Exercise 1.1

https://www.sans.org/security-resources/policies

SANS

Login Join Community

Find Training | Live Training | Online Training | Programs | Resources | Vendor | About

Information Security Policy Templates

Welcome to the SANS Security Policy Resource page, a consensus research project of the SANS community. The ultimate goal of the project is to offer everything you need for rapid development and implementation of information security policies. You'll find a great set of resources posted here already, including policy templates for twenty-seven important security requirements.

Find the Policy Template You Need!

- **General**
- **Network Security**
- **Server Security**
- **Application Security**
- **Old/Retired**

There is no cost for using these resources. They were compiled to help the people attending SANS training programs, but security of the Internet depends on vigilance by all participants, so we are making this resource available to the entire community.

Find the Policy Template You Need!

General

Network Security

- Acquisition Assessment Policy
- Bluetooth Baseline Requirements Policy
- Remote Access Policy
- Remote Access Tools Policy
- Router and Switch Security Policy
- Wireless Communication Policy
- Wireless Communication Standard

Server Security

Application Security

Old/Retired

There is no cost for using these resources. They were compiled to help the people attending SANS training programs, but security of the Internet depends on vigilance by all participants, so we are making this resource available to the entire community.

Over the years a frequent request of SANS attendees has been for consensus policies, or at least security policy templates, that they can use to get their security programs updated to reflect 21st century requirements. While SANS has provided some policy resources for several years, we felt we could do more if we could get the community to work together. This page provides a vastly improved collection of policies and policy templates.

This page will continue to be a work in-progress and the policy templates will be living documents. We hope all of you who are SANS attendees will be willing and able to point out any problems in the models we post by emailing us at policies@sans.org. We also hope

Acquisition Assessment Policy

Defines responsibilities regarding corporate acquisitions, and defines the minimum requirements of an acquisition assessment to be completed by the Infosec Team.

Download Policy Template

- PDF
- DOC

Bluetooth Baseline Requirements Policy

Defines the minimum baseline standard for connecting Bluetooth enabled devices to the enterprise network or company owned devices. The intent of the minimum standard is to ensure sufficient protection Personally Identifiable Information (PII) and confidential company information.

Download Policy Template

- PDF
- DOC

Remote Access Policy

Defines standards for connecting to the organization's network from any host or network external to the organization.

Download Policy Template

- PDF
- DOC

https://www.sans.org/security-resources/policies/network-security/pdf/acquisition-assessment-policy

SANS **Consensus Policy Resource Community**

Acquisition Assessment Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: Updated and converted to new format June 2014

1. Overview

The process of integrating a newly acquired company can have a drastic impact on the security poster of either the parent company or the child company. The network and security infrastructure of both entities may vary greatly and the workforce of the new company may have a drastically different culture and tolerance to openness. The goal of the security acquisition assessment and integration process should include:

- Assess company's security landscape, posture, and policies
- Protect both <Company Name> and the acquired company from increased security risks
- Educate acquired company about <Company Name> policies and standard
- Adopt and implement <Company Name> Security Policies and Standards
- Integrate acquired company
- Continuous monitoring and auditing of the acquisition

2. Purpose

The purpose of this policy is to establish Infosec responsibilities regarding corporate acquisitions, and define the minimum security requirements of an Infosec acquisition assessment.

Old/Retired

- Analog/ISDN Line Security Policy
- Anti-Virus Guidelines
- Server Audit Policy
- Automatically Forwarded Email Policy
- Communications Equipment Policy
- Dial In Access Policy
- Extranet Policy
- Internet DMZ Equipment Policy
- Internet Usage Policy
- Mobile Device Encryption Policy
- Personal Communication Devices and Voicemail Policy
- Removable Media Policy
- Risk Assessment Policy
- Server Malware Protection Policy
- Social Engineering Awareness Policy
- DMZ Lab Security Policy
- Email Retention Policy
- Employee Internet Use Monitoring and Filtering Policy
- Lab Anti Virus Policy
- Mobile Employee Endpoint Responsibility Policy
- Remote Access Mobile Computing Storage
- Virtual Private Network Policy

There is no cost for using these resources. They were compiled to help the people attending SANS training programs, but security of the Internet depends on vigilance by all participants, so we are making this resource available to the entire community.

Risk Assessment Policy

Defines the requirement that the Infosec Team has the authority to perform periodic information security risk assessments (RAs) for purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Download Policy Template

- PDF
- DOC

Server Malware Protection Policy

Defines the requirements for which server systems are required to have anti-virus and/or anti-spyware applications.

Download Policy Template

- PDF
- DOC

Social Engineering Awareness Policy

Defines guidelines to provide awareness around the threat of social engineering and defines procedures when dealing with social engineering threats. Relevant content was added to the Acceptable Use Policy.

Download Policy Template

- PDF
- DOC

SANS **Consensus Policy Resource Community**

Risk Assessment Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Retired*

1. Overview

See Purpose.

2. Purpose

To empower Infosec to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

3. Scope

Risk assessments can be conducted on any entity within <Company Name> or any outside entity that has signed a *Third Party Agreement* with <Company Name>. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

4. Policy

The execution, development and implementation of remediation programs is the joint responsibility of Infosec and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Infosec Risk Assessment Team in the development of a remediation plan.

Find the Policy Template You Need!

General

- Acceptable Encryption Policy
- Acceptable Use Policy
- Clean Desk Policy
- Data Breach Response Policy
- Disaster Recovery Plan Policy
- Digital Signature Acceptance Policy
- Email Policy
- Ethics Policy
- Pandemic Response Planning Policy
- Password Construction Guidelines
- Password Protection Policy
- Security Response Plan Policy
- End User Encryption Key Protection Policy

Network Security

Server Security

Application Security

Old/Retired

Ethics Policy

Defines the guidelines and expectations of individuals within the company to demonstrate fair business practices and encourage a culture of openness and trust.

Download Policy Template

- PDF
- DOC

Pandemic Response Planning Policy

Defines the requirements for planning, preparation and performing exercises for pandemic disease outbreak over and above the normal business continuity and disaster recovery planning process.

Download Policy Template

- PDF
- DOC

Password Construction Guidelines

Defines the guidelines and best practices for the creation of strong passwords.

Download Policy Template

- PDF
- DOC

Password Protection Policy

Defines the standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Download Policy Template

- PDF
- DOC

1 of 4

SANS **Consensus Policy Resource Community**

Ethics Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

1. Overview

<Company Name> is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When <Company Name> addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

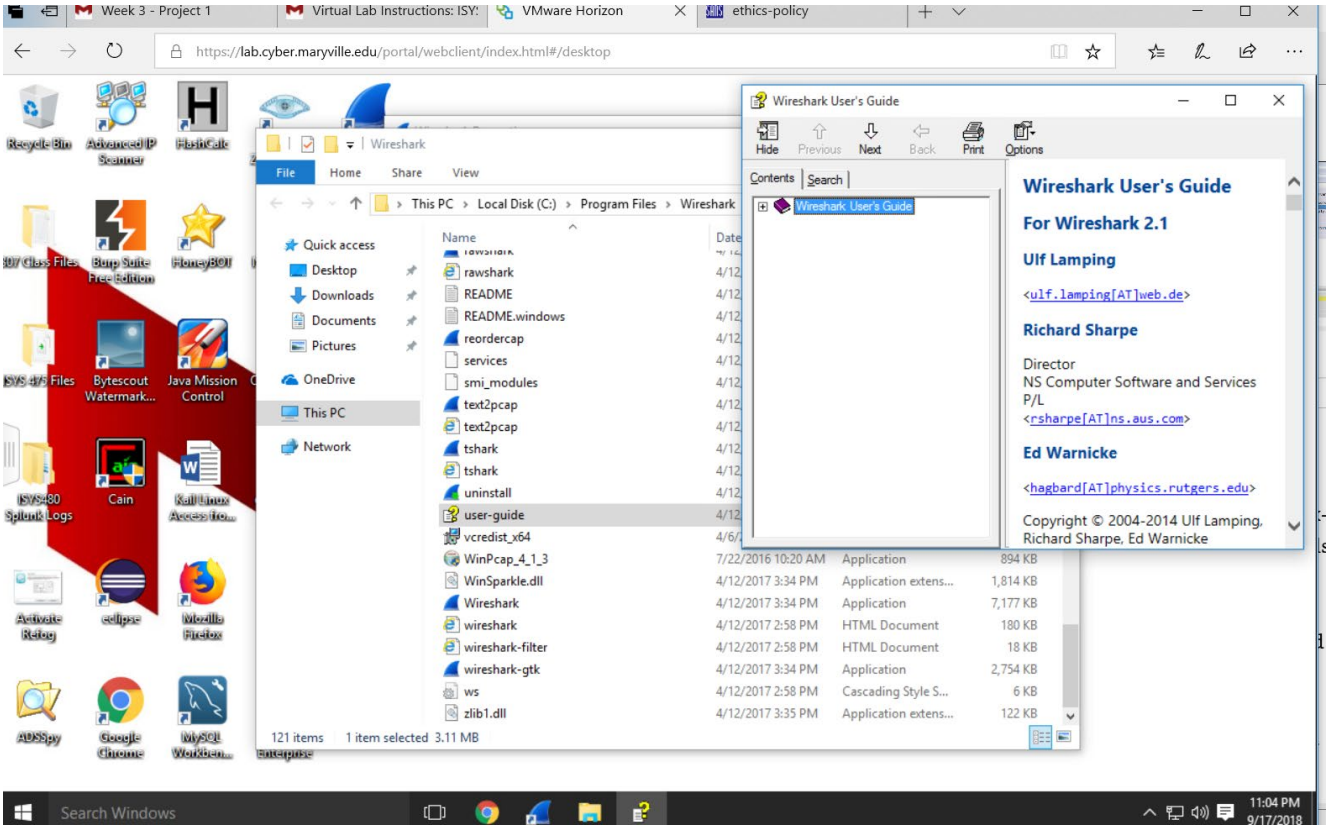
<Company Name> will not tolerate any wrongdoing or impropriety at any time. <Company name> will take the appropriate measures act quickly in correcting the issue if the ethical code is broken.

2. Purpose

The purpose of this policy is to establish a culture of openness, trust and to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct. Effective ethics is a team effort involving the participation and support of every <Company Name> employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

3. Scope

Exercise 2.1



imap.cap (libpcap) A short IMAP session using Mutt against an MSX server.

RawPacketIPv6Tunnel-UK6x.cap (libpcap) - Some IPv6 packets captured from the 'sit1' interface on Linux. The IPv6 packets are carried over the UK's UK6x network, but what makes this special, is the fact that it has a Link-Layer type of "Raw packet data" - which is something that you don't see everyday.

iseries.cap (IBM iSeries communications trace) FTP and Telnet traffic between two AS/400 LPARS.

FTPv6-1.cap (Microsoft Network Monitor) FTP packets (IPv6)

FTPv6-2.cap (Microsoft Network Monitor) Some more FTP packets (IPv6)

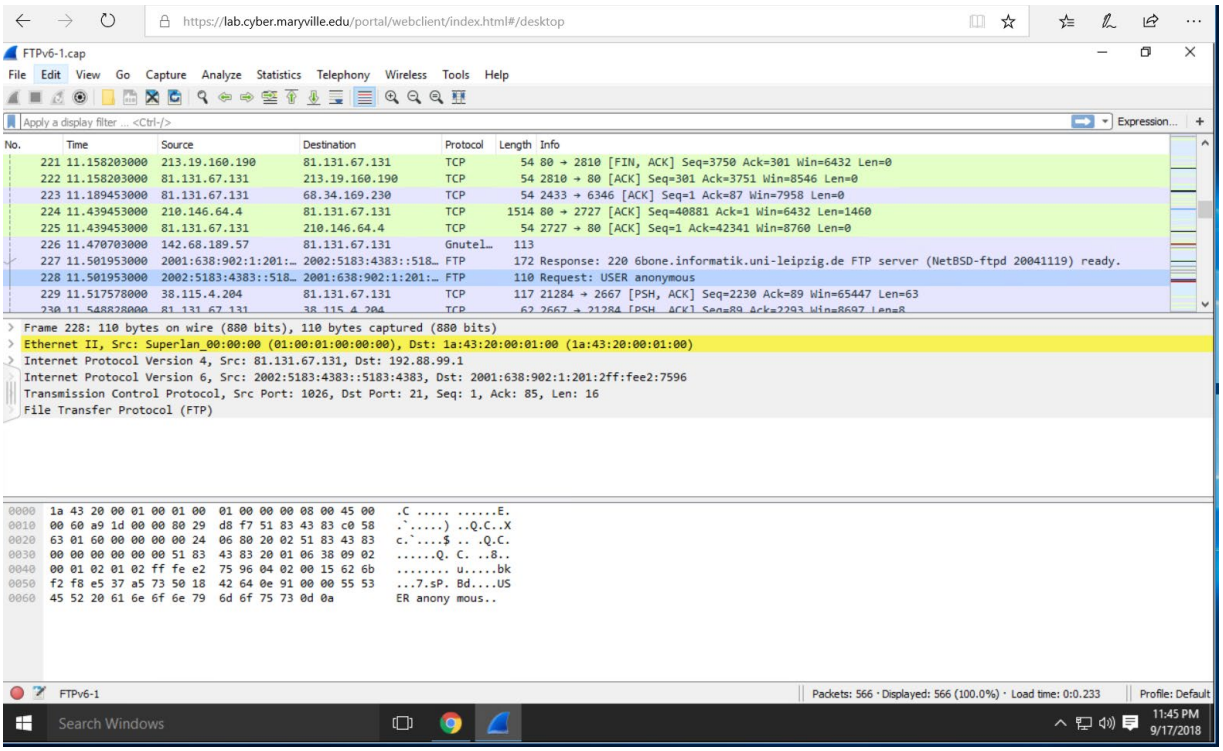
gearman.cap Gearman Protocol packets

isl-2-dot1q.cap (libpcap) A trace including both ISL and 802.1q-tagged Ethernet frames. Frames 1 through 381 represent traffic encapsulated using Cisco's ISL, frames 382-745 show traffic sent by the same switch after it had been reconfigured to support 802.1Q trunking.

kafka-testcases-v4.tar.gz (libpcap) Apache Kafka dissector testcases (generated with this scripts).

lacp1.pcap.gz (libpcap) Link Aggregation Control Protocol (LACP, IEEE 802.3ad) traffic.

linx-setup-pingpong-shutdown.pcap (libpcap) Successive setup of LINX on two hosts, exchange of packets and shutdown.


https://lab.cyber.maryville.edu/portal/webclient/index.html#/desktop
FTPv6-1.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
221 11.158203000 213.19.160.190 81.131.67.131 TCP 54 80 → 2810 [FIN, ACK] Seq=3750 Ack=301 Win=6432 Len=0
222 11.158203000 81.131.67.131 213.19.160.190 TCP 54 2810 → 80 [ACK] Seq=301 Ack=3751 Win=8546 Len=0
223 11.189453000 81.131.67.131 68.34.169.230 TCP 54 2433 → 6346 [ACK] Seq=1 Ack=87 Win=7958 Len=0
224 11.439453000 210.146.64.4 81.131.67.131 TCP 1514 80 → 2727 [ACK] Seq=40881 Ack=1 Win=6432 Len=1460
225 11.439453000 81.131.67.131 210.146.64.4 TCP 54 2727 → 80 [ACK] Seq=1 Ack=42341 Win=8760 Len=0
226 11.470703000 142.68.189.57 81.131.67.131 Gnutel… 113
227 11.501953000 2001:638:902:1:201:… 2002:5183:4383::518… FTP 172 Response: 220 6bone.informatik.uni-leipzig.de FTP server (NetBSD-ftpd 20041119) ready.
228 11.501953000 2002:5183:4383::518… 2001:638:902:1:201:… FTP 110 Request: USER anonymous
229 11.517578000 38.115.4.204 81.131.67.131 TCP 117 21284 → 2667 [PSH, ACK] Seq=2230 Ack=89 Win=65447 Len=63
Frame 228: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: Superlan_00:00:00 (01:00:01:00:00:00), Dst: 1a:43:20:00:01:00 (1a:43:20:00:01:00)
Internet Protocol Version 4, Src: 81.131.67.131, Dst: 192.88.99.1
Internet Protocol Version 6, Src: 2002:5183:4383::5183:4383, Dst: 2001:638:902:1:201:2ff:fee2:7596
Transmission Control Protocol, Src Port: 1026, Dst Port: 21, Seq: 1, Ack: 85, Len: 16
File Transfer Protocol (FTP)
0000 1a 43 20 00 01 00 01 00 01 00 00 00 08 00 45 00 .C ....E.
0010 00 60 a9 1d 00 00 80 29 d8 f7 51 83 43 83 c0 58 .`.....) ..Q.C..X
0020 63 01 60 00 00 00 00 24 06 80 20 02 51 83 43 83 c.`....$ .. .Q.C.
0030 00 00 00 00 00 00 51 83 43 83 20 01 06 38 09 02 .....Q. C. ..8..
0040 00 01 02 01 02 ff fe e2 75 96 04 02 00 15 62 6b ..... u.....bk
0050 f2 f8 e5 37 a5 73 50 18 42 64 0e 91 00 00 55 53 ...7.sP. Bd....US
0060 45 52 20 61 6e 6f 6e 79 6d 6f 75 73 0d 0a ER anony mous..
FTPv6-1
Packets: 566 · Displayed: 566 (100.0%) · Load time: 0:0.233
Profile: Default
Search Windows
11:45 PM
9/17/2018

Exercise 2.2

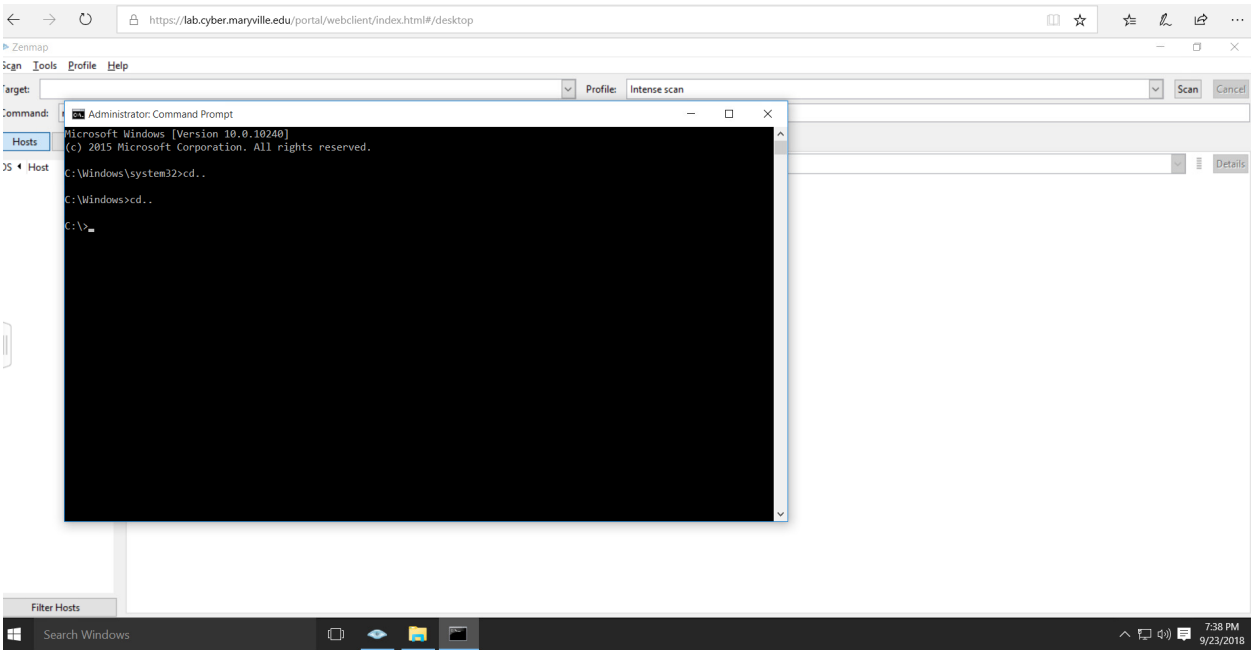
Layer	Layer Responsibility	Protocols, Ports, or Services	Potential Attacks
Application	Communication	SNMP, Telnet, DNS, SSH, SMTP	Password Attacks through Telnet or FTP
Host-to-host	Connection and connectionless communication	TCP and UDP	Session hijacking, connectionless, scanning communication
Internet	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

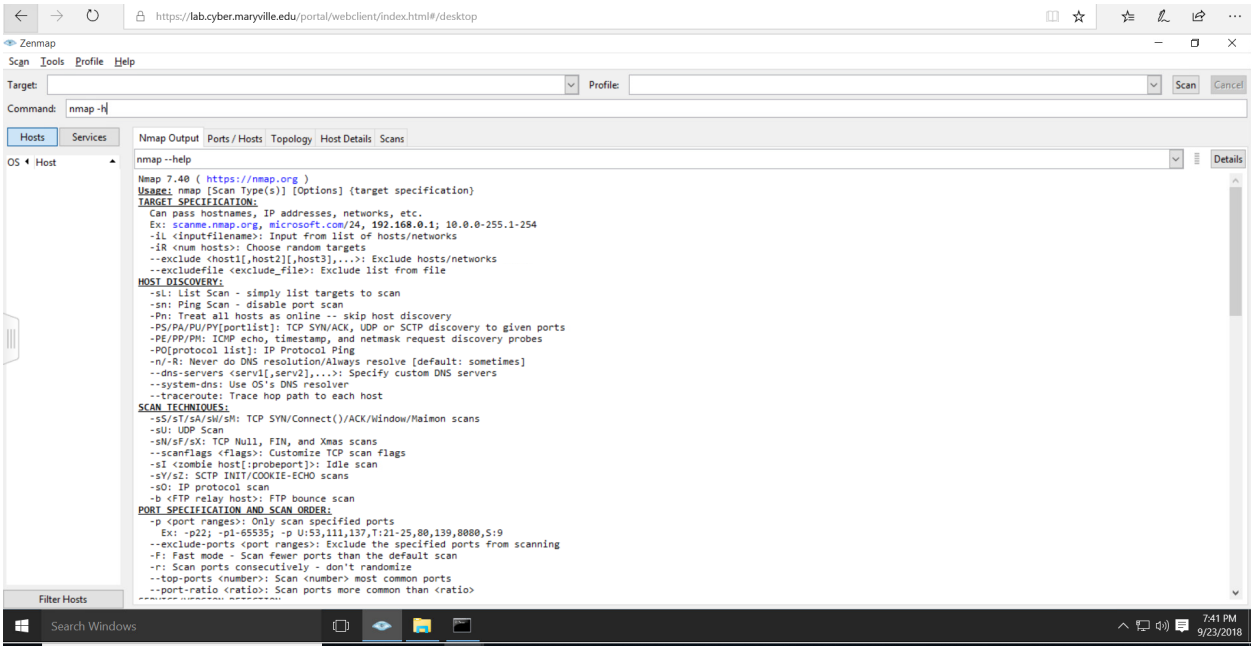
Domain Name	IP Address	Location	Contact Person	Address and Pone Number
Redriff.com	162.251.87.184	*Panama City*	Whois Foundation	Ramon Arias Avenue, Ropardi BBuilding, Office 3-C PO Box 0823-03015 (507)=836-5679
Examcram.com	159.182.72.15	*New Jersey*	Pearson Education, Inc.	200 Old Tappan Road Old Tappan, NJ. 07675 (201)-767-5000
Rackspace.com	72.3.246.59	*Texas*	Chris Hansell	1 Fanatical Place Windcrest, Texas, 78218 (210)-312-4000 Hostmaster@rackspace.com
Rutgers.edu	192.230.123.124	*New Jersey*	Office of Information Technology Telecommunications Division	96 Davidson Road Piscataway, NJ 08854 (848)-445-7541 netmanager@rutgers.edu

Exercise 3.2

Step 2



Step 3



Steps 4-7

NMap commands

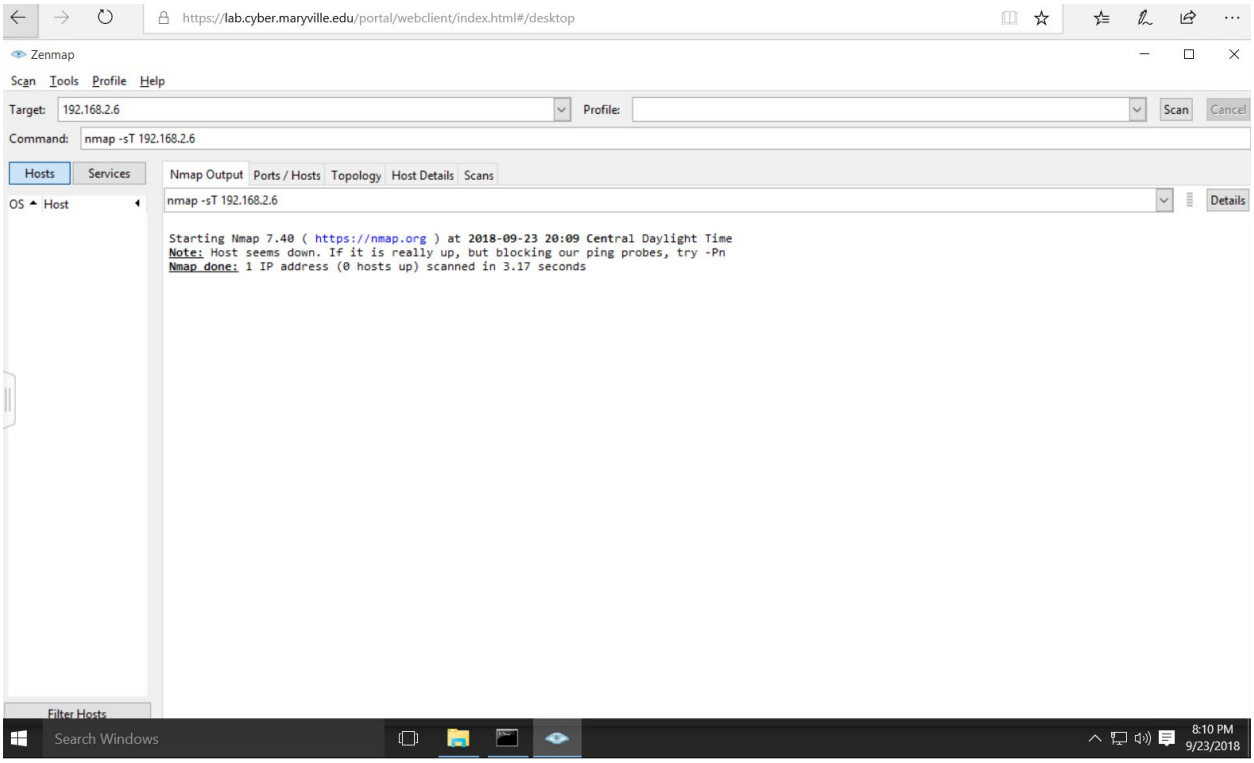
Full connect Scan: sT

Stealth Scan: sS

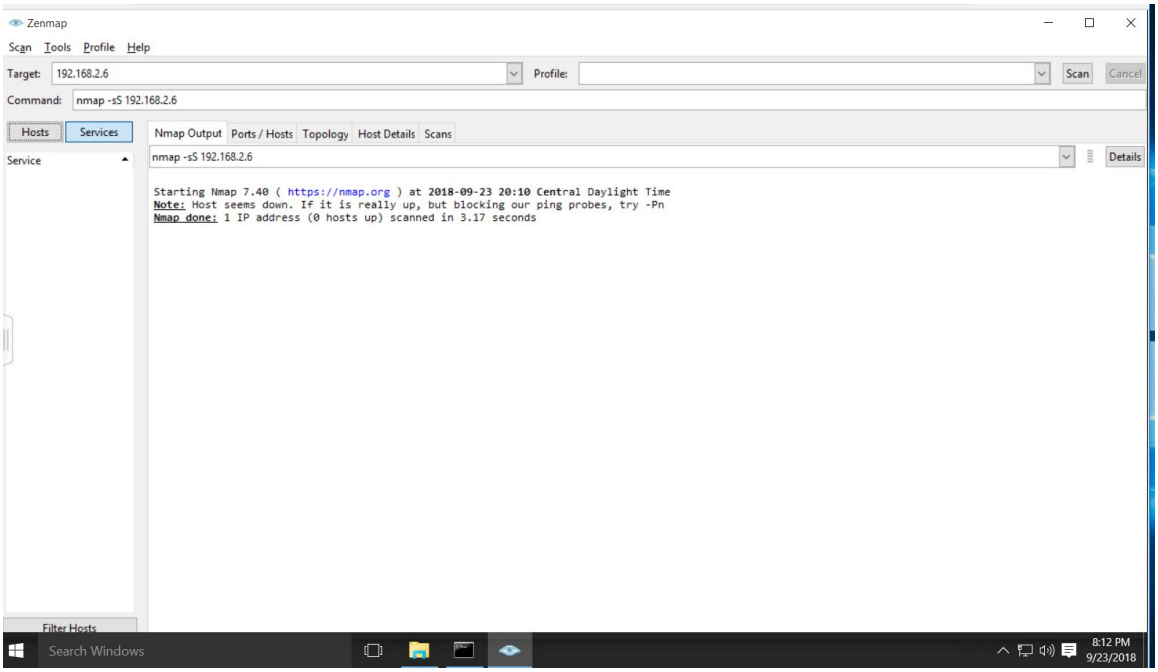
UDP Scan: sU

Fingerprint Scan: OS

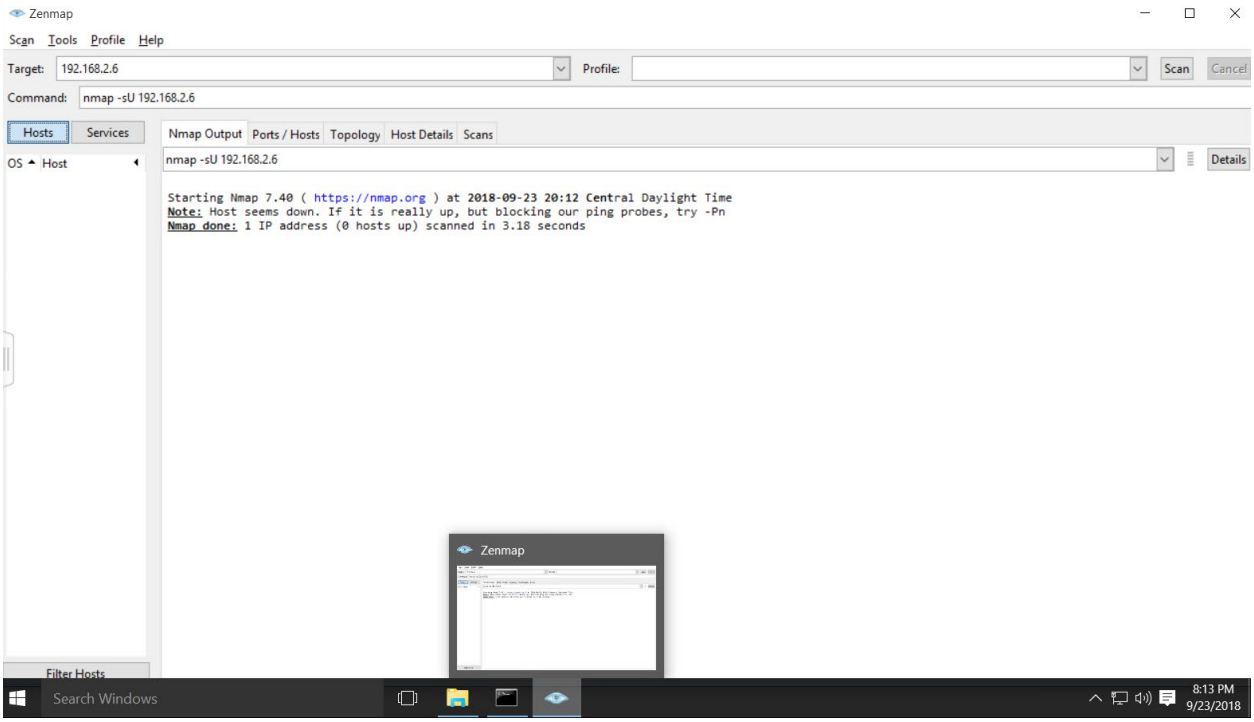
Step 8



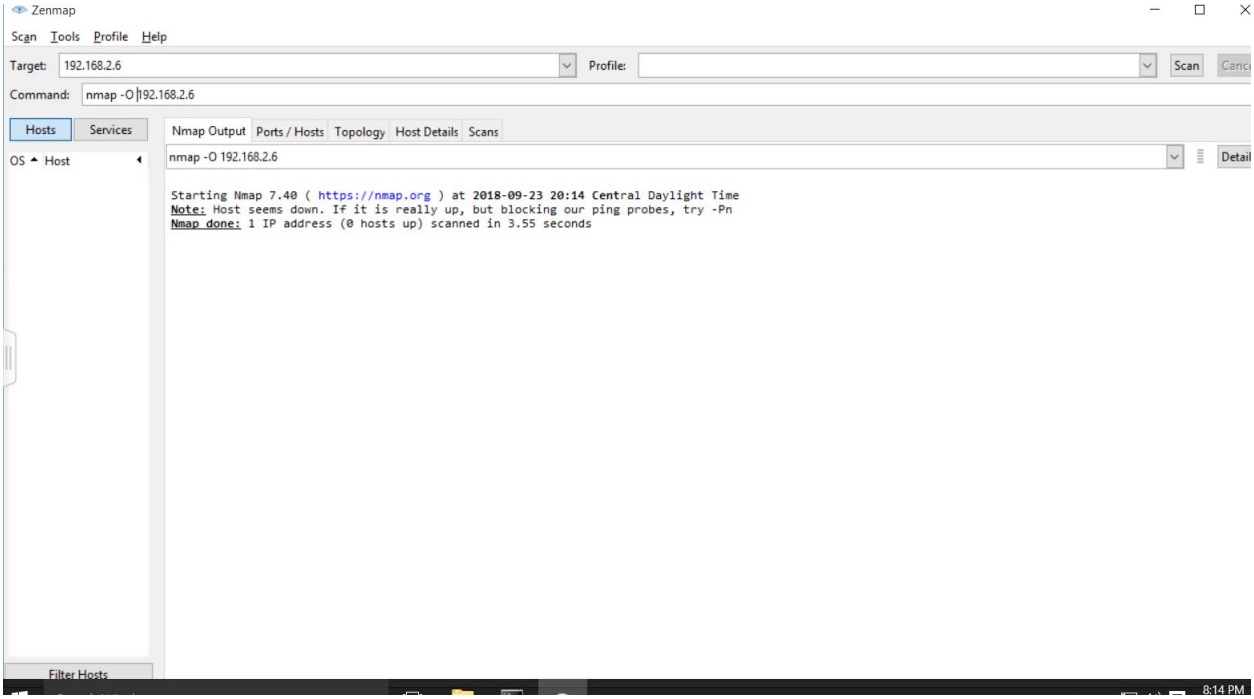
Step 9



Step 10



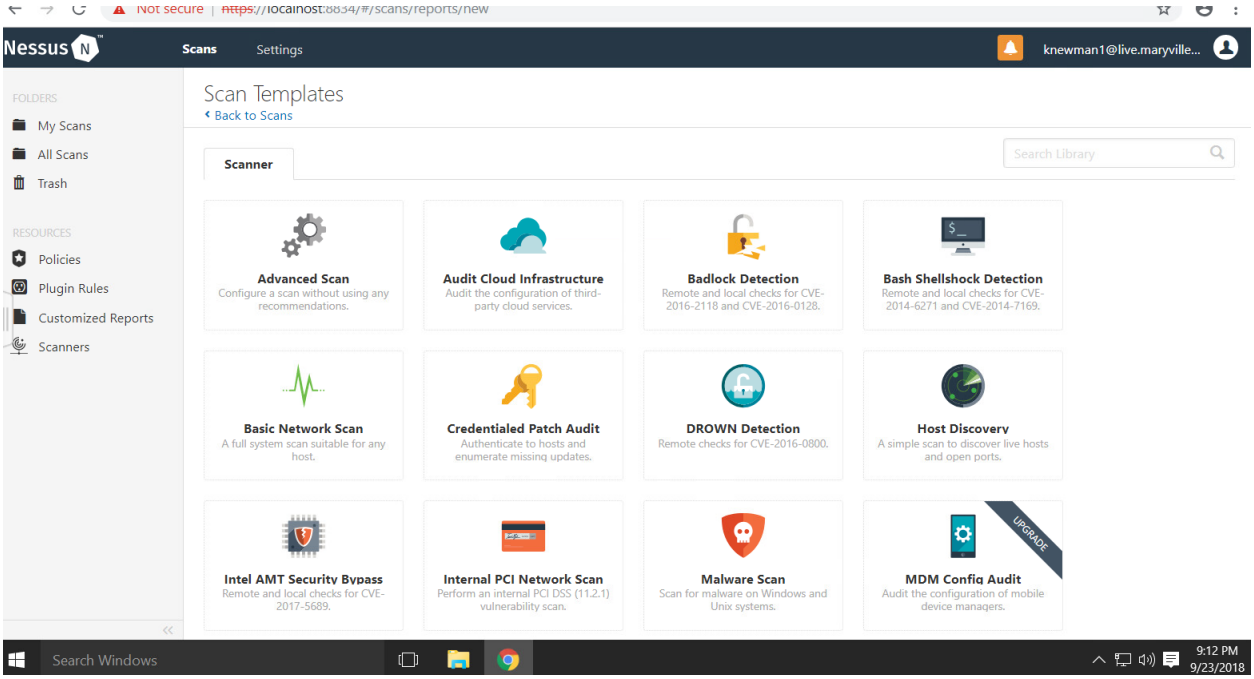
Step 11

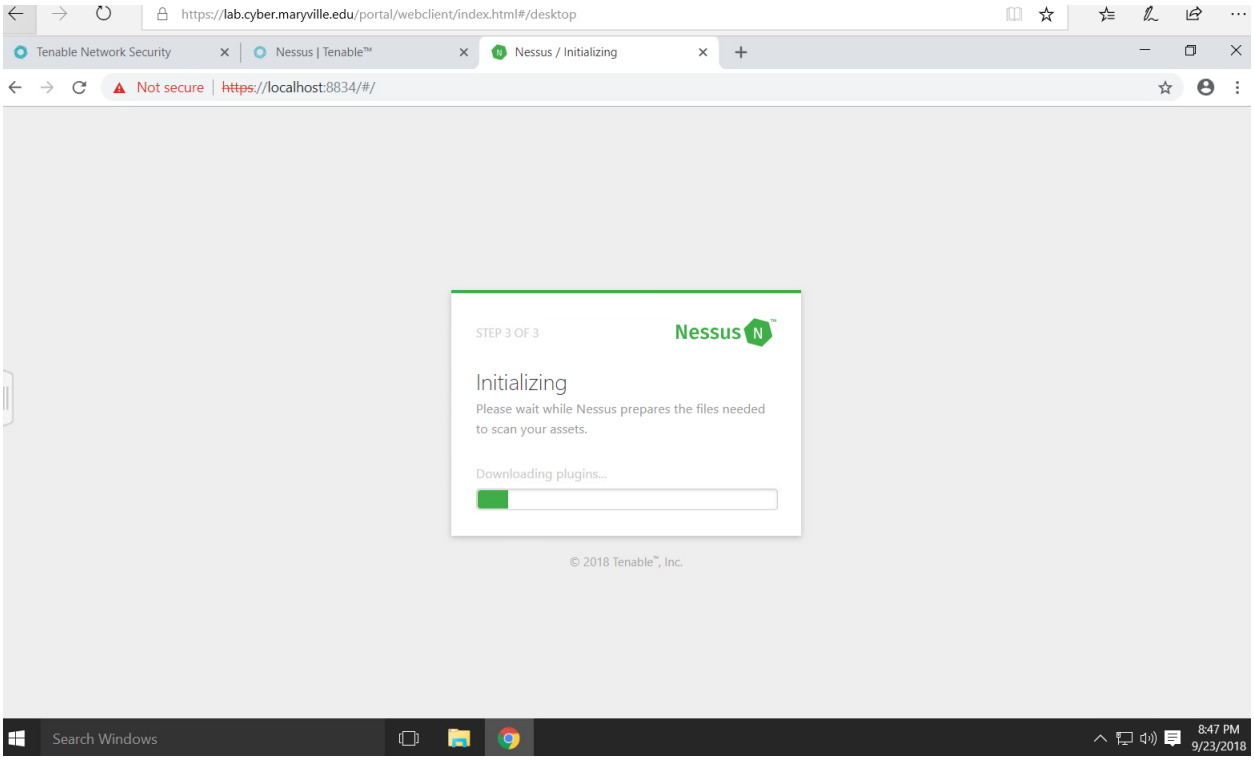


Step 12

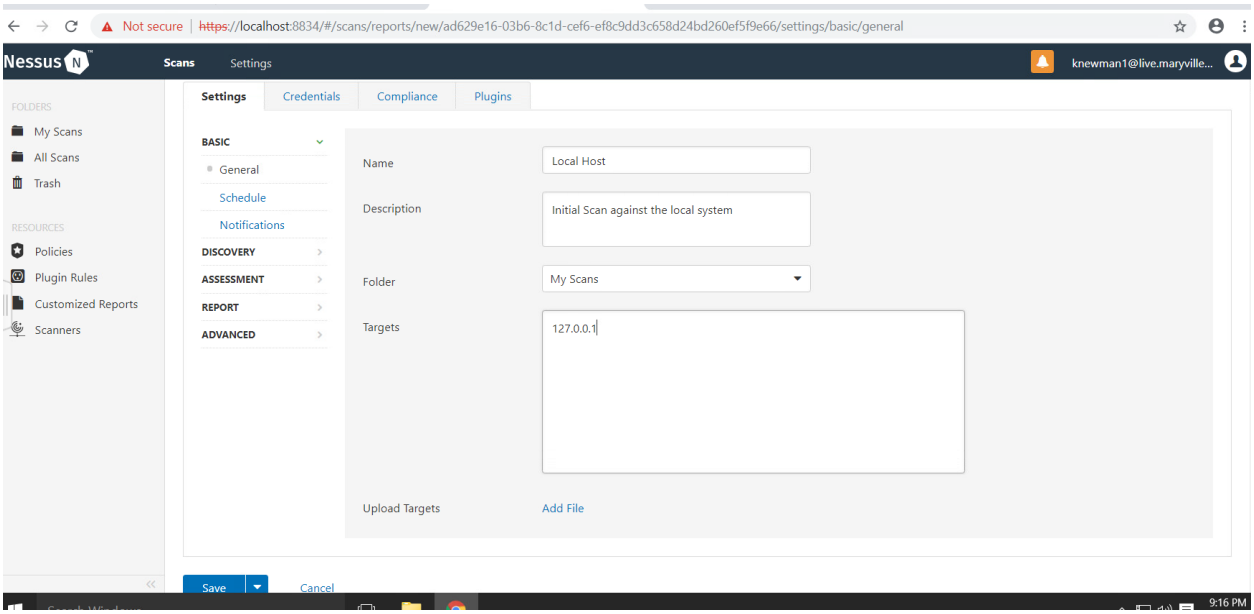
NMap couldn't identify the system was blocked the ping probes.

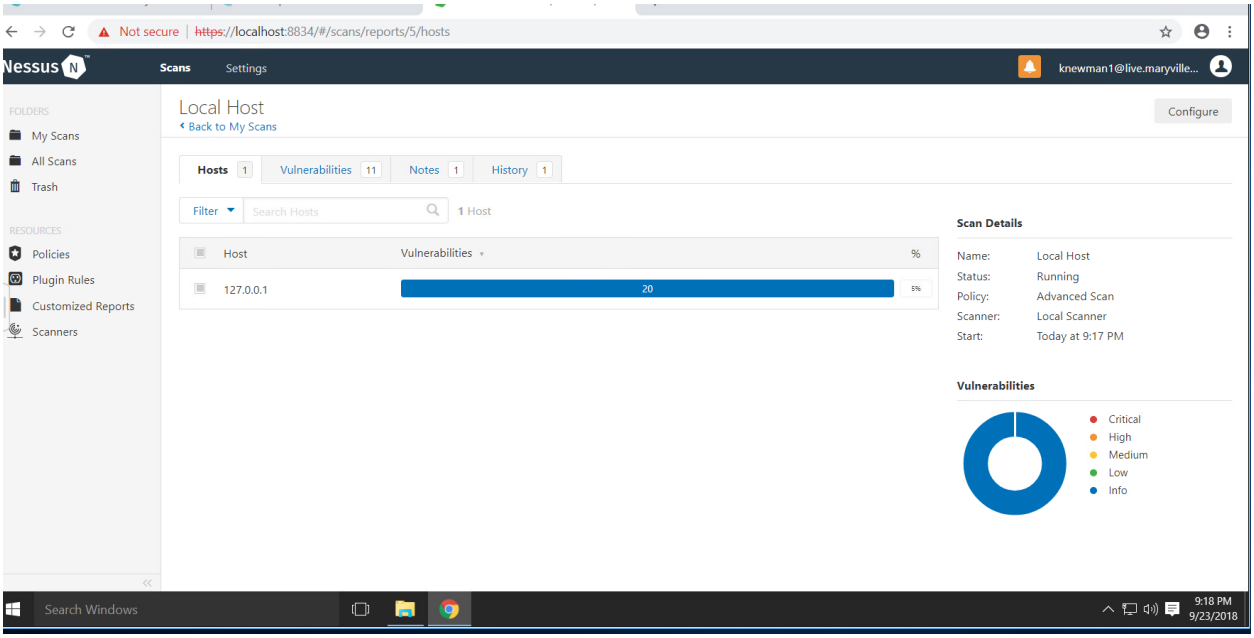
A vulnerability assessment identifies vulenarbilties in a system, and a penetration test is an stimulated attack on a system by an ethical hacker. A vunlerabity assessment can be a part of a penertration test.





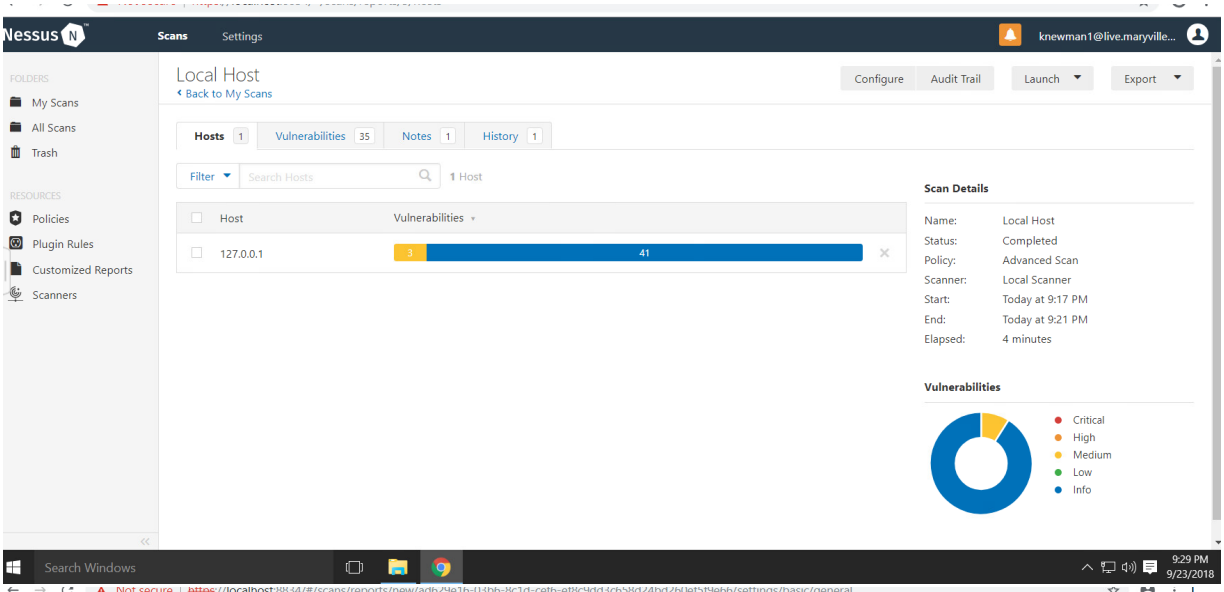
An unauthenticated scan is a scan that done without anyone credentials, while authenticated scan requires user credentials.

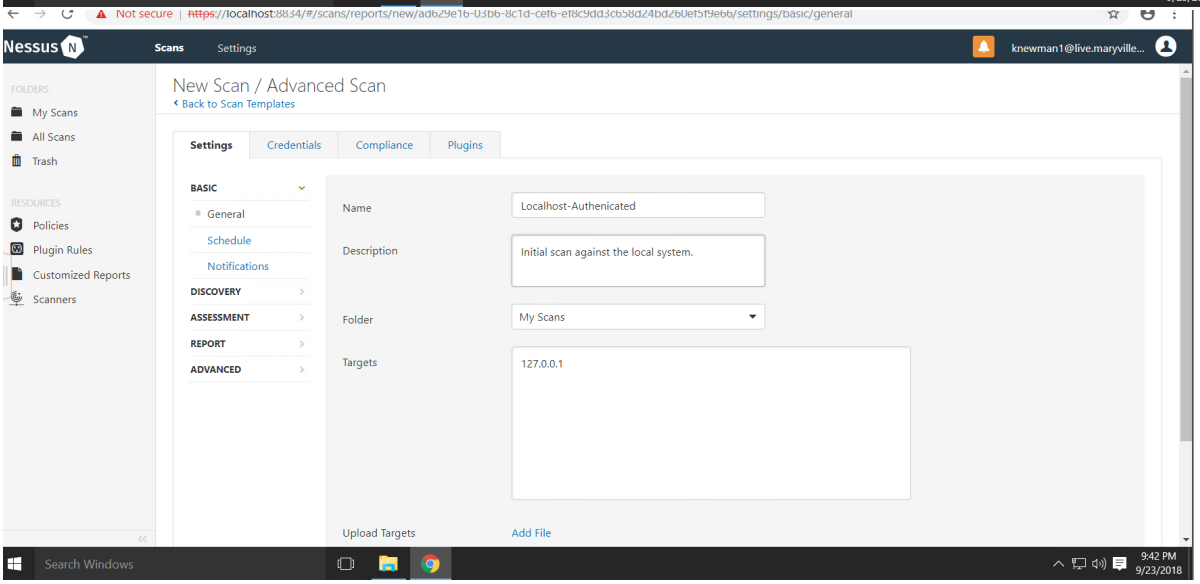


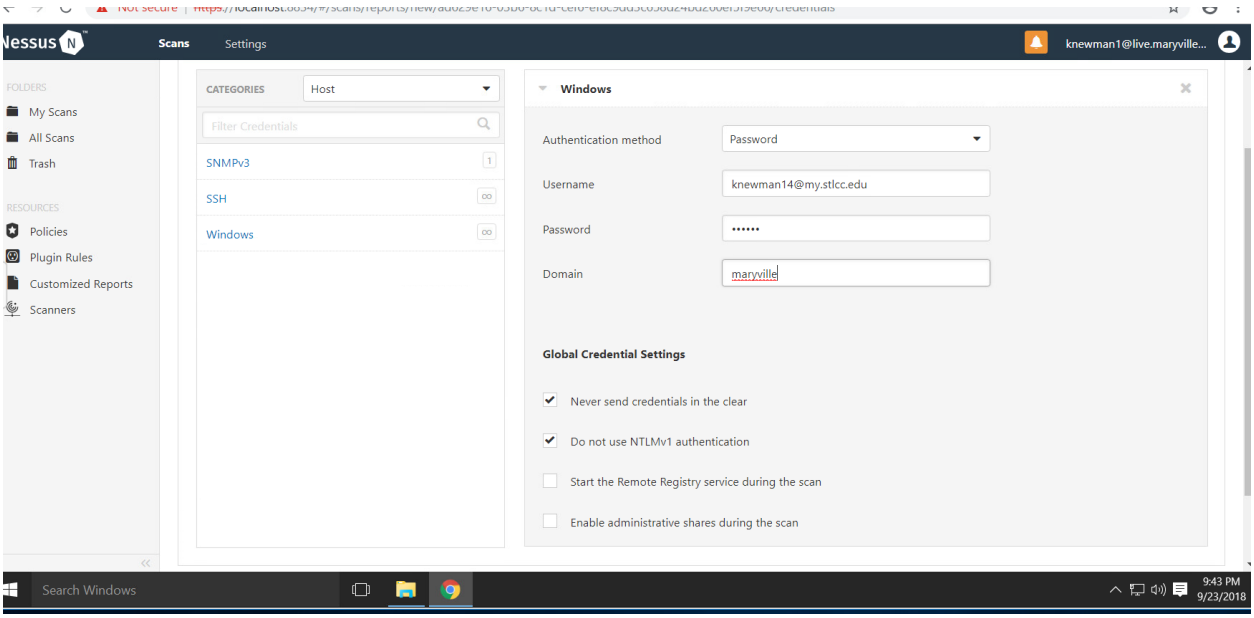


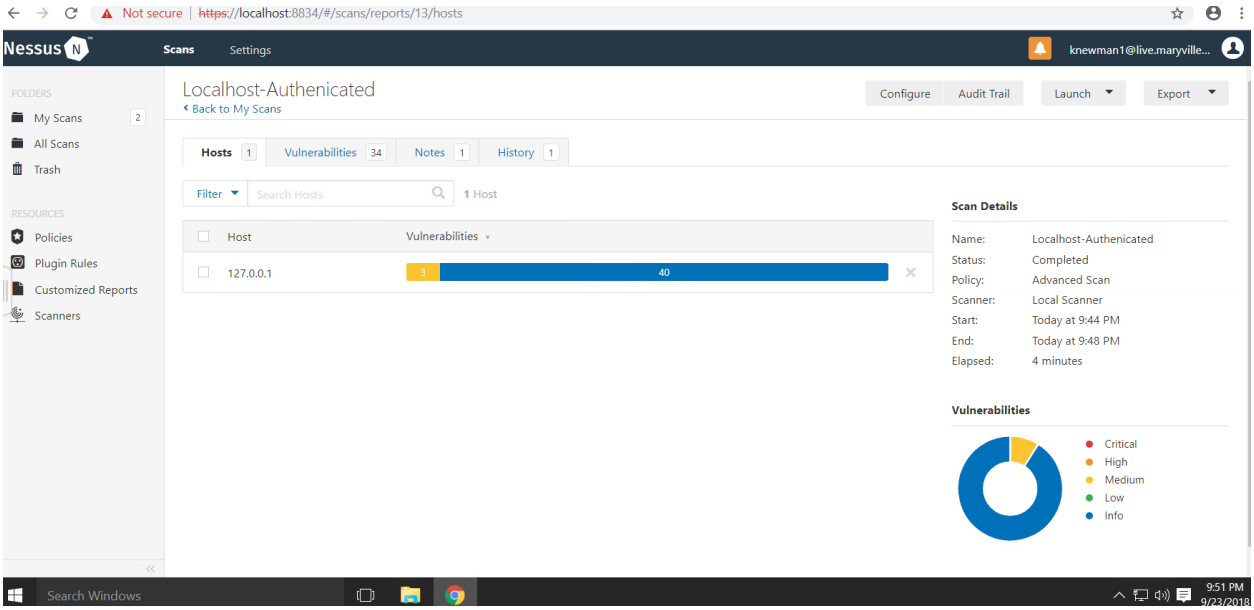
I would use this tool to run scans on my network and I would run it at the end of every work week. I would also run the scans on all systems to avoid missing any vulnerabilities. . As penetration tester this tool could help cut down the time it takes to find vulnerabilities and weak spots in a targets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

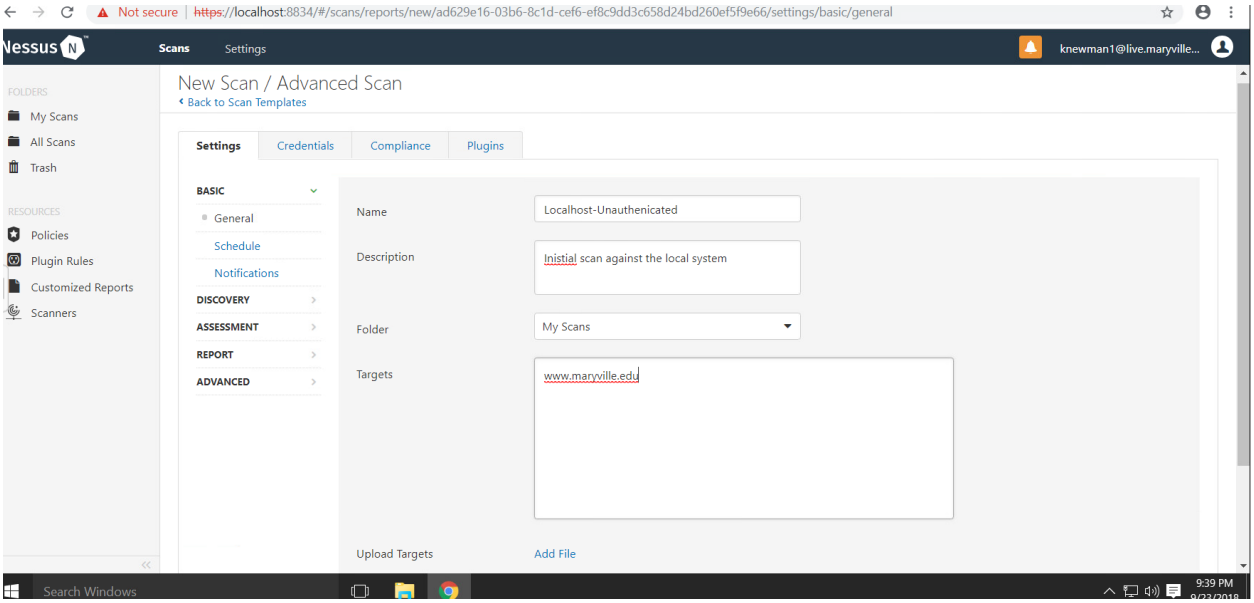
They type scan that was performed in step 2 is an unauthenticated scan.

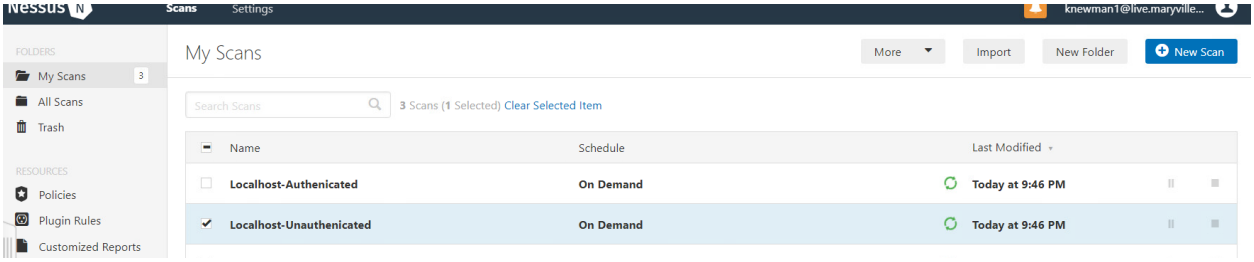

Nessus
Scans
Settings
knewman1@live.maryville...
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Local Host
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 35
Notes 1
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
127.0.0.1
3
41
Scan Details
Name: Local Host
Status: Completed
Policy: Advanced Scan
Scanner: Local Scanner
Start: Today at 9:17 PM
End: Today at 9:21 PM
Elapsed: 4 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Search Windows
9:29 PM
9/23/2018


Not secure
Nessus
Scans
Settings
knewman1@live.maryville...
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Localhost-Authenicated
Description
Initial scan against the local system.
Folder
My Scans
Targets
127.0.0.1
Upload Targets
Add File
Search Windows
9:42 PM
9/23/2018


Nessus
Scans
Settings
knewman1@live.maryville...
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
CATEGORIES
Host
Filter Credentials
SNMPv3
SSH
Windows
Windows
Authentication method
Password
Username
knewman14@my.stlcc.edu
Password
Domain
maryville
Global Credential Settings
Never send credentials in the clear
Do not use NTLMv1 authentication
Start the Remote Registry service during the scan
Enable administrative shares during the scan
Search Windows
9:43 PM
9/23/2018


Not secure
https://localhost:8834/#/scans/reports/13/hosts
Nessus
Scans
Settings
knewman1@live.maryville...
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Localhost-Authenicated
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 34
Notes 1
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
127.0.0.1
3
40
Scan Details
Name: Localhost-Authenicated
Status: Completed
Policy: Advanced Scan
Scanner: Local Scanner
Start: Today at 9:44 PM
End: Today at 9:48 PM
Elapsed: 4 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Search Windows
9:51 PM
9/23/2018


Not secure | https://localhost:8834/#/scans/reports/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/basic/general
Nessus
Scans
Settings
knewman1@live.maryville...
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Localhost-Unauthenicated
Description
Inistial scan against the local system
Folder
My Scans
Targets
www.maryville.edu
Upload Targets
Add File
Search Windows
9:39 PM


Nessus
Scans
Settings
knewman1@live.maryville...
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
My Scans
More
Import
New Folder
New Scan
Search Scans
3 Scans (1 Selected) Clear Selected Item
Name
Schedule
Last Modified
Localhost-Authenicated
On Demand
Today at 9:46 PM
Localhost-Unauthenicated
On Demand
Today at 9:46 PM