Scenario:

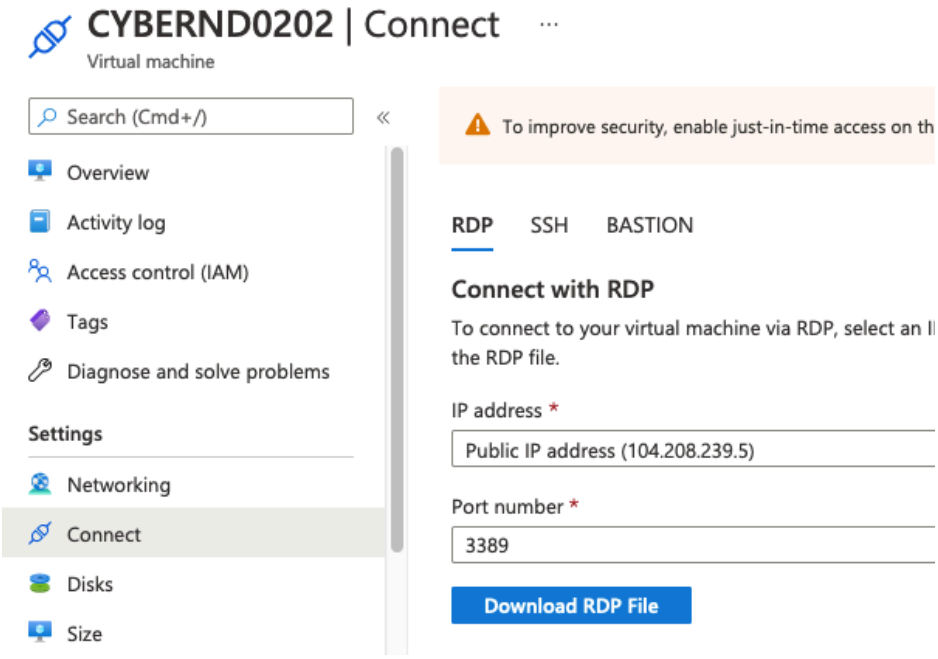
Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI we are happy to bring you on as our first **InfoSec employee!** Once you are settled in and finished orientation we have your first 2-Weeks assignments ready.

Week One:

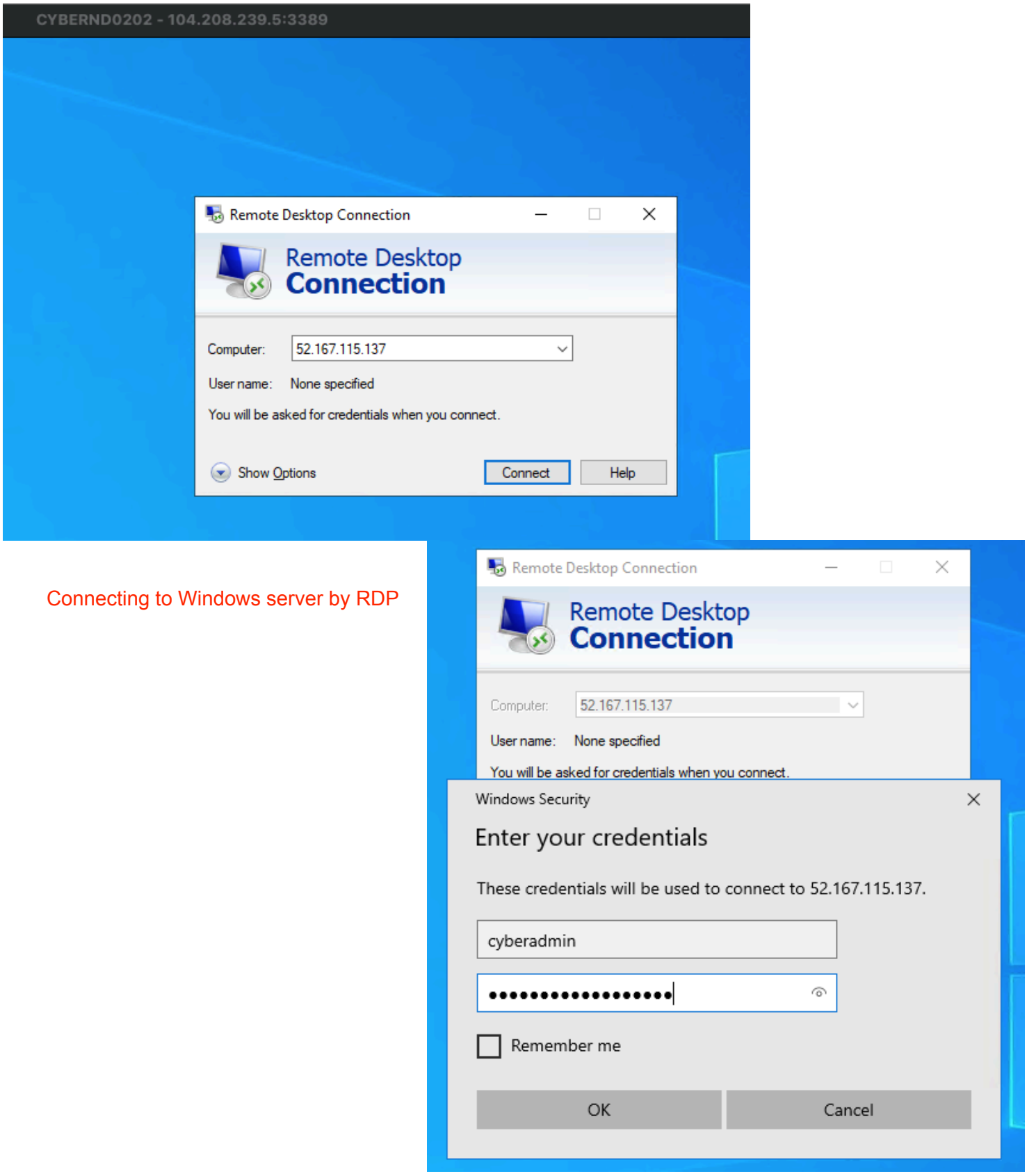
1. **Connect:**

All of the subsequent steps will take place in the DFI environment. You will need to **RDP** into the Windows 10 workstation and use it to connect with the Windows and Linux servers provided using RDP and SSH (via PowerShell) respectively.

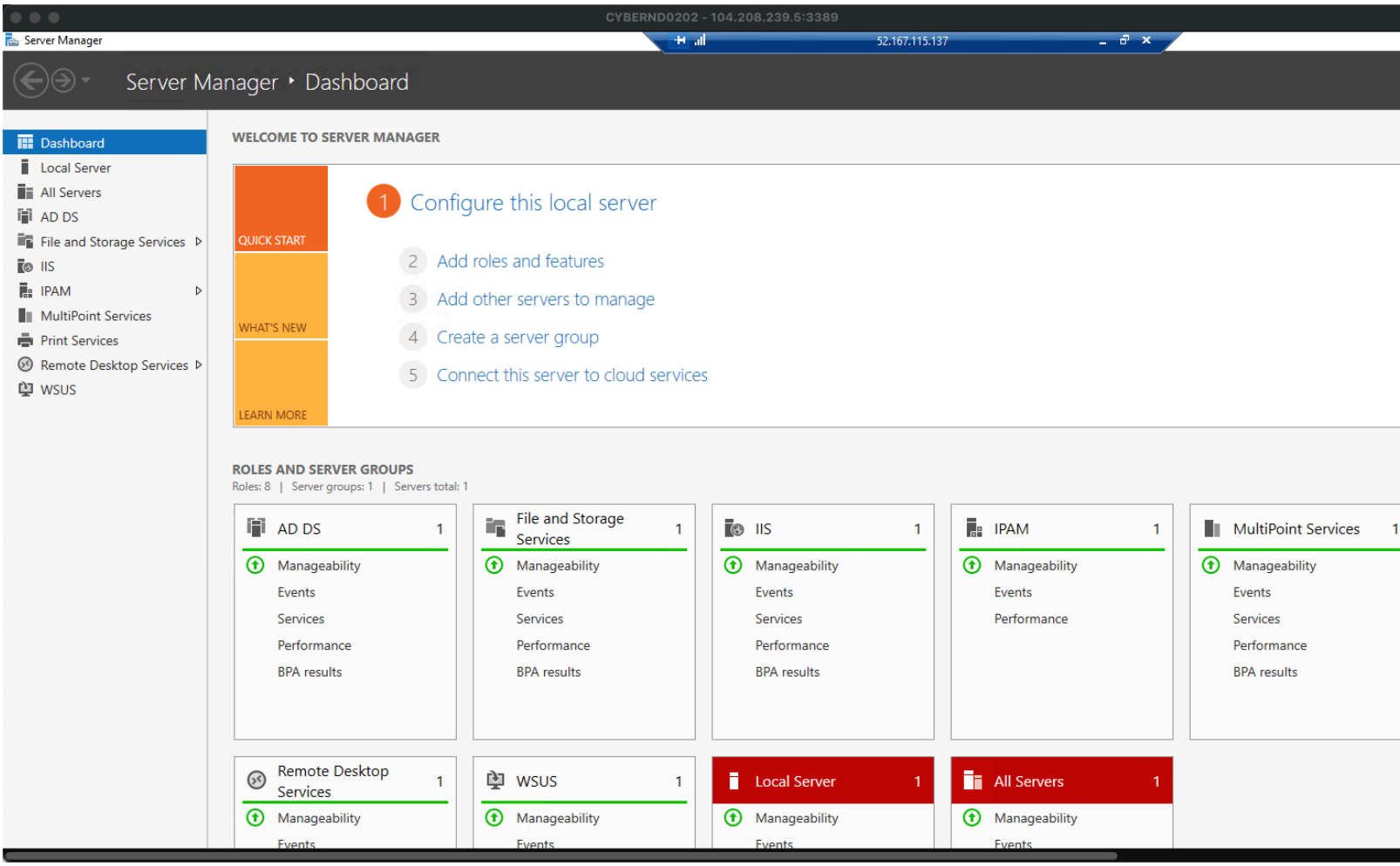
[Please Provide Screenshots of the RDP and SSH here as evidence that you completed this step.]

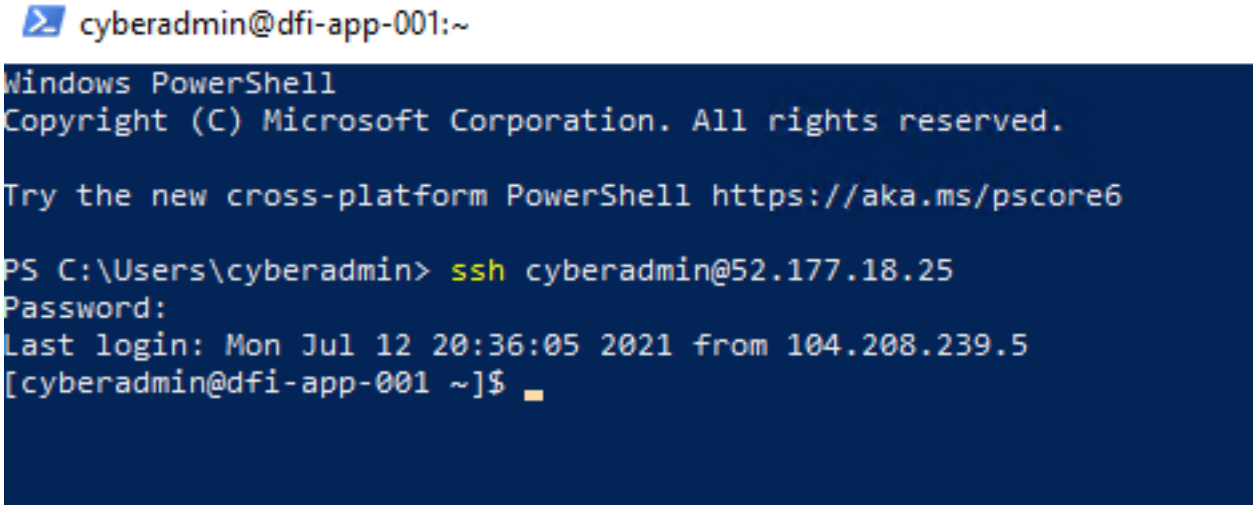


Windows workstation RDP



Connecting to Windows server by RDP


CYBERND0202 - 104.208.239.5:3389
Server Manager
52.167.115.137
Server Manager ‣ Dashboard
Dashboard
Local Server
All Servers
AD DS
File and Storage Services
IIS
IPAM
MultiPoint Services
Print Services
Remote Desktop Services
WSUS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 8 | Server groups: 1 | Servers total: 1
AD DS 1
File and Storage Services 1
IIS 1
IPAM 1
MultiPoint Services 1
Manageability
Events
Services
Performance
BPA results
Remote Desktop Services 1
WSUS 1
Local Server 1
All Servers 1


cyberadmin@dfi-app-001:~
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\cyberadmin> ssh cyberadmin@52.177.18.25
Password:
Last login: Mon Jul 12 20:36:05 2021 from 104.208.239.5
[cyberadmin@dfi-app-001 ~]$

2. **Security Analysis**:

DFI has an excellent SysAdmin team, but they have been focused on system reliability and scaling to meet our growing needs and as a result, security may not be as tight as we'd like. Your first assignment is to familiarize yourself with **our file and application servers**.
Please perform an analysis of the **Windows server** and provide a written report detailing any security configuration issues found and a brief explanation and justification of the changes you recommend. DFI is a PCI compliant organization and will likely be Sarbanes-Oxley in the near future. Use NIST, Microsoft, Defense-in-Depth, Principle of Least Privilege and other resources to determine the changes that should be made. Note changes can be to **add/remove/change** services, permissions and other settings.Defense-in-Depth documentation. NIST 800-123 (other NIST documents could also apply.)
[Place your security analysis here]

- File permissions :

  The first issue is the default account System the best solution is to remove it and change cyberadmin principal from full control access to modify access , And also I suggest to add user groups with restricted permission.
  DFI its become a large company so its needs to assign users to groups and assign permission to it , it can help prevent disclosure of sensitive or restricted information.

- Services :

  The services need to be disabled :

  - CDPUserSvc
  - Certificate Propagation.
  - CNG key isolation
  - Connected user experience and telemetry
  - Cryptographic services
  - Data sharing services
  - DHCP client

  The need to disable these services its because its could be open access for attacker to attack and use these services in malicious way and also other services may have defects and could harm the server , by reducing the number of services detecting unexpected behavior will be increase.

- Roles :

  The rules are not needed on Windows server :

  Remote Desktop services , IPAM,IIS
  Multipoint ,printserver

3. **Firewall Rules:**

DFI does not have a dedicated networking department just yet, once again these tasks normally fall under the SysAdmin group. Now that we have you as a security professional, you'll take over the creation of our **firewall rules**. We recently entered into a new partnership and require new IP connections.
Using Cisco syntax, create the text of a firewall rule allowing a new DFI partner WBC International, access to DFI-File-001 access via port tcp-9082.

The partner's IP is 21.19.241.63 and DFI-File-001's IP is 172.21.30.44.

For this exercise assume the two IP objects **have not** been created in the firewall. **Note*** Use *DFI-Ingress* as the interface for the rule. For documentation purposes, **please explain the syntax for non-technical** management on the change control board that meets weekly.

[Place your firewall rules and explanation here]

- Name 21.19.241.63 partner's
- Name 172.21.30.44 DFI-File-001
- *Access-list DFI-Ingress extended permit tcp host partners host DFI-File-001 eq 9082*

Syntax Explanation :

DFI-Ingress : its the interface been used
Permit : its the action being taken its could be deny or permit
9082 : its the protocol being used
Host : its objects involved could be host , object groups
21.19.241.63 : its the source IP
172.21.30.44 : its the destination IP

4. VPN Encryption Recommendation:

DFI is creating a payroll processing partnership with **Payroll-USA,** this will involve creating a VPN connection between the two. Research, recommend and justify an encryption solution for the connection that is using the latest available encryption for Cisco. Use the Cisco documentation as a guide.

[Place your VPN Encryption Recommendation here]

Choose one of the appropriate encryption methods from the documentation provided. Provide justification for the method you chose

AES-256, its allows to process large volumes of data quickly, and efficiently, its simple implementation and high speed, AES is used as an encryption standard in WPA2, SSH,IPSec, and its algorithm is used to encrypt compressed files such as 7-Zip or RAR. The information encrypted with AES is safe as long as the key remains secret.

5. IDS Rule:

The *System Administrator* gave you a heads up that **DFI-File-001** with an IP address of 172.21.30.44 has been receiving a high volume of **ICMP traffic** and is concerned that a DDoS attack is imminent. She has requested an **IDS rule for this specific server**.

The VoIP Administrator is also concerned that an attacker is attempting to connect to her primary VoIP server which resides at 172.21.30.55 via TFTP. She has requested an IDS rule for this traffic.

For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.

[Place your System Admin rule and explanation here]

Alert ICMP any any -> 172.21.30.44 any (msg”ICMP Attempt Attack”)

[Place your VoIP Admin rule and explanation here]

Alert UDP any any -> 172.21.30.55 any (msg”TFTP Attempt Attack”)

IDS, IPS or Firewalls programs follow a set of rules; To pass, reject or alert when a particular connection occurs from within the network to outside it, or opposite .

The correct way to right the rules :

1. Action
2. Portocol
3. Ip source
4. Port
5. Direction way
6. Ip destination
7. Port
8. Massage

The commands are

alert Show call alerts.
log Log connection data.
pass Ignore the connection.
reject Reject the connection with the log data and send the rejection message to the sender.
sdrop Refused to connect without registering it.

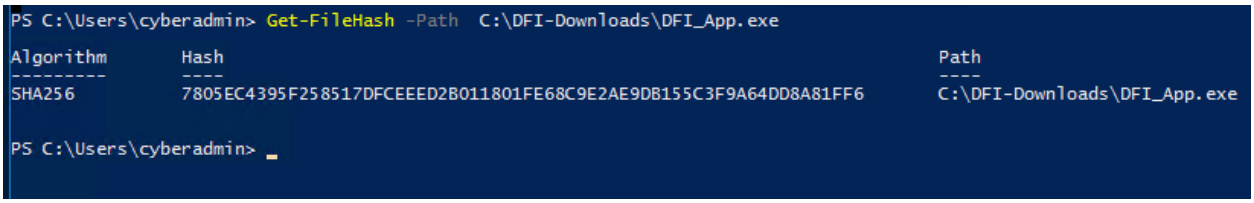
6. **File Hash verification:**

A software vendor has supplied DFI with a custom application. They have provided the file on their public FTP site and e-mailed you directly a file hash to verify the integrity and authenticity. The hash provided is a SHA256.

Hash: 7805EC4395F258517DFCEEED2B011801FE68C9E2AE9DB155C3F9A64DD8A81FF6

Perform a file hash verification and submit a screenshot of your command and output.
The File is stored on the Windows 2016 Server in C Drive under DFI-Download.

[Place your screenshot verification here]



Week Two:

Now that you've performed a light audit and crafted Firewall and IDS Signatures we're ready for you to make some additional recommendations to tighten up our security.

7. **Automation:**

The IT Manager has tasked you with some introductory research on areas that could be improved via automation.

Research and recommend products, technologies and areas within DFI that could be improved via automation.

Recommended areas are:

- SOAR products and specifically what could be done with them
- Automation of mitigation actions for IDS and firewall alerts.
- Feel free to elaborate on other areas that could be improved.

Complete the chart below including the area/technology within DFI and a proposed solution, with a minimum of 3 areas. Provide a brief explanation for your choices.

DFI Area/Technology	Solution	Justification for Recommendation
Windows event log	Monitor windows event log by using application that alert about critical event	By manually tracking issues can take time to find and troubleshoot
Passwords	Implement two factor authentication	Resetting passwords its important task , the two factor mechanism closely validate user input
Access control list updates Firewall rules	Create database in which to store the acl policy definitions That why each policy exist and the criteria for changing or deleting	Firewall rules can be challenging to maintain and sometime we could forget the origin of rules

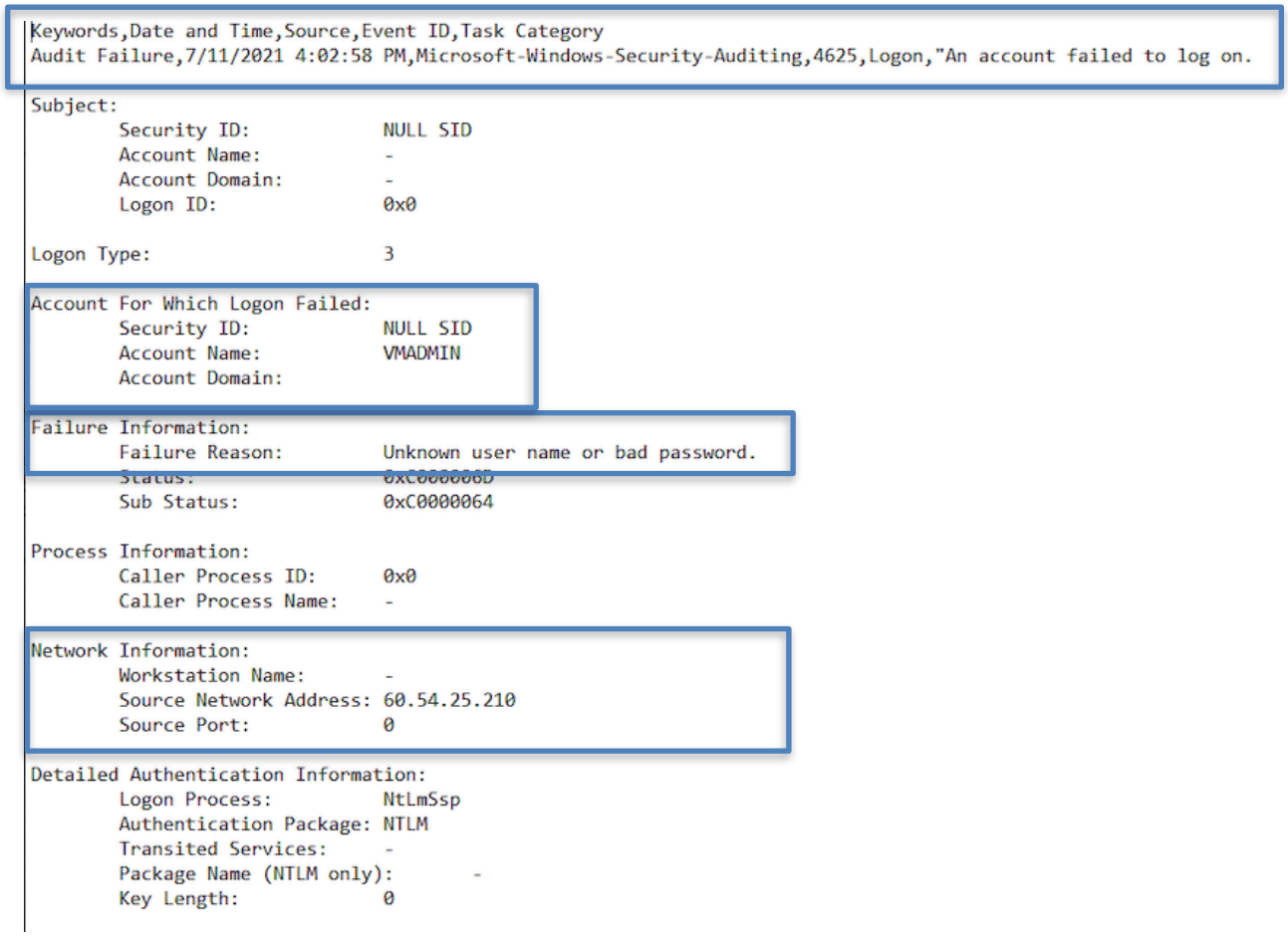
8. **Logging RDP Attempts:**

The IT Manager suspects that someone has been attempting to login to DFI-File-001 via RDP.

Prepare a report that **lists unsuccessful attempts** in connecting over the last 24-hours. Using **Powershell or Eventviewer**, search the Windows Security Log for Event 4625. **Export to CSV.**

For your deliverable, open the CSV with notepad and take a screenshot from your personal computer for your explanation. Please also include this file in your submission. Then in your report below explain your findings, recommendations and justifications to the IT Manager.

[Place IT Manager Report Here]



```
Keywords,Date and Time,Source,Event ID,Task Category
Audit Failure,7/11/2021 4:02:58 PM,Microsoft-Windows-Security-Auditing,4625,Logon,"An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           VMADMIN
        Account Domain:

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC0000064

Process Information:
        Caller Process ID:      0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       -
        Source Network Address: 60.54.25.210
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0
```

1. The failed login come from VMADMIN account.
2. The failure reason is unknown name or bad password.
3. The origin IP address
4. The event detailed :
    - Event id
    - Event description

9. **Windows Updates:**

Using NIST 800-40r3 and Microsoft Security Update Guide, analyze the windows servers and provide your answers in the table below of available updates (KB and CVE) that should be installed as well as any updates that can be safely ignored for DFI's purpose. To assist, be aware that DFI is concerned with stability and security, any update that is not labeled as a 'critical' or 'security' can be left off.

Justify your recommendations as to why you are making your choices.
Add as many rows or additional columns as you need to the table.

Available Updates	Update/Ignore	Justification
Windows Server 2012 Critical	Update	A remote code execution vulnerable , an attacker could use this by installing programs ,view ,change or delete data; or create new accounts with full user rights
Windows 10	Update	This security update resolves vulnerabilities in Adobe Flash Player ;remote attacker to execute arbitrary code by convincing a user to visit a website containing specially crafted Flash content
Microsoft Malware Protection Engine	update	Denial of service
Windows explorer	Ignore	Its not high security update
Microsoft edge	Ignore	Its not high security update
Microsoft .net	Ignore	Its not high security update

10. **Linux Data Directories:**

The IT Manager has requested your help with **creating directories** on the CentOS server DFI-App-001 (reachable by ssh from the Windows 10 machine. in the DFI subnet.)

- The root directory should be 'Home'
- The first subdirectory should be "Departments" with subdirectories: HR, Accounting, Public, IT and OperaITtions.
- Set owner permissions for the **groups IT, HR, Operations and Accounting**
- Create the users AmyIT, PamOps, MandyAcct and TimHR in the appropriate groups so that they can read/write/execute in their respective departmental folders.

For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.

[Provide a screenshot(s) of completed tasks and the correctly set permissions here]

[Provide your non-technical syntax explanation for management here]

```
[cyberadmin@dfi-app-001 ~]$ mkdir home
[cyberadmin@dfi-app-001 ~]$ cd home
[cyberadmin@dfi-app-001 home]$ mkdir department
[cyberadmin@dfi-app-001 home]$ cd department
[cyberadmin@dfi-app-001 department]$ mkdir HR
[cyberadmin@dfi-app-001 department]$ mkdir Accounting
[cyberadmin@dfi-app-001 department]$ mkdir Public
[cyberadmin@dfi-app-001 department]$ mkdir IT
[cyberadmin@dfi-app-001 department]$ mkdir Operation
```

```
[cyberadmin@dfi-app-001 home]$ sudo groupadd IT
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 home]$ sudo groupadd HR
[cyberadmin@dfi-app-001 home]$ sudo groupadd Operation
[cyberadmin@dfi-app-001 home]$ sudo groupadd Accounting
[cyberadmin@dfi-app-001 home]$
```

```
[sudo] password for cyberadmin:
Sorry, try again.
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 home]$ sudo useradd AmyIT
useradd: user 'AmyIT' already exists
[cyberadmin@dfi-app-001 home]$ sudo useradd PamOps
[cyberadmin@dfi-app-001 home]$ sudo useradd MandyAcct
[cyberadmin@dfi-app-001 home]$ sudo useradd TimHR
[cyberadmin@dfi-app-001 home]$
```

```
[cyberadmin@dfi-app-001 home]$ sudo usermod -a -G IT AmyIT
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 home]$ sudo usermod -a -G HR TimHR
[cyberadmin@dfi-app-001 home]$ sudo usermod -a -G Operation PamOps
[cyberadmin@dfi-app-001 home]$ sudo usermod -a -G Accounting MandyAcct
```

```
[cyberadmin@dfi-app-001 department]$ sudo chown AmyIT:IT ./IT
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 department]$ ls -l
total 0
drwxrwxr-x. 2 cyberadmin cyberadmin 6 Jul 12 23:48 Accounting
drwxrwxr-x. 2 cyberadmin cyberadmin 6 Jul 12 23:48 HR
drwxrwxr-x. 2 AmyIT      IT         6 Jul 12 23:49 IT
drwxrwxr-x. 2 cyberadmin cyberadmin 6 Jul 12 23:50 Operation
drwxrwxr-x. 2 cyberadmin cyberadmin 6 Jul 12 23:49 Public
[cyberadmin@dfi-app-001 department]$ sudo chown MandyAcct:Accounting ./Accounting
[cyberadmin@dfi-app-001 department]$ sudo chown PamOps:Operation ./Operation
[cyberadmin@dfi-app-001 department]$ sudo chown TimHR:HR ./HR
```

```
[cyberadmin@dfi-app-001 home]$ sudo chmod -R 777 ./department
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 home]$ ls -l
total 0
drwxrwxrwx. 7 cyberadmin cyberadmin 75 Jul 12 23:50 department
[cyberadmin@dfi-app-001 home]$ cd department
[cyberadmin@dfi-app-001 department]$ ls -l
total 0
drwxrwxrwx. 2 MandyAcct  Accounting 6 Jul 12 23:48 Accounting
drwxrwxrwx. 2 TimHR      HR         6 Jul 12 23:48 HR
drwxrwxrwx. 2 AmyIT      IT         6 Jul 12 23:49 IT
drwxrwxrwx. 2 PamOps     Operation  6 Jul 12 23:50 Operation
drwxrwxrwx. 2 cyberadmin cyberadmin 6 Jul 12 23:49 Public
[cyberadmin@dfi-app-001 department]$
```

[Provide your non-technical syntax explanation for management here]

1. Mkdir : create a folder / directory
2. Cd : navigate to the directory or folder
3. Groupadd : add a group and name it
4. Useradd : add a user and name it
5. User mod : assign user to group
6. Chown: set owner to file or directory
7. Chmod : set right permission to file or directory (readwrite,excute)

11. **Firewall Alert Response**:

The IT Manager took a look at firewall alerts and was concerned with some traffic she saw, please take a look and provide a **mitigation response** to the below firewall report. Remember to justify your mitigation strategy.
This file is available from the project resources title: **DFI_FW_Report.xlsx**. Please download and use this file to complete this task.

[Firewall mitigation response and justification goes here]

IP	Mitigation response Block / friend	Justifaction
192.109.240.69	Block	Malicious
103.125.191.115	Block	Malicious
192.34.57.157	Block	Malicious
185.244.39.112	Block	Malicious
117.131.14.38	Block	Malicious
41.50.139.255	Block	Malicious
154.8.140.74	Block	Malicious
175.6.47.5	Friend	Clean
103.79.141.158	Block	Malicious
34.201.223.194	Friend	Clean
3.132.217.60	Friend	Clean
37.110.85.110	Block	Malicious
104.50.90.145	Friend	Clean
51.79.21.228	Block	Malicious
208.113.129.65	Block	Malicious
208.113.167.204	Block	Malicious
39.116.31.62	Block	Malicious
104.50.90.145	Block	Malicious
51.15.88.139	Block	Malicious
170.210.83.86	Block	Malicious
61.161.143.170	Block	Malicious
104.50.90.145	Friend	Clean
208.113.167.204	Block	Malicious

12. **Status Report and where to go from here:**

As your first two weeks wind down, the IT Manager, HR Manager as well as other management are interested in your experience. With your position being the first dedicated Information Security role, they would like a 'big picture' view of what you've done as well as the security posture of DFI.

Similar to Defense-in-Depth, an organization has multiple layers of security from the edge of their web presence all the way to permissions on a file.

In your own words explain the work you've done, the recommendations made and how DFI should proceed from a security standpoint. This is your opportunity to provide a thoughtful analysis that shows your understanding of Cyber Security and how all of the tasks you've performed contribute to the security of DFI. As this will be reviewed by non-technical management please keep the technical jargon to a minimum.

[Provide your Status Report Here]

In the first week :

Step one doing security analysis its methods that helps Identify the organizational assets and resolve vulnerabilities and then recommend the best solution to reach DFI security requirement The second step applying the first line of defense firewall rules , in here we have partnership with WBC a new ip connection the rules identify its fine to allow traffic through this new ip and IDS rule we make alert of attempted attack . We also recommended the best vpn encryption and we checked the hash file and verified the integrity of it

In the second week :

We started this week by recommending the area in the DFI that could be improved by automation we save time by using exictng technology that helps after that we started to look logging event we manage find out there is failure login attempt then we extract the user account and IP address to it , the third step is checking any update in the windows server and determining if its critical or just update pack and last step is analyzing the firewall report and define whither the ip is malicious or save

Security policy : Least privilege, defense of depth
Security product: SEIM and SOAR

13. **File Encryption:**

As your final task, assemble all of the deliverables you have created in Steps 1-12 and encrypt them using 7zip with a strong password.

When you submit the file you must also include your password as a note to the reviewer at Udacity or they will not be able to review your project.