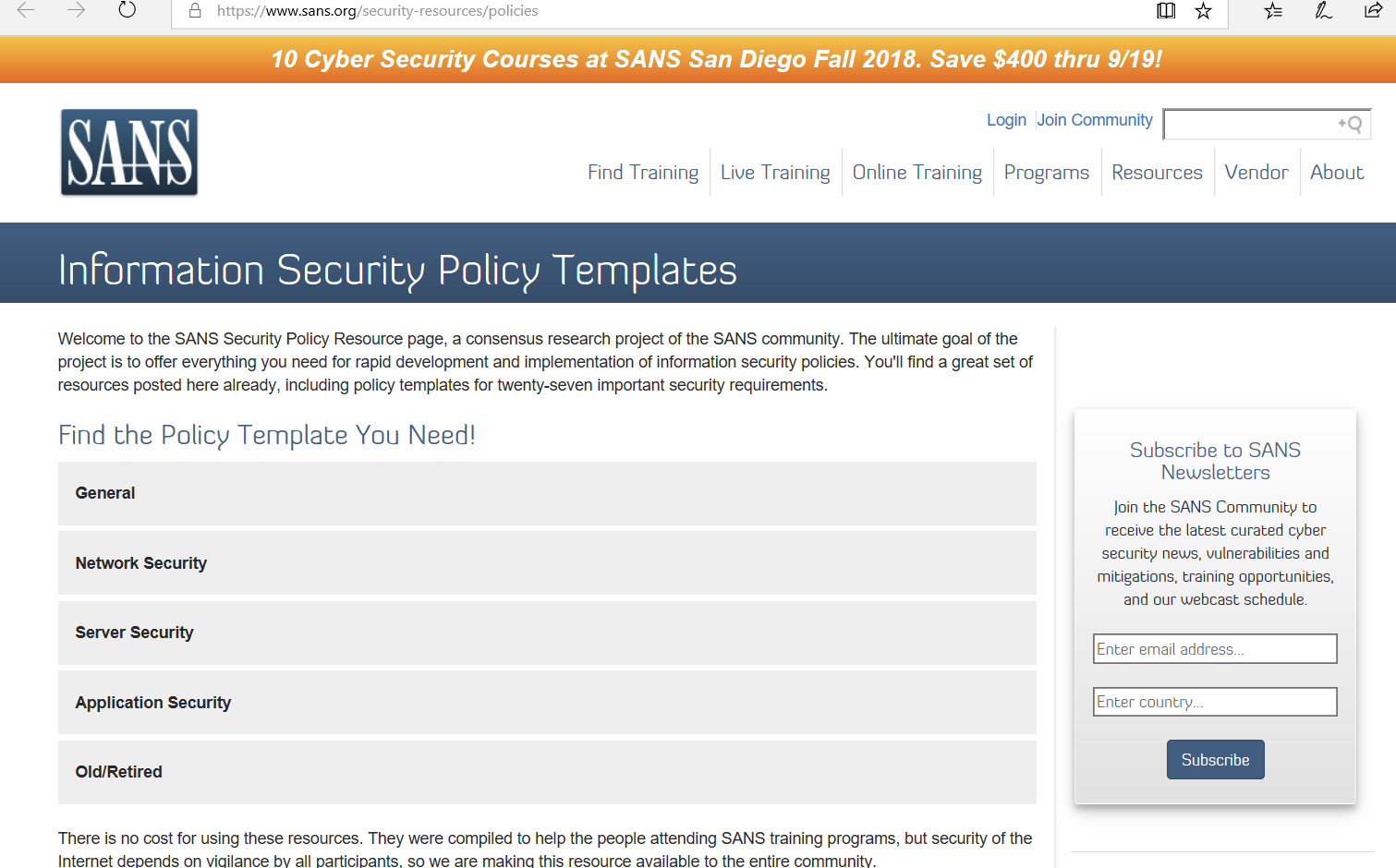
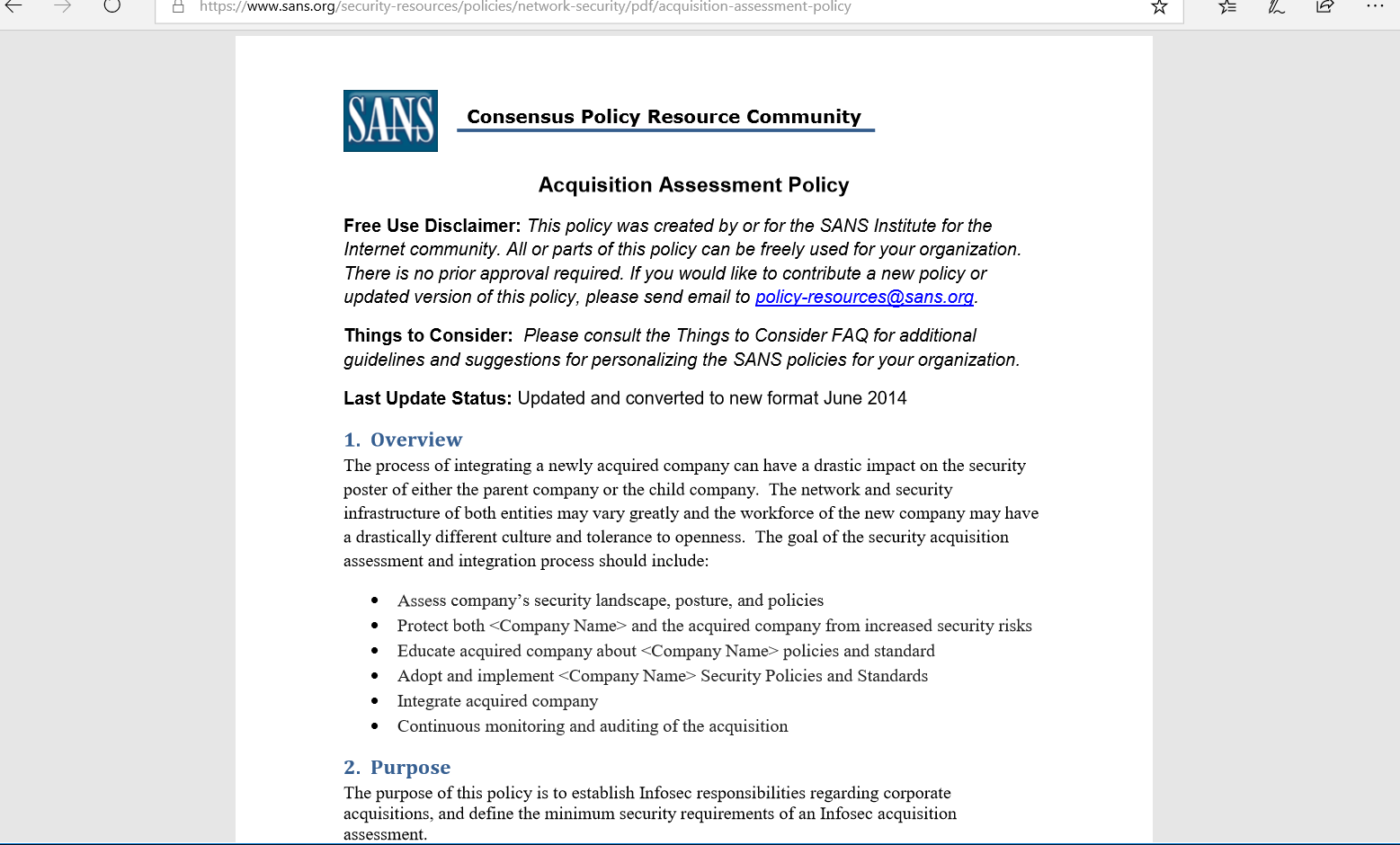
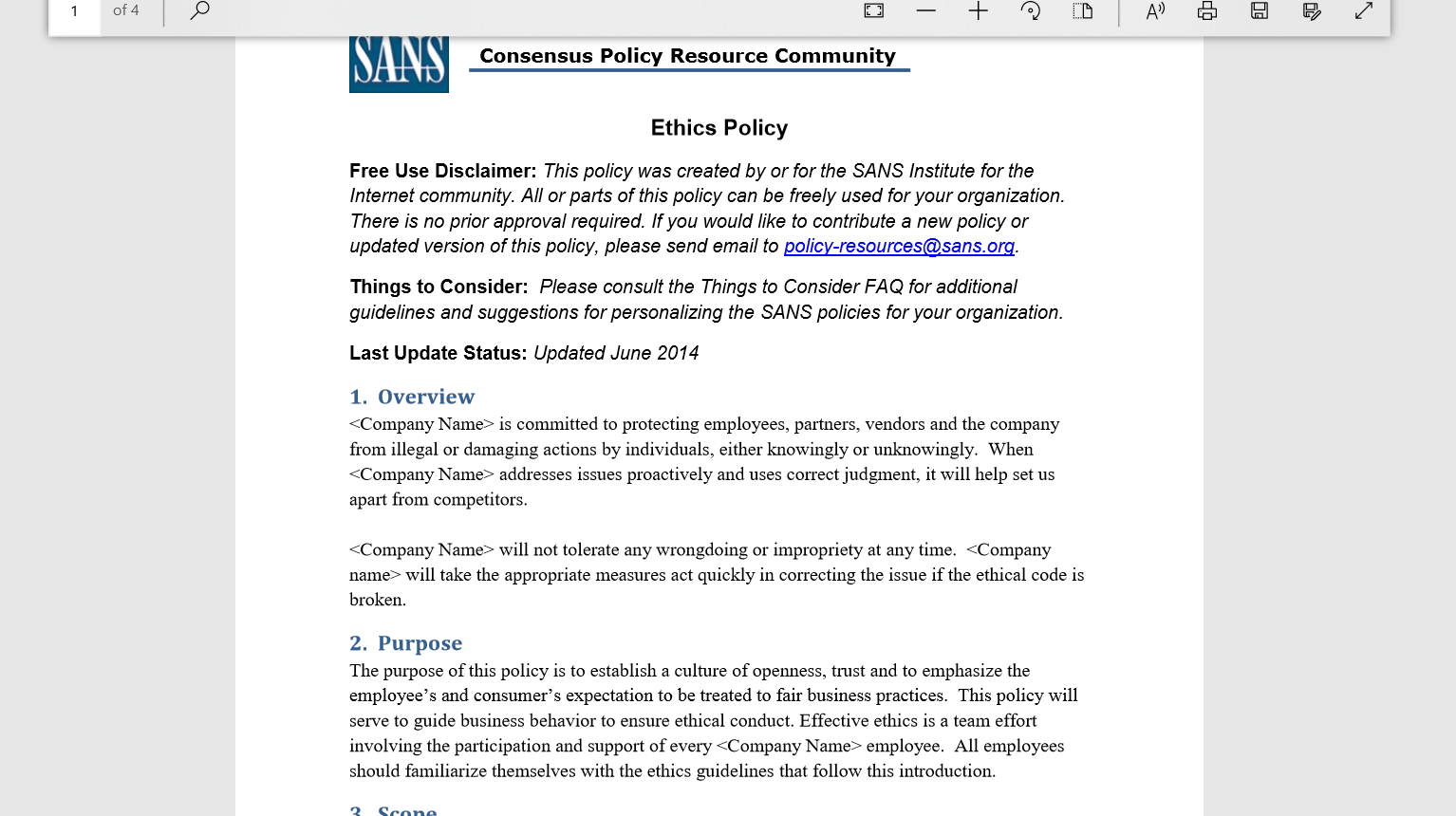
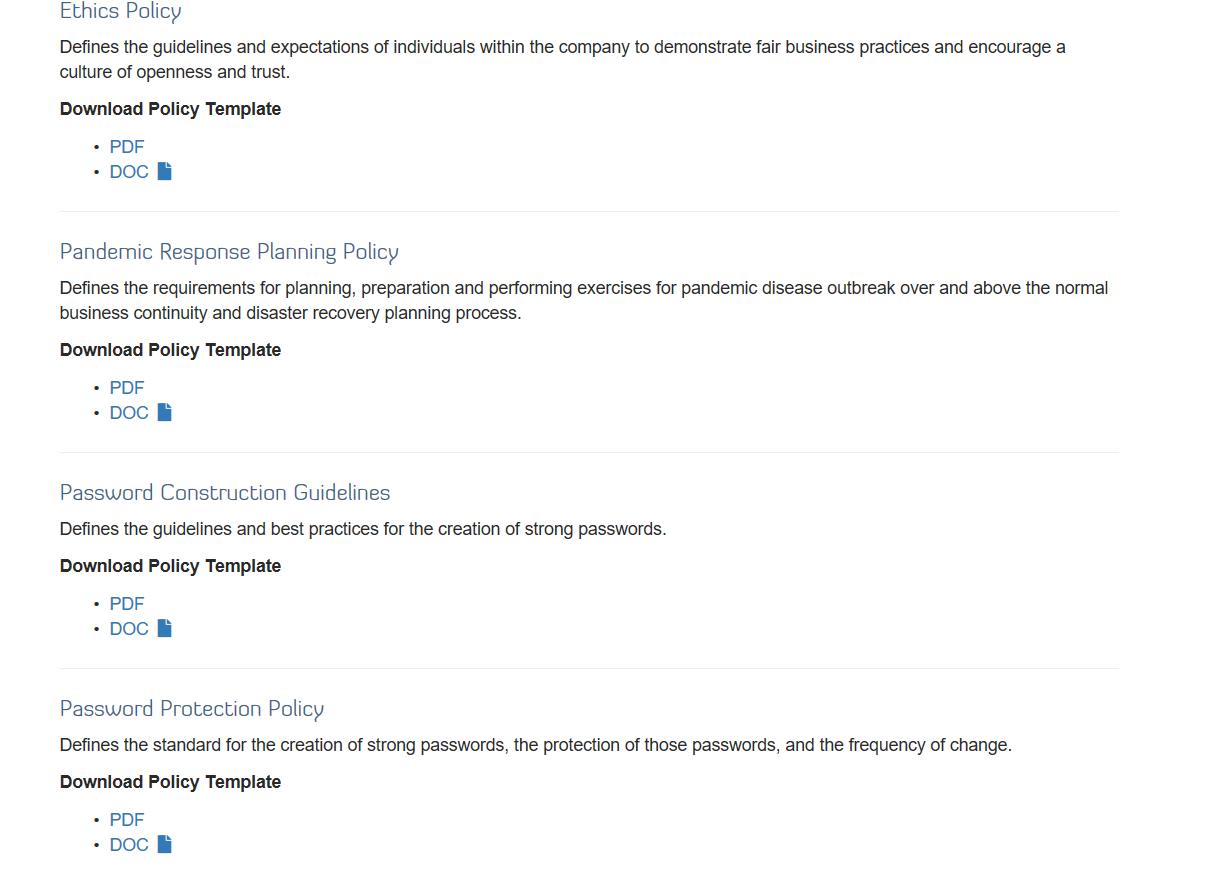
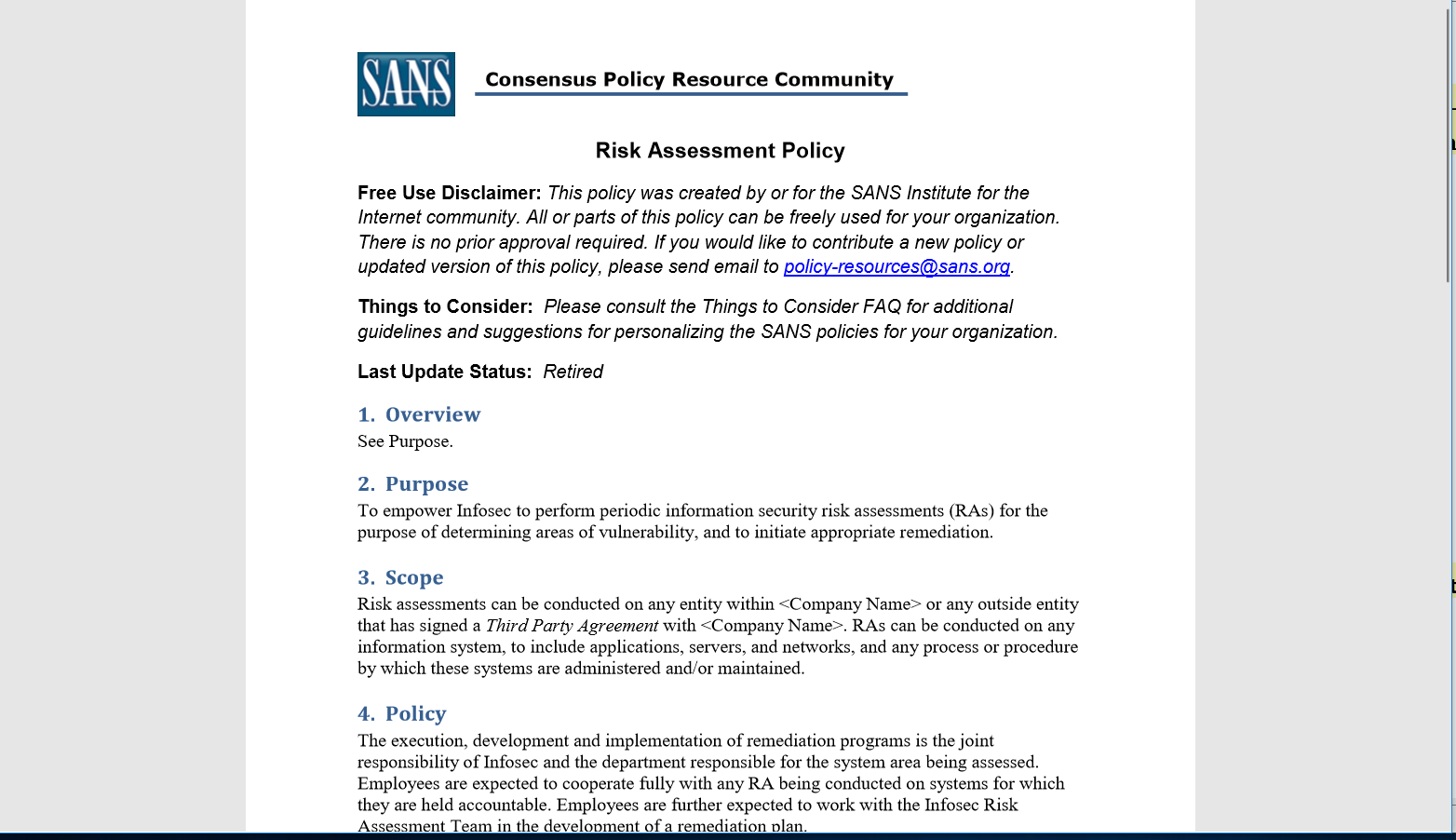
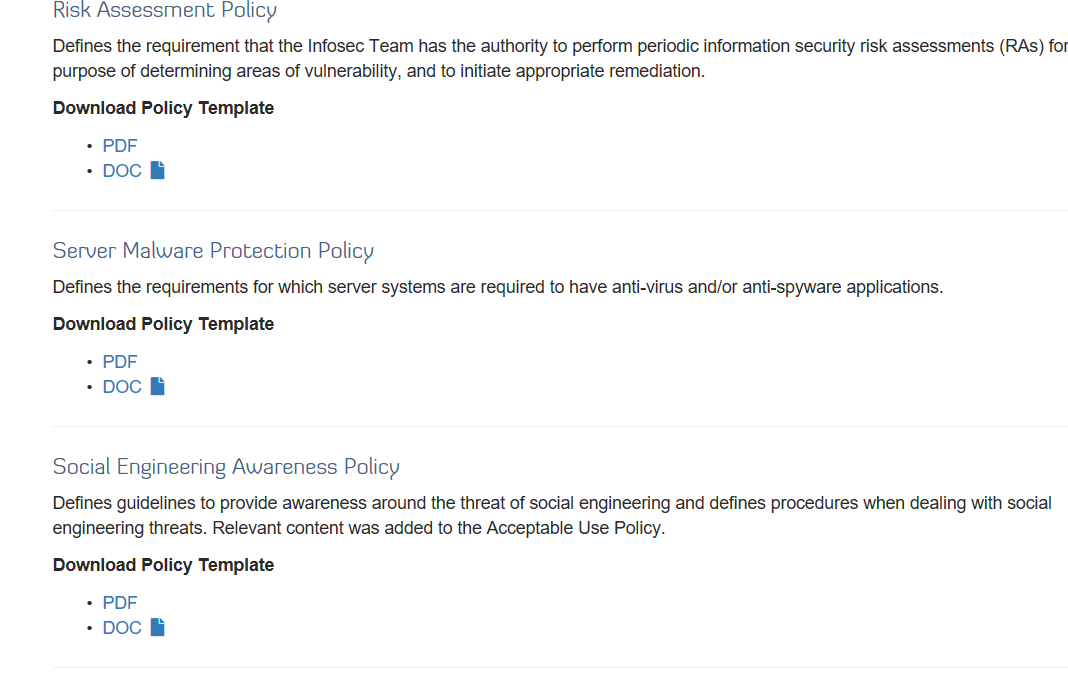
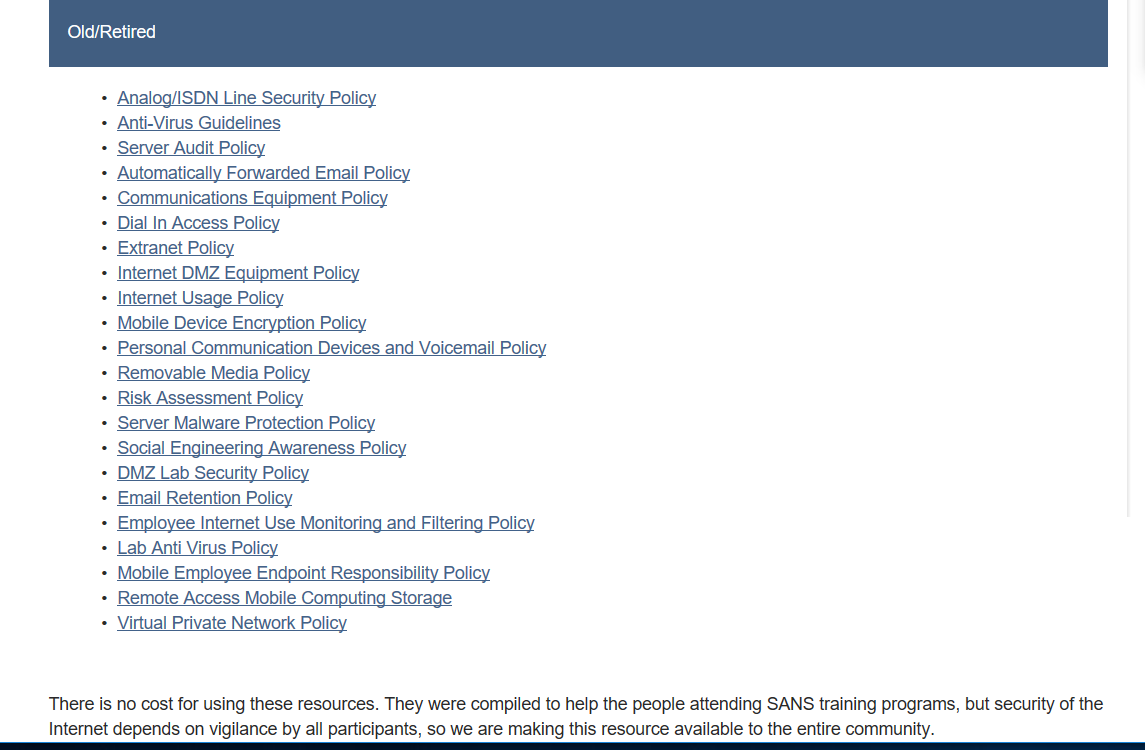
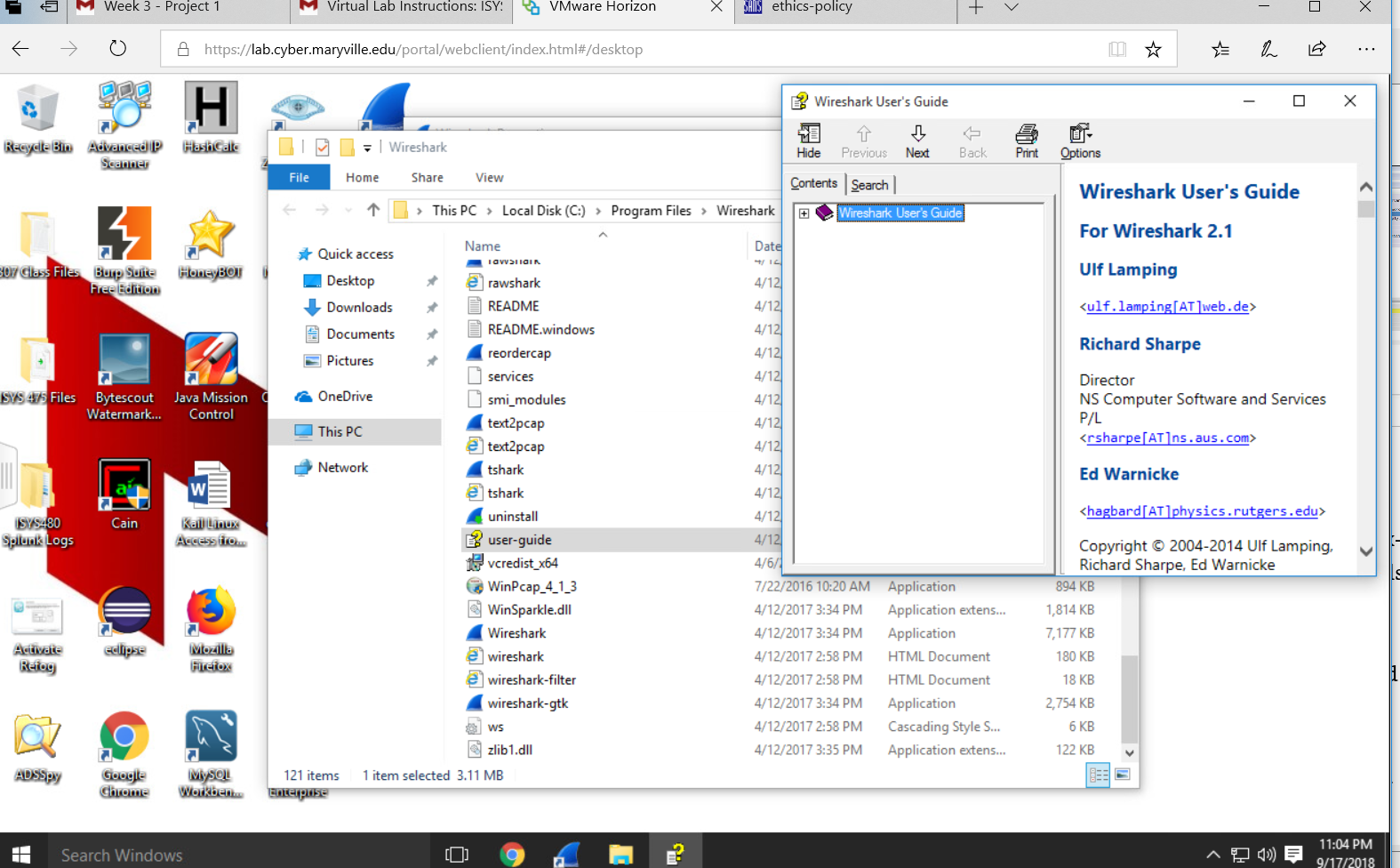
Exercise 1.1

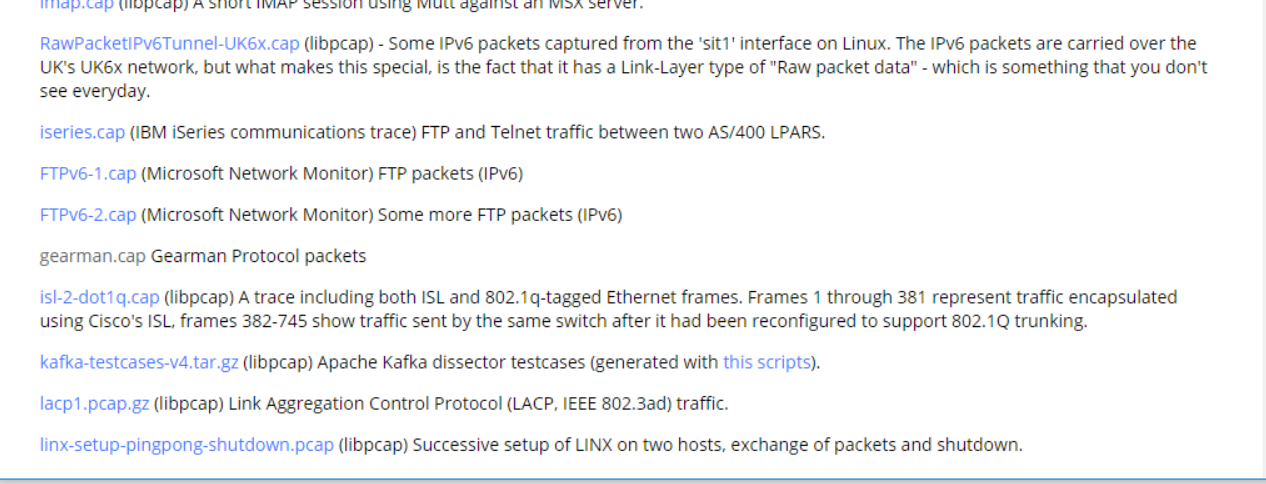


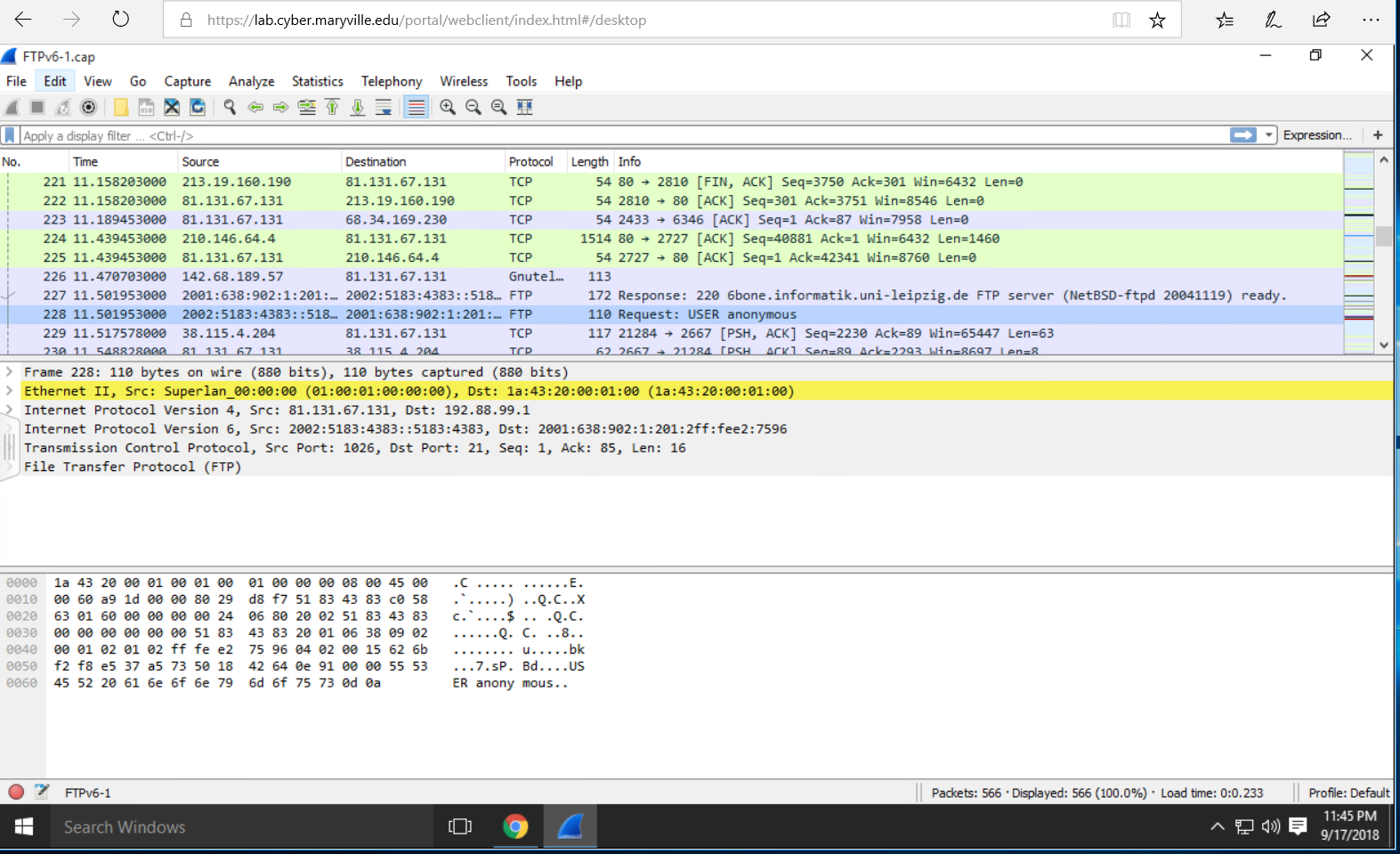




Exercise 2.1







Exercise 2.2

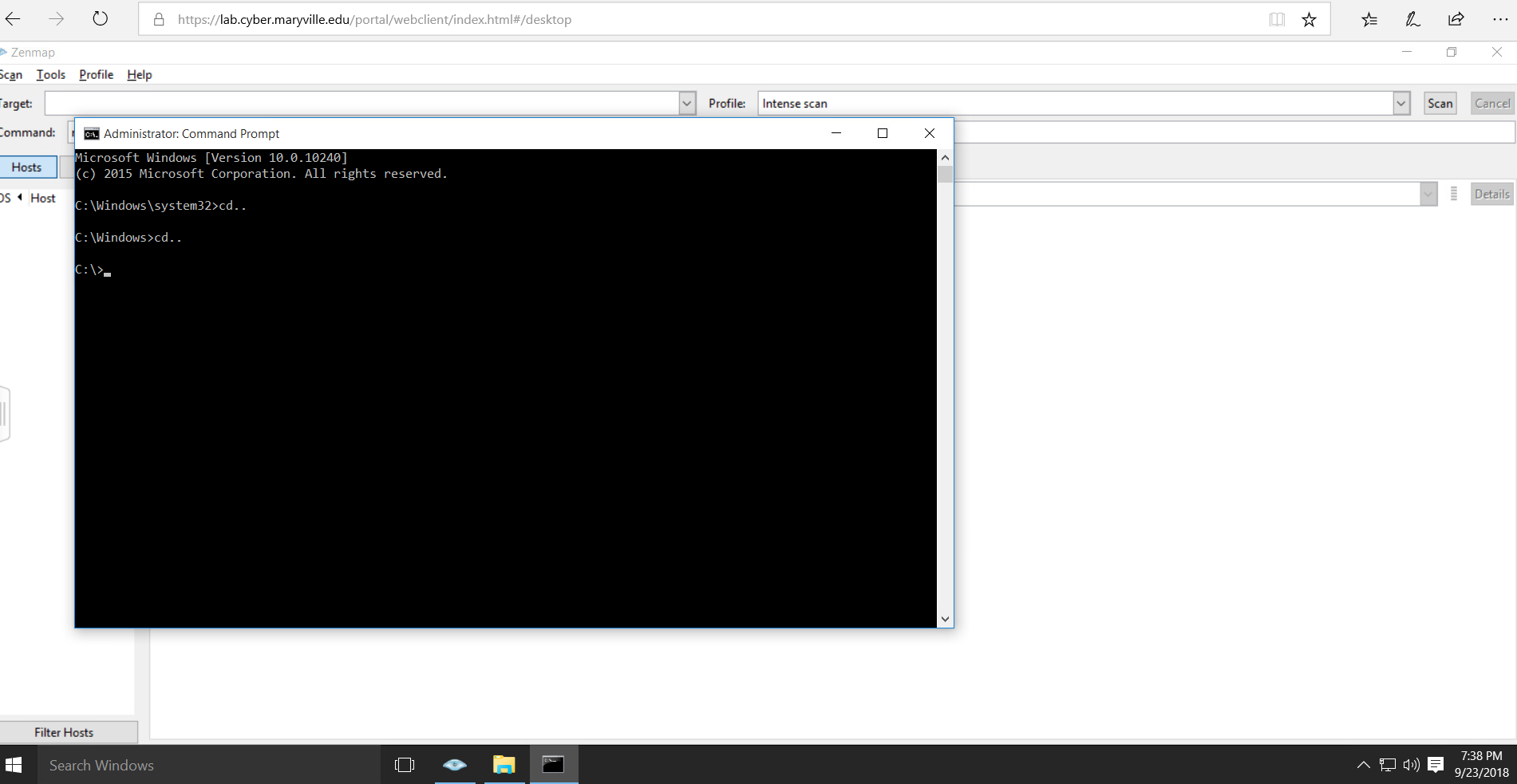
|  |  |  |  |
| --- | --- | --- | --- |
| Layer | Layer Responsibility | Protocols, Ports, or Services | Potential Attacks |
| Application | Communication | SNMP, Telnet, DNS, SSH, SMTP | Password Attacks through Telnet or FTP |
| Host-to-host | Connection and connectionless communication | TCP and UDP | Session hijacking, connectionless, scanning communication |
| Internet | Deliver, and route data; detect errors | IP and ICMP | Routing attacks, man-in-the-middle attacks |
| Network access | Physical layer delivery | ARP | Spoof MAC address |

Exercise 3.1

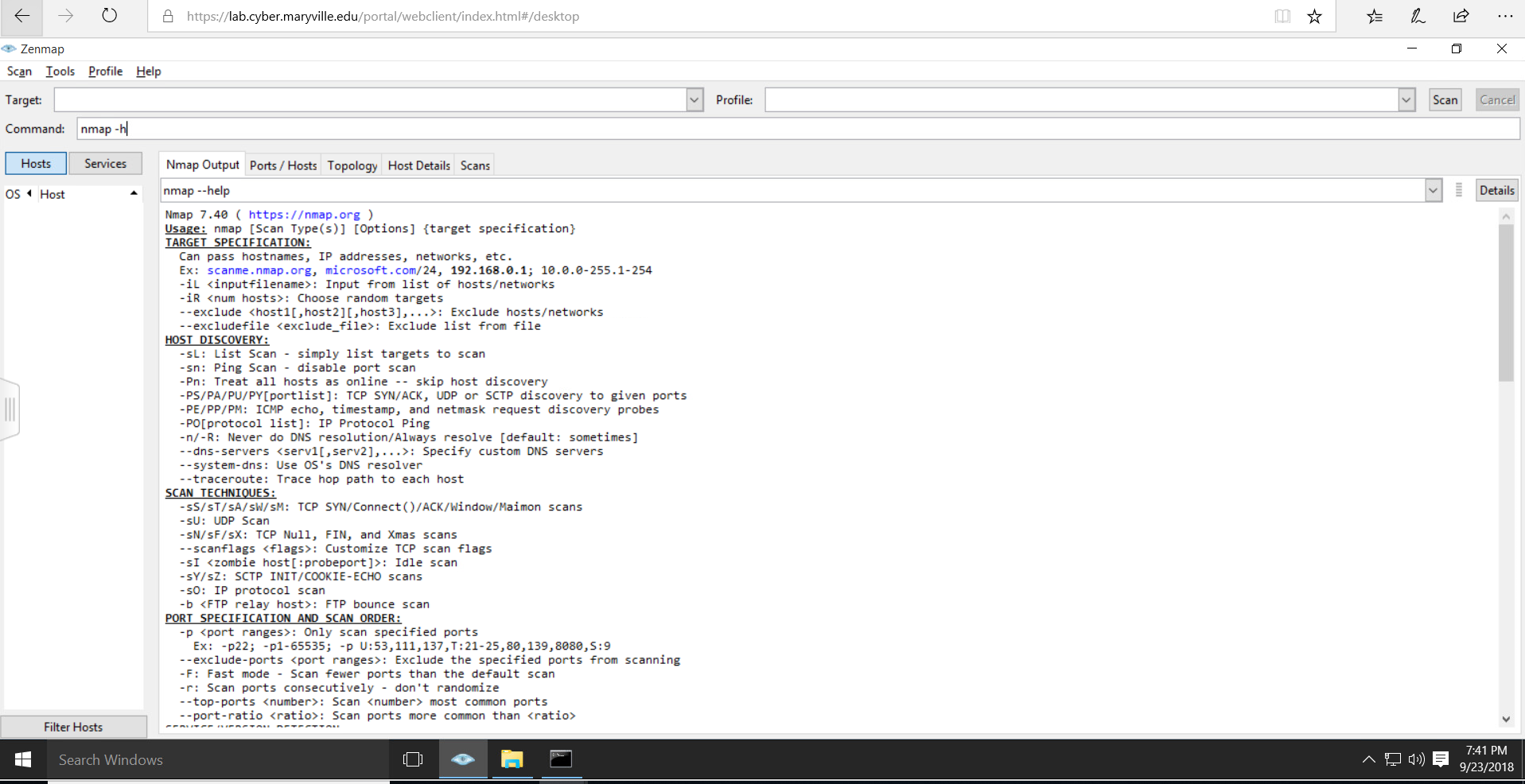
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Domain Name | IP Address | Location | Contact Person | Address and Pone Number |
| Redriff.com |  |  | Whois Foundation | Office 3-C PO Box 0823-03015  (507)=836-5679 |
| Examcram.com |  |  | Pearson Education, Inc. | Old Tappan, NJ. 07675  (201)-767-5000 |
| Rackspace.com |  |  | Chris Hansell | (210)-312-4000  Hostmaster@rackspace.com |
| Rutgers.edu |  |  | Office of Information Technology Telecommunications Division | Piscataway, NJ 08854 (848)-445-7541 netmanager@rutgers.edu |
|  |  |  |  |  |

Exercise 3.2

Step 2



Step 3



Steps 4-7

NMap commands

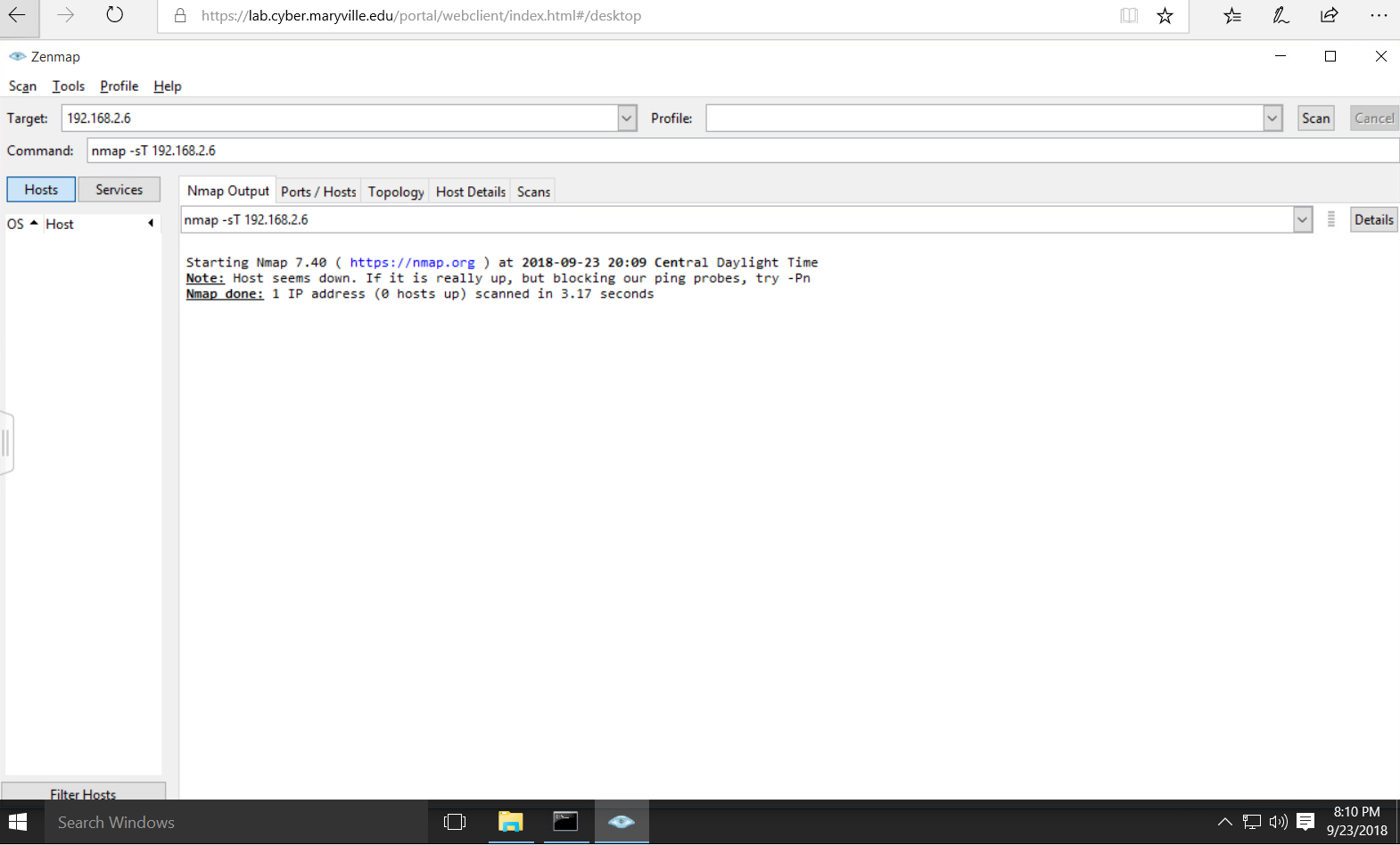
Full connect Scan: sT

Stealth Scan: sS

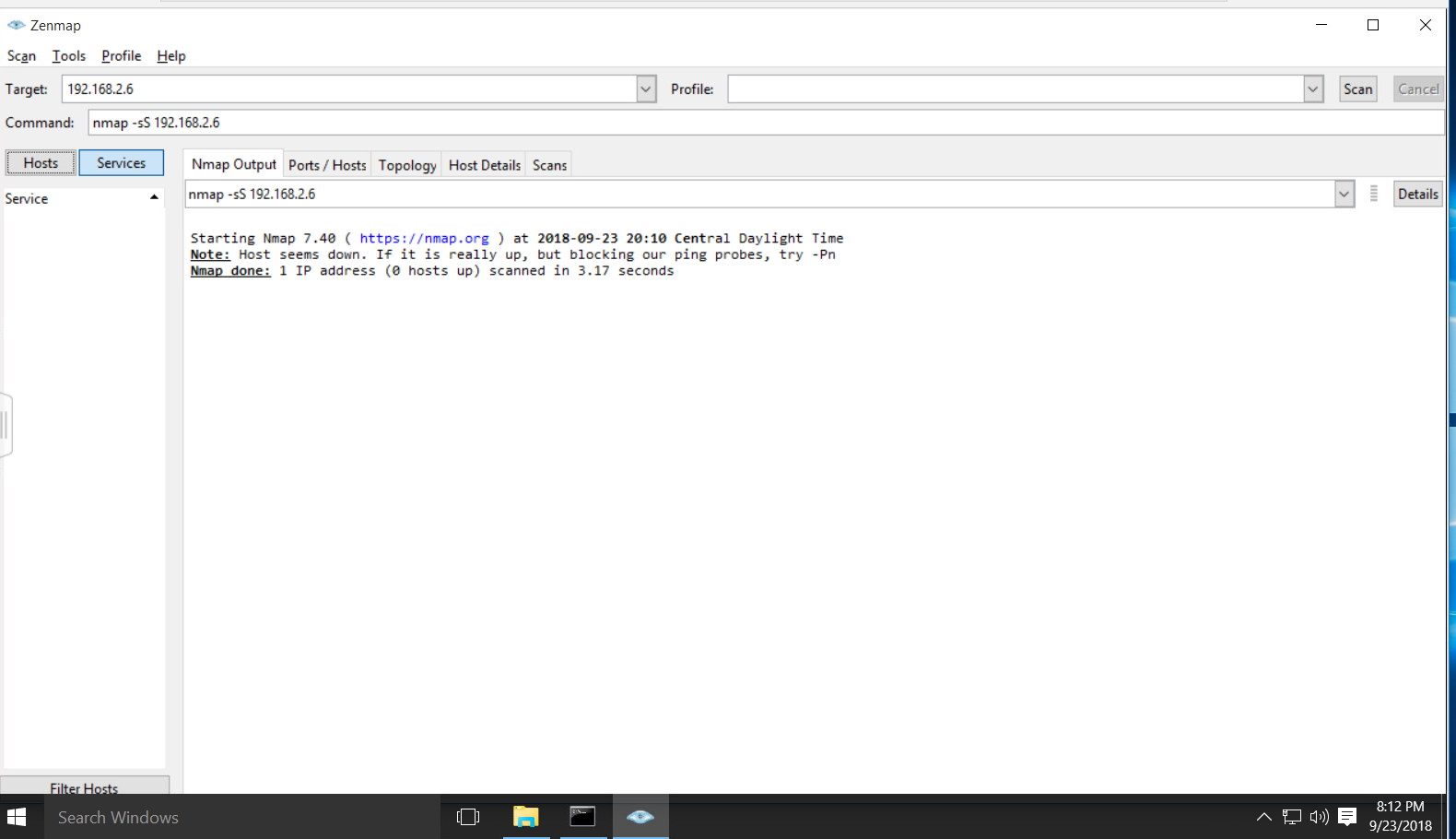
UDP Scan: sU

Fingerprint Scan: OS

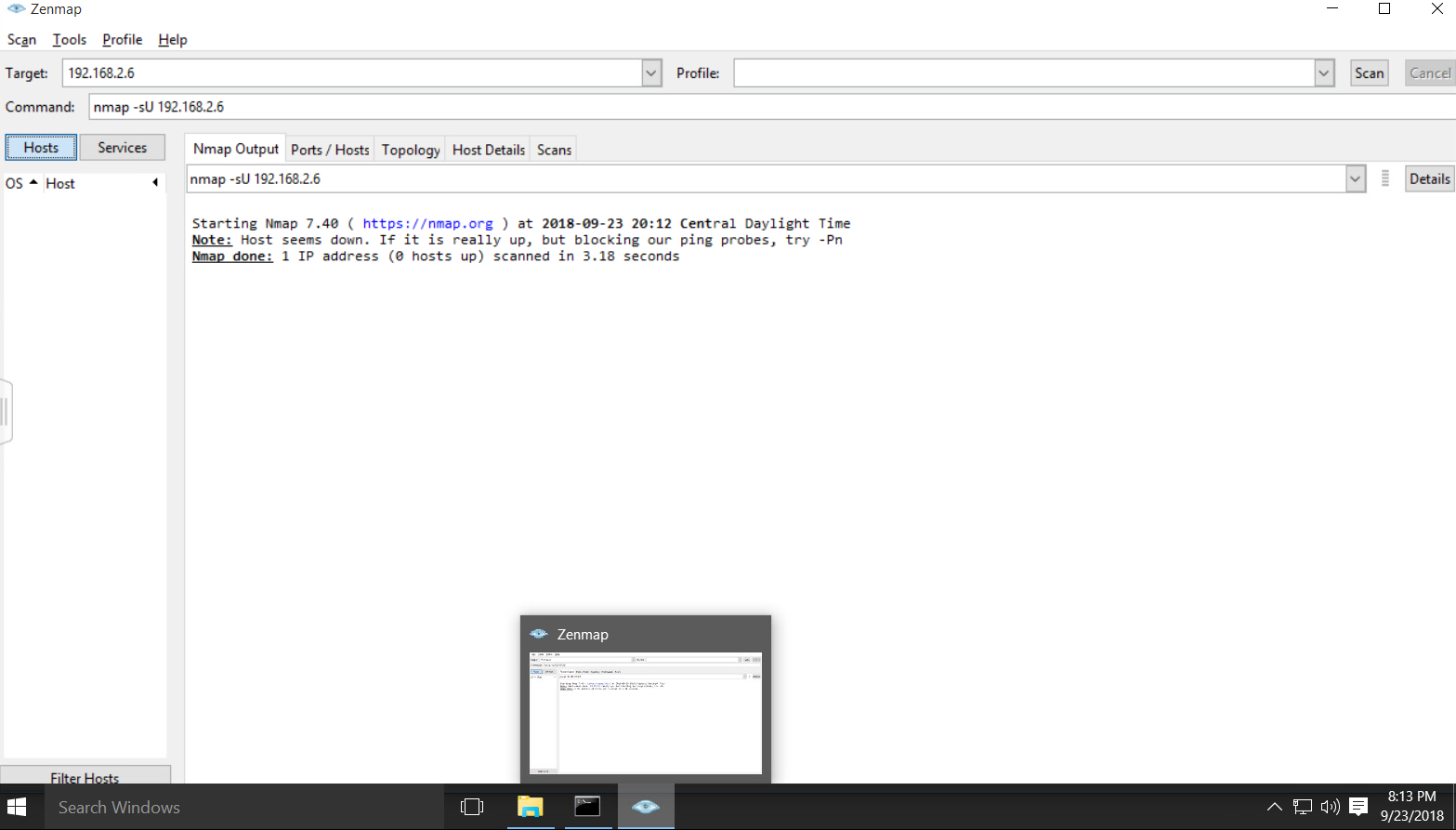
Step 8



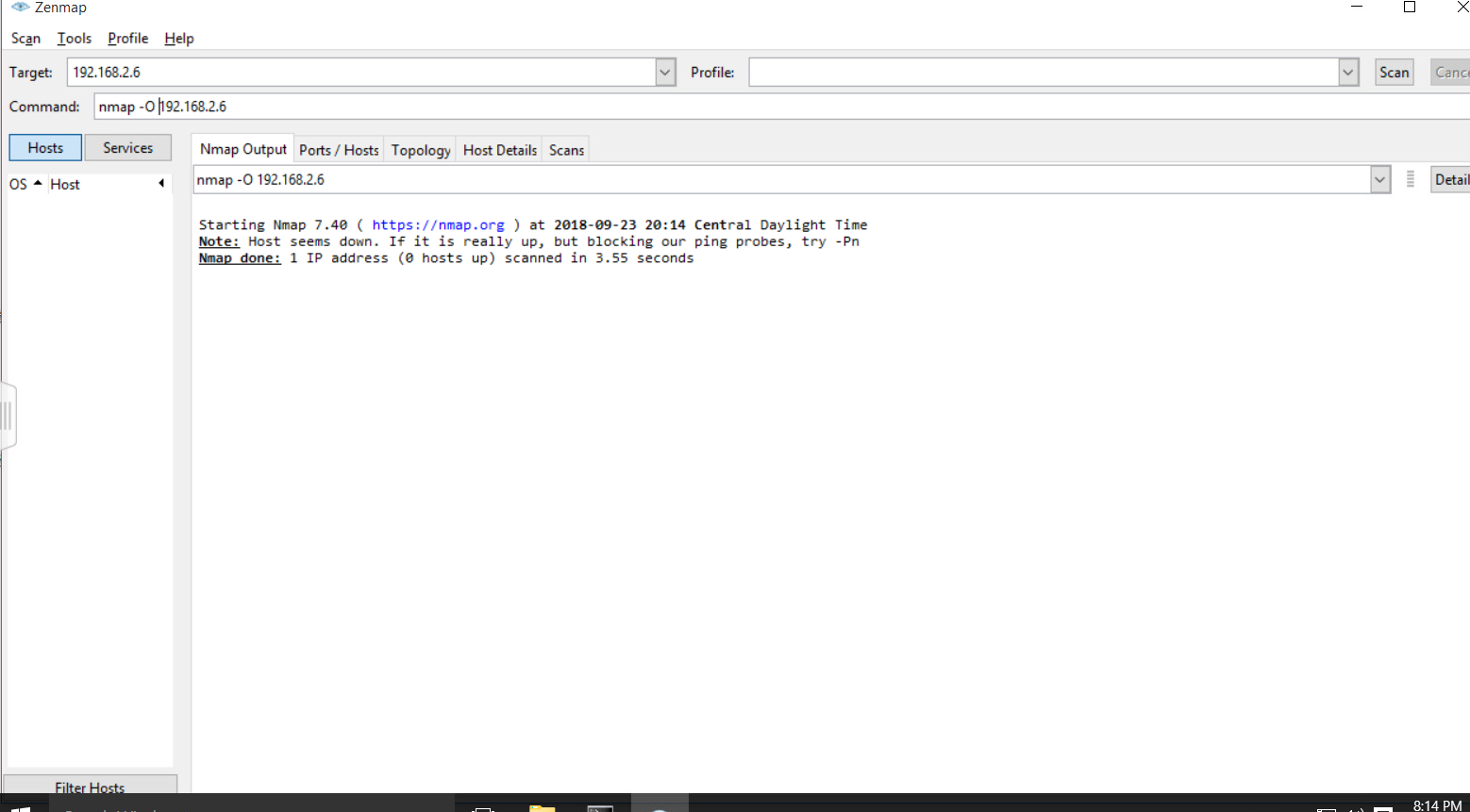
Step 9



Step 10



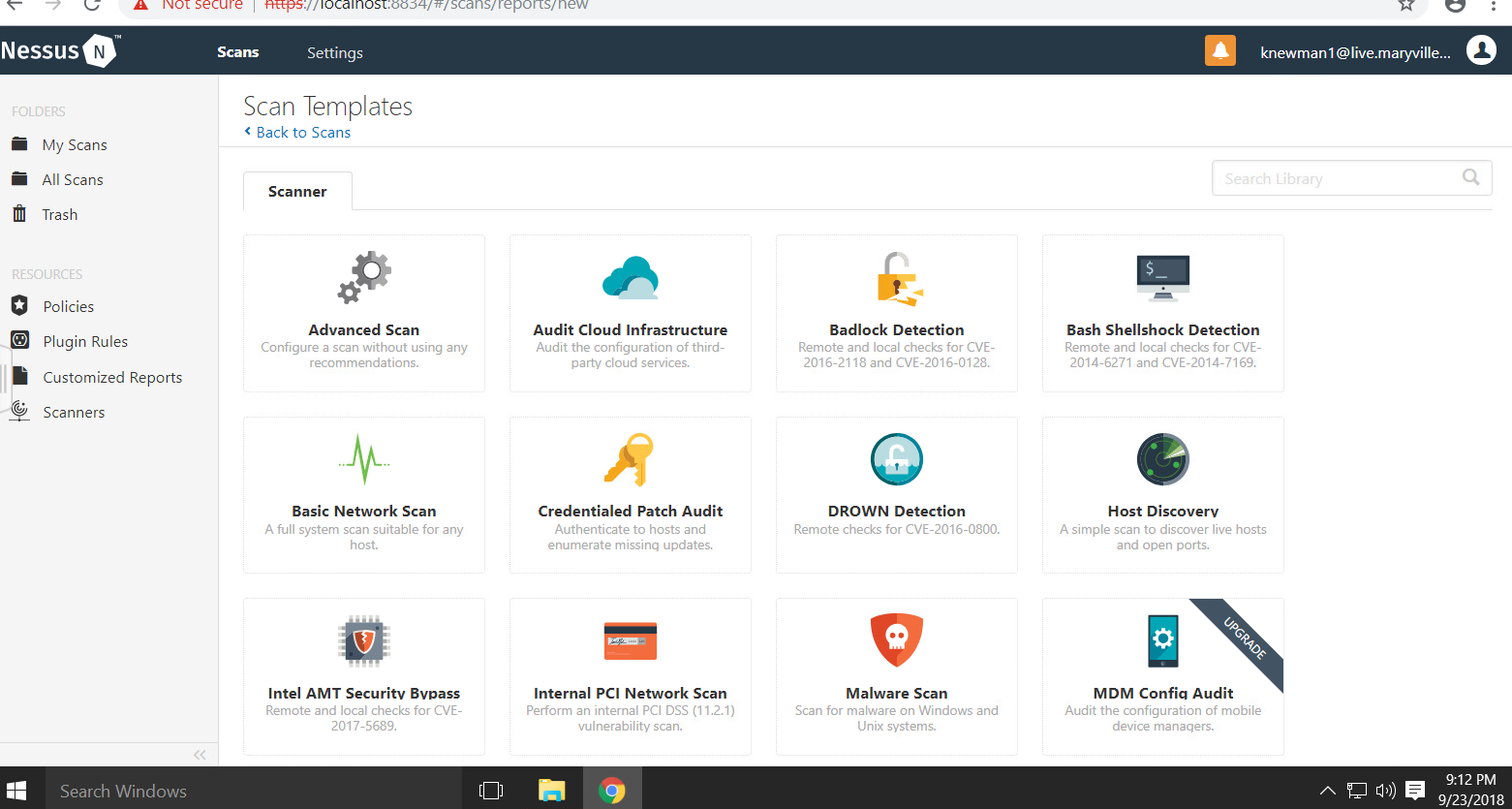
Step 11

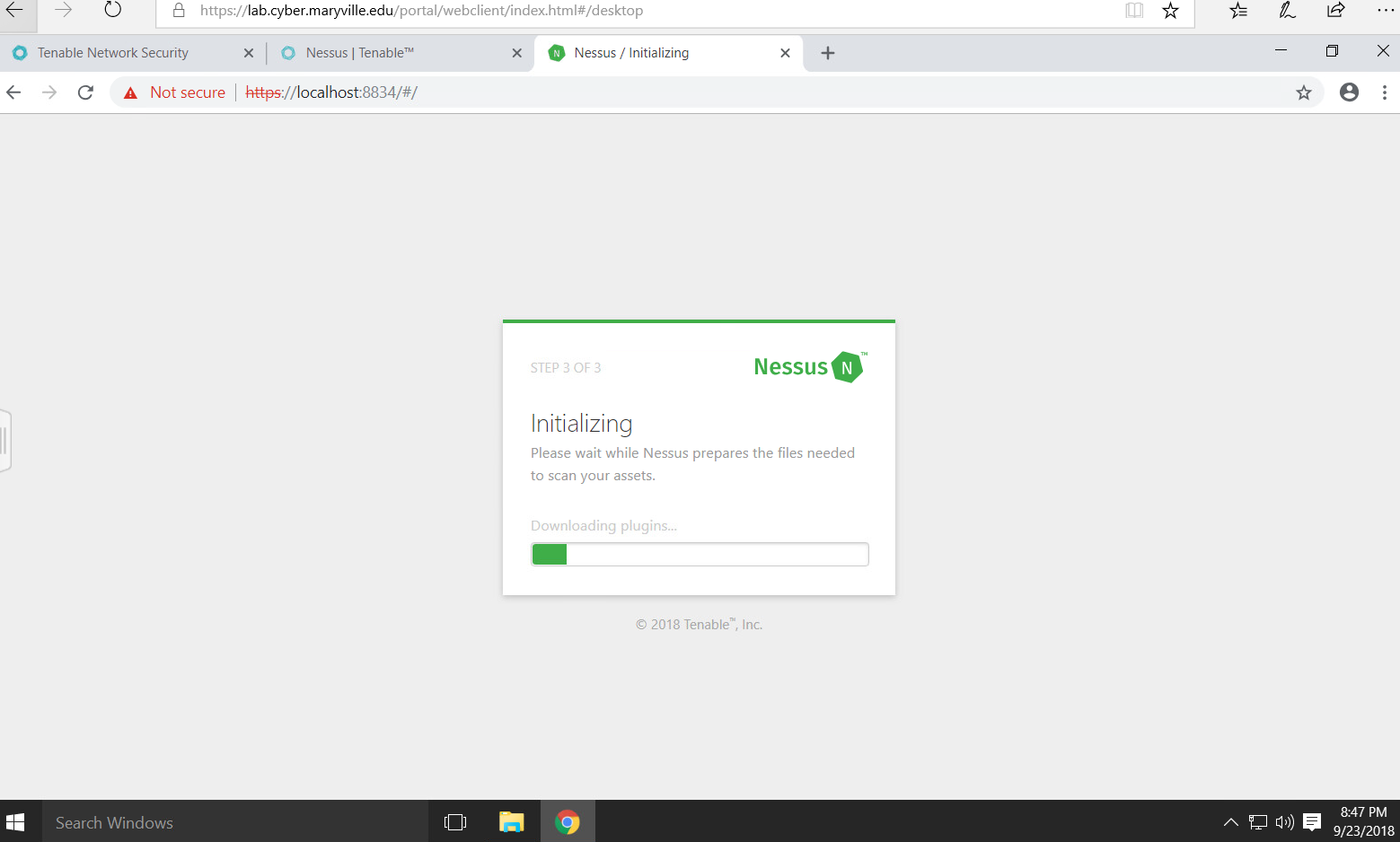


Step 12

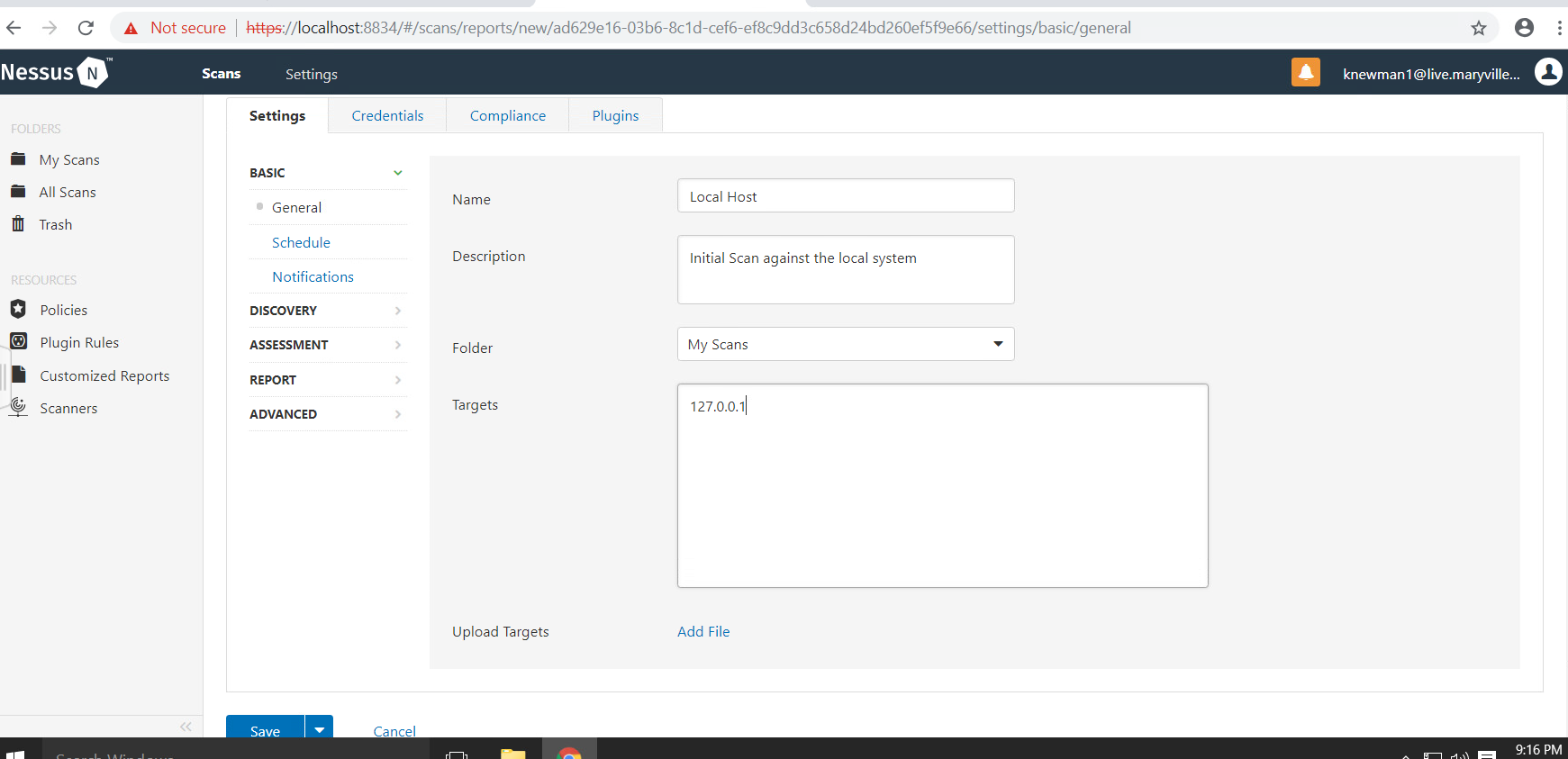
NMap couldn’t identify the system was blocked the ping probes.

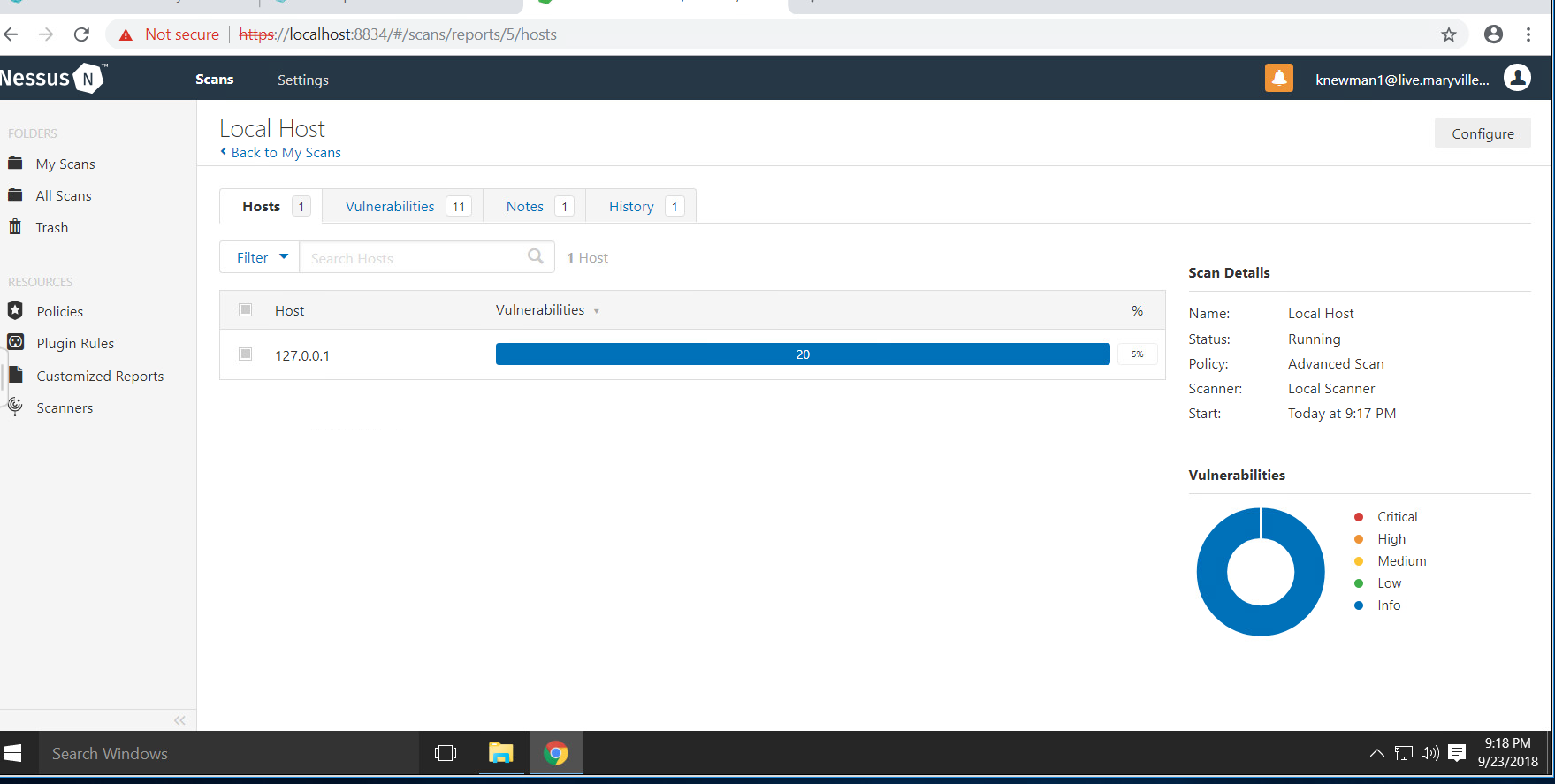
A vulnerability assessment identifies vulenarbilties in a system, and a penetration test is an stimulated attack on a system by an ethical hacker. A vunlerabity assessment can be a part of a penertration test.





An unauthenticated scan is a scan that done without anyone credentials, while authenticated scan requires user credentials.





I would use this tool to run scans on my network and I would run it at the end of every work week. I would also run the scans on all systems to avoid missing any vulnerabilities. . As penetration tester this tool could help cut down the time it takes to find vulnerabilities and weak spots in a targets system.

They type scan that was performed in step 2 is an unauthenticated scan.

