

Colby Heilner

Professor Torres

11/27

IT 120

Lab 13

Part A:

Click on the below link and play the Targeted Attack Game. Screenshot your final results:

- <http://targetedattacks.trendmicro.com/>(Links to an external site.) (Links to an external site.)



Part B: [Netlab1 Security+v3](#)Links to an external site.

Ensure HIPAA compliance against the lab environment (5 **checks** from the provided HIPAA checklist). Use the **HIPAA checklist**. Screenshot what you did.

1.

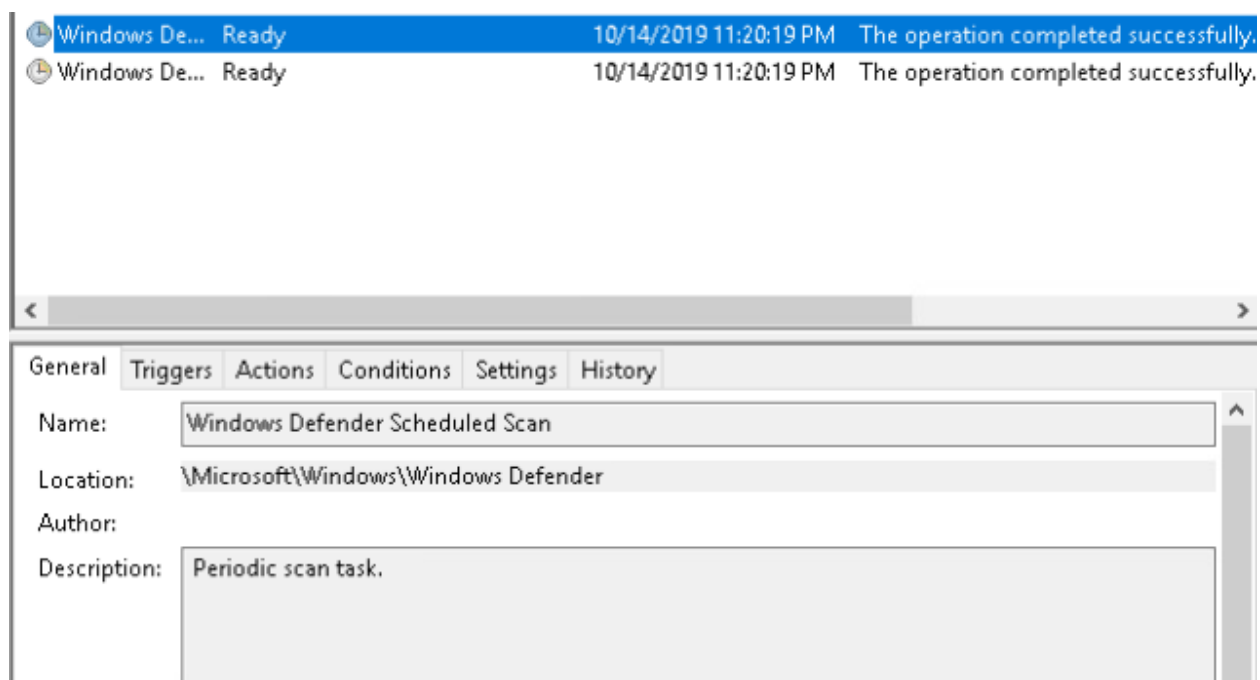
Security Awareness and Training §164.308(a)(5)(i)	Protection from Malicious Software	Are procedures in place to make sure virus checking software is installed and running on all computer systems within the organization?	Virus Protection will be required on computer system(s), that can detect virus programs that attach to other files or programs to replicate, a code fragment that can reproduce by attaching itself to another program, or an embedded code that can copy or insert itself into one or more programs.
---------------------------------------------------	------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

To fix this I can make sure any computer that connects to our internal network has the built-in Windows firewall as well as UFW or Iptables rules set. I can do this via my domain controller for windows. This is normally where companies would use Sophos or CrowdStrike to maintain their Linux infrastructure.

2.

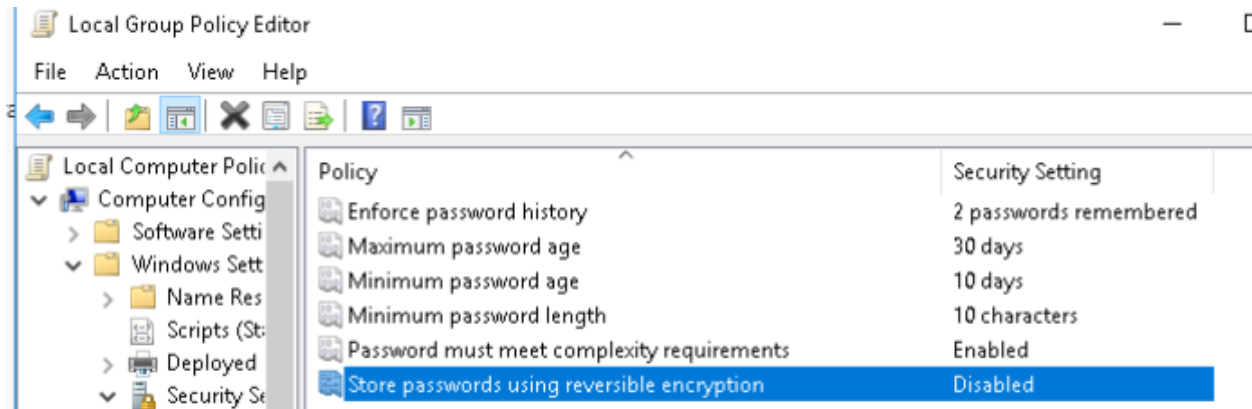
Security Awareness and Training §164.308(a)(5)(i)	Protection from Malicious Software	Do the procedures call for periodic scanning for viruses? How often is the virus software configured to scan for viruses?	Accurate virus protection is based on the constancy of updating definition files, and scanning.
---------------------------------------------------	------------------------------------	---------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------

I went into my windows pc and did this setting, make sure this is enabled



<p>Security Awareness and Training §164.308(a)(5)(i)</p>	<p>Password Management</p>	<p>What password guidelines exist and what procedures are followed to ensure the user makes a good selection?</p>
--------------------------------------------------------------	----------------------------	-------------------------------------------------------------------------------------------------------------------






















3.



4.

<p>Access Control §164.312(a)(1)</p>	<p>Unique User Identification</p>	<p>Are unique user id(s) in place/use (network and application)? If yes, for which systems and are they governed by written security procedures?</p>	<p>Unique user IDs are a combination name/number assigned to identify and track individuals.</p>
------------------------------------------	-----------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------

Use different usernames for the accounts you make and document them. Looks good to me

 Administrator	User	Built-in account for ad...
 Administrator2	User	
 Allowed RO...	Security Group...	Members in this group c...
 Cert Publish...	Security Group...	Members of this group ...
 Cloneable D...	Security Group...	Members of this group t...
 Denied ROD...	Security Group...	Members in this group c...
 DnsAdmins	Security Group...	DNS Administrators Gro...
 DnsUpdateP...	Security Group...	DNS clients who are per...
 Domain Ad...	Security Group...	Designated administrato...
 Domain Co...	Security Group...	All workstations and ser...
 Domain Con...	Security Group...	All domain controllers i...
 Domain Gue...	Security Group...	All domain guests
 Domain Users	Security Group...	All domain users
 Enterprise A...	Security Group...	Designated administrato...
 Enterprise R...	Security Group...	Members of this group ...
 Group Polic...	Security Group...	Members in this group c...
 Guest	User	Built-in account for gue...
 lab user	User	
 lab users	Security Group...	
 lab2 user	User	
 Protected Us...	Security Group...	Members of this group ...

5.

Access Control §164.312(a)(1)	Automatic Logoff	Are controls in place and configured to allow for automatic logoffs (network and application)?	Applications will be required to provide automatic user logoff (example: 15 minutes).
----------------------------------	------------------	------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------

This is another simple one with domain controller

The three I enabled are to set to screen saver after certain time and then require a password to wake it back up

Personalization

Enable screen saver

Edit [policy setting](#)

Requirements:
At least Windows 2000 Service Pack 1

Description:
Enables desktop screen savers.

If you disable this setting, screen savers do not run. Also, this setting disables the Screen Saver dialog in the Personalization or Display Control Panel. As a result, users cannot change the screen saver options.

If you do not configure it, this setting has no effect on the system.

If you enable it, a screen saver runs, provided the following two

Setting	State
Prevent changing color scheme	Not configured
Prevent changing theme	Not configured
Prevent changing visual style for windows and buttons	Not configured
Enable screen saver	Enabled
Prohibit selection of visual style font size	Not configured
Prevent changing color and appearance	Not configured
Prevent changing desktop background	Not configured
Prevent changing desktop icons	Not configured
Prevent changing mouse pointers	Not configured
Prevent changing screen saver	Not configured
Prevent changing sounds	Not configured
Password protect the screen saver	Enabled
Screen saver timeout	Enabled
Force specific screen saver	Not configured
Load a specific theme	Not configured
Force a specific visual style file or force Windows Classic	Not configured

- There is a HIPAA Assessment Checklist in the files area, inside class files.

Part C: Security+v3

Execute a PCI Compliance Audit against pfSense firewall in the lab. Utilize the **PCI Prioritized Approach**, (See Word Document). against the pfSense firewall. For the Audit, you were **ONLY** provided access to the firewall and the Firewall policy (The firewall policy is in the files folder -"Firewall Policy Homework). Only audit 10 areas

- There is a link to the PCI documentation within the reference area (Prioritized Approach for PCI DSS)
- [Firewall Policy](#)

1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks. Applicability Notes A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.	1	Yes	
1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: <ul style="list-style-type: none"> Shows all account data flows across systems and networks. Updated as needed upon changes to the environment. Applicability Notes A data-flow diagram(s) or other technical or topological solution that identifies flows of account data across systems and networks can be used to meet this requirement.	1	NO	Connection shown but not up-to date and no data flow shown.
1.2.5 All services, protocols and ports allowed are identified, approved, and have a defined business need.	2	No	
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	2	No	

1.3.1 Inbound traffic to the CDE is restricted as follows: <ul style="list-style-type: none"> To only traffic that is necessary, All other traffic is specifically denied. 	2	Yes
1.3.2 Outbound traffic from the CDE is restricted as follows: <ul style="list-style-type: none"> To only traffic that is necessary, All other traffic is specifically denied. 	2	Yes

If you have your firewall rules backed up this, it is good to delete the Auto lockout rule and replace it with your admins IP so that only they can access it. I will be doing this in our upcoming challenge.

I assume this means using things like https and not http so in this case it does not comply

2.2.7 All non-console administrative access is encrypted using strong cryptography. Applicability Notes This includes administrative access via browser-based interfaces and application programming interfaces (APIs).	2	No
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---	----

These are simple but important you need to make sure you don't just keep a bunch of copies of you keys AND make sure you don't let a lot of people with different security levels have access to them.

3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	5	Yes
3.6.1.4 Cryptographic keys are stored in the fewest possible locations.	5	Yes

Finally this is just saying that my workers like janitors and other people should not be able to login to high level servers and desktops. As long as it is not required for them to perform their job.

7.2.1 An access control model is defined and includes granting access as follows: <ul style="list-style-type: none"> • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. 	4	Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---	-----

Part D: NDG Security+v3 Lab 01

LAB PREP

Log on to all systems

Win16/Win12R2

Configure two admin accounts, Batman and Wonderwoman

Enable/open a port for RDP

```
C:\Users\Administrator>net localgroup administrators superman /add
The command completed successfully.

C:\Users\Administrator>net localgroup administrators batman /add
The command completed successfully.
```

DVL, Ubuntu

Configure two accounts, Superman and theFlash

Enable/open a port for SSH

pfSense

USING NAT:

Configure ports 3389 to Win16

Configure ports 3390 to Win12R2

Configure ports 22 to DVL port 22

Configure ports 2222 to Ubuntu port 22





















```

Starting Nmap 6.47 ( http://nmap.org ) at 2024-11-27 17:
Nmap scan report for 203.0.113.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
2222/tcp  open  EtherNet/IP-1
3389/tcp  open  ms-wbt-server
3390/tcp  open  dsc
MAC Address: 00:50:56:9C:D3:F6 (VMware)

```

ENABLE LOGGING

ENABLED!

		IPv4 TCP	*	*	192.168.1.50	2222	*	none		NAT UBUNTU			
		IPv4 TCP	*	*	10.1.1.10	22 (SSH)	*	none		NAT DVL			
		IPv4 TCP	*	*	10.1.1.12	3390	*	none		NAT 12R2			
		IPv4 TCP	*	*	192.168.1.100	3389 (MS RDP)	*	none		NAT WIN16			

○ From KALI

- RDP to Win16 as admin and Superman
 - RDP to Win12R2 as admin and Wonderwoman
 - SSH to DVL as superman and batman
 - SSH to Ubuntu as Wonderwoman and theflash
- Here is all my connection somewhat organized


```
File Edit View Search Terminal Tabs Help
16 x 16 x K12 x K12 x DVL x DVL x ubuntu x ubuntu
Permission denied, please try again.
superman@192.168.1.50's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

0 packages can be updated.
0 updates are security updates.

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2017.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

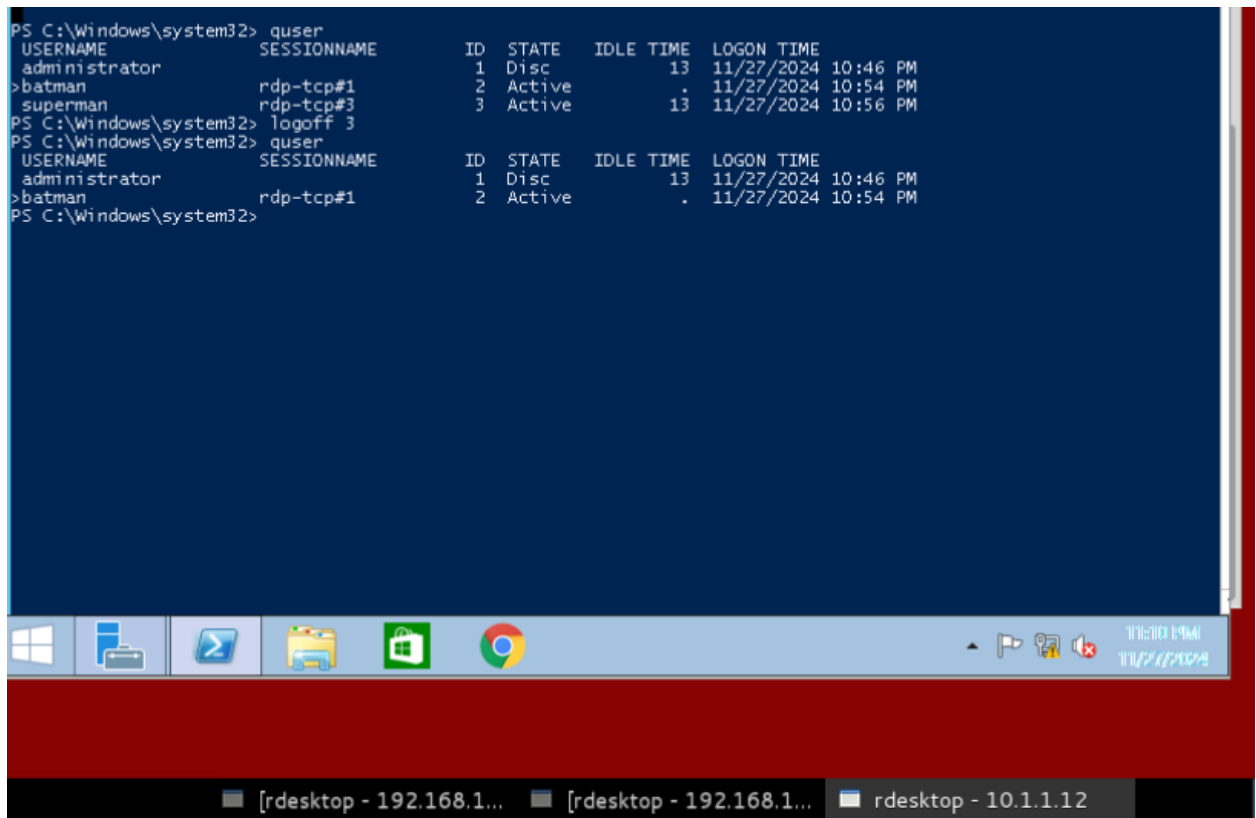
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

superman@Ubuntu:~$
```

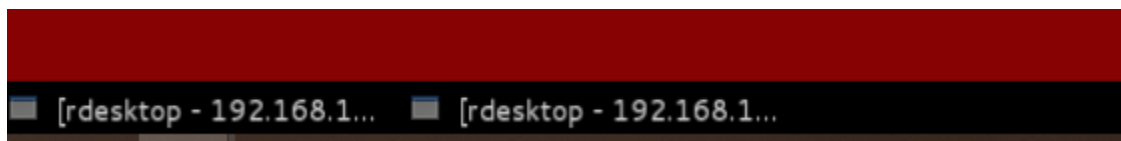
- Attempt to drop the connections, ONE BY ONE, using the pfSense firewall, or the local firewall.
 - **YOUR GOAL IS TO DISCONNECT CONNECTIONS IN AS MANY DIFFERENT WAYS AS YOU CAN**
 - **YOUR SECONDARY GOAL IS TO RESTRICT WHO CAN CONNECT REMOTELY**

Different ways to disconnect the connections

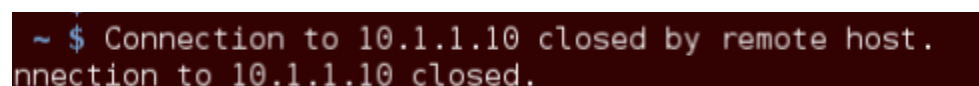
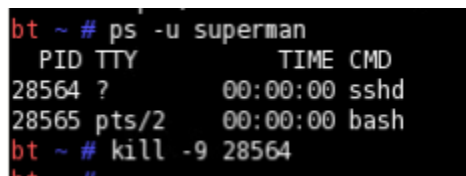
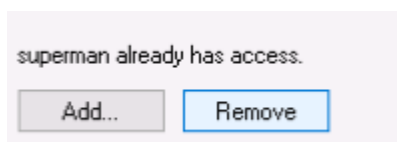
One rdp down



I then used CMD to do the same thing and logoff myself (batman)





If don't need RDP i can just turn it off same way i turned it on. If i still need it, I could just only allow one account through such as an admin account



```
root
bt ~ # iptables -A INPUT -s 203.0.113.2 -j DROP
bt ~ # w
23:42:04 up 2:10, 2 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM      LOGIN@    IDLE       JCPU       PCPU      WHAT
root      tty1     -          21:41     2:00m     0.01s     0.00s    /bin/sh /
theflash  pts/3    203.0.113.2  22:59     54.00s    0.00s     0.00s    -bash
```



















































I added this rule finally and now my connection just hangs on attempt.

		IPv4	TCP	203.0.113.2	*	*	*	*	none		
-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	------	-----	-------------	---	---	---	---	------	--	--

```
connection to 192.168.1.50 closed.
root@Kali-Attacker:~# ssh superman@192.168.1.50 -p 2222
```

And now I have disconnected everything.

Here is a look at some of the logs I got. (blocking kali ip from connection on 2222 after I made the block rule.

	Nov 27 23:55:03	EXTERNAL_GW	  203.0.113.2:52133	  192.168.1.50:2222	TCP:S
	Nov 27 23:55:04	EXTERNAL_GW	  203.0.113.2:52133	  192.168.1.50:2222	TCP:S
	Nov 27 23:55:06	EXTERNAL_GW	  203.0.113.2:52133	  192.168.1.50:2222	TCP:S
	Nov 27 23:55:10	EXTERNAL_GW	  203.0.113.2:52133	  192.168.1.50:2222	TCP:S
	Nov 27 23:55:18	EXTERNAL_GW	  203.0.113.2:52133	  192.168.1.50:2222	TCP:S
	Nov 27 23:55:34	EXTERNAL_GW	  203.0.113.2:52133	  192.168.1.50:2222	TCP:S
	Nov 27 23:56:06	EXTERNAL_GW	  203.0.113.2:52133	  192.168.1.50:2222	TCP:S
	Nov 27 23:56:16	EXTERNAL_GW	  203.0.113.2:52134	  192.168.1.50:2222	TCP:S
	Nov 27 23:56:17	EXTERNAL_GW	  203.0.113.2:52134	  192.168.1.50:2222	TCP:S
	Nov 27 23:56:19	EXTERNAL_GW	  203.0.113.2:52134	  192.168.1.50:2222	TCP:S