Honeypot Project:
Final Project

SAAD1002 – Introduction to Systems Analysis and Design

Adriano Valenga Carneiro

Alex Kelly

Mohammed Hussain

Zach Slaunwhite

Table of Contents

Introduction

This document is a delivery method for the information as specified by the Honeypot Final Project. This includes any work completed during phase 1 and phase 2.

Planning Documentation

Activity Plan #1: Windows Server 2016

<table>
<tr><th colspan="6">Activity List/Plan</th></tr>
<tr><td colspan="5">Project: Honeypot – Windows Server 2016</td><td>Date: 10-05-2016</td></tr>
<tr><td>Activity ID No.</td><td>Activity Name</td><td colspan="3">Description of Work</td><td>Responsibility</td></tr>
<tr><td>A001</td><td>Create Activity Plan for implementation</td><td colspan="3"></td><td>Adriano, Alex Mohammed, and Zach</td></tr>
<tr><td>A002</td><td>Documentation required for install and configuration.</td><td colspan="3">ISEC3700_Final Project_Checkpoint 1_v9.10.19</td><td>“</td></tr>
<tr><td>A003</td><td>Resources required for install.</td><td colspan="3">Windows Server 2016 ISO</td><td>“</td></tr>
<tr><td rowspan="11">A004</td><td rowspan="11">Documentation of object names required for implementation</td><td colspan="3">Specify object names in preparation for implementation</td><td rowspan="11">“</td></tr>
<tr><td>Hardware Location:</td><td colspan="2">Room D316</td></tr>
<tr><td>Operating System</td><td colspan="2">Windows Server 2016</td></tr>
<tr><td rowspan="4">Hardware Configuration:</td><td>HD</td><td>250 GB</td></tr>
<tr><td>RAM</td><td>16 GB</td></tr>
<tr><td>CPU</td><td>Intel Core i5 3470 @ 3.20GHz</td></tr>
<tr><td>NIC (1)</td><td>Intel 82579LM Gigabit</td></tr>
<tr><td rowspan="4">Network</td><td>IP Address (Static)</td><td>172.16.136.73</td></tr>
<tr><td>Subnet Mask</td><td>255.255.252.0</td></tr>
<tr><td>G/W Address</td><td>172.16.136.250</td></tr>
<tr><td>DNS Server Addresses (2)</td><td>172.16.136.3
172.16.136.2</td></tr>
</table>

<table>
<tr><td></td><td></td><td><table>
<tr><td>Installation Mode</td><td>New Install</td></tr>
<tr><td>Time Zone:</td><td>Atlantic</td></tr>
<tr><td>Server Type</td><td>N/A</td></tr>
<tr><td>Change Log:</td><td>Change log will be located on our group OneDrive within the ISEC - Honeypot directory.</td></tr>
<tr><td>Server “Administrator” Password:</td><td>Passw0rd</td></tr>
<tr><td>Server Host Name:</td><td>LeafcutterBee</td></tr>
<tr><td>Domain Name:</td><td>N/A</td></tr>
<tr><td>Test Internet connection:</td><td>See test plan.</td></tr>
<tr><td>Backup Admin User:</td><td>CBruce</td></tr>
<tr><td>Password:</td><td>PAssw0rdCB</td></tr>
<tr><td>Additional User:</td><td>N/A</td></tr>
<tr><td>Password:</td><td>N/A</td></tr>
</table></td><td></td></tr>
<tr><td>A005</td><td>Test system functionality</td><td>See test plan.</td><td></td></tr>
<tr><td>A006</td><td>Additional Configurations or settings applied</td><td>- All critical updates performed.
- Setup auditing on object access.</td><td></td></tr>
<tr><td>A007</td><td>Additional Software required as part of initial install</td><td>- VMware Workstation Pro
- Notepad ++
- 7Zip
- Zabbix Agent
- Google Chrome
- Splunk Universal Forwarder</td><td></td></tr>
</table>

Activity Plan #2: CentOS 7

<table>
<tr><th colspan="6">Activity List/Plan</th></tr>
<tr><td colspan="5">Project:</td><td>Date:</td></tr>
<tr><td>Activity ID No.</td><td>Activity Name</td><td colspan="3">Description of Work</td><td>Responsibility</td></tr>
<tr><td>A001</td><td>Create Activity Plan for implementation</td><td colspan="3"></td><td>Adriano, Alex Mohammed, and Zach</td></tr>
<tr><td>A002</td><td>Documentation required for install and configuration.</td><td colspan="3">ISEC3700_Final Project_Checkpoint 1_v9.10.19</td><td>“</td></tr>
<tr><td>A003</td><td>Resources required for install.</td><td colspan="3">CentOS 7 ISO</td><td>“</td></tr>
<tr><td rowspan="12">A004</td><td rowspan="12">Documentation of object names required for implementation</td><td colspan="3">Specify object names in preparation for implementation</td><td rowspan="12">“</td></tr>
<tr><td>VM Folder:</td><td colspan="2">C:\Windows\ADFS\vm-za (hidden)</td></tr>
<tr><td>VM Name:</td><td colspan="2">Leafcutter.zabbix.splunk</td></tr>
<tr><td>VM OS (selected during VM build):</td><td colspan="2">CentOS 7</td></tr>
<tr><td rowspan="4">VM Hardware Configuration:</td><td>HD</td><td>40 GB</td></tr>
<tr><td>RAM</td><td>4 GB</td></tr>
<tr><td>Processors/Cores</td><td>1/1</td></tr>
<tr><td>VM Compatibility</td><td>15.x</td></tr>
<tr><td rowspan="4">Network</td><td>IP Address (Static)</td><td>DHCP</td></tr>
<tr><td>Subnet Mask</td><td>DHCP</td></tr>
<tr><td>G/W Address</td><td>DHCP</td></tr>
<tr><td>DNS Server Addresses (2)</td><td>DHCP</td></tr>
<tr><td>Installation Mode</td><td colspan="2">New Install</td></tr>
<tr><td>Time Zone:</td><td colspan="2">Atlantic</td></tr>
</table>

		Server Type	Security Server	
		Installation Settings & Change Log:	Install located: C:\Windows\ADFS\vm-za Change log will be located on our group OneDrive within the ISEC - Honeypot directory.	
		Server "Administrator" Password:	LeafcutterPassw0rd	
		Server Host Name:	leafcutter.zabbix.splunk	
		Domain Name:	N/A	
		Test Internet connection:	See testing plan.	
		Backup Admin User:	leafcutter	
		Password:	LeafcutterPassw0rd	
		Additional User:	N/A	
		Password:	N/A	
A006	"Snapshot" information: Regular rollback points for the system	Snapshots will be made after any modification to the CentOS server and named by date.		"
A007	"Gold" Copy information: Backup the system	Gold copies will be made after any modification to the CentOS server and stored on a separate external SSD.		"
A008	Test system functionality	See test plan.		
A009	Additional Configurations or settings applied	- All updates performed.		
A010	Additional Software required as part of initial install	- Zabbix - Splunk		

Testing Plan

Windows Server 2016

Test ID	Test Member	Description	Acceptable Baseline	Pass / Fail	Notes/Results
T001	Alex Kelly	Start-up server and login to OS with admin account to verify OS install is functional	Server starts-up and login is successful	Pass	Server started/login successful
T002	“”	Check license activation status via Server Manager.	License is activated	Pass	License is activated
T003	“”	Confirm network settings are configured as per activity plan using “netsh interface ipv4 show config” command.	Network settings are properly configured	Pass	Network settings meet activity plan
T004	“”	Verify internet connectivity by ping google.ca, nscc.ca, and bing.ca.	All websites are accessible within a reasonable period.	Pass	Websites accessed in 50 ms, deemed acceptable.
T005	“”	Verify that a successful remote connection to the server can be made using RDC on a Net172 computer	Net172 computer successfully remotes into server	Pass	Remove connection successful
T006	“”	Test auditing by creating test file, applying audit policy, opening test file, and checking security log.	Event manager shows event.	Pass	Events shown.
T007	“”	Test Splunk forwarder by performing 5 failed logins to Windows 2016 server. Verify Splunk is detecting and monitoring the Windows 2016 server.	If forwarder is successfully working, group will receive email regarding failed logins.	Pass	Emails received.
T008	“”	Test Zabbix agent by verifying Zabbix is detecting and monitoring the Windows 2016 server based on traffic created during T004.	Zabbix is detecting and monitoring the Windows 2016 server.	Pass	Ping from T004 is captured.

CentOS 7

Test ID	Test Member	Description	Acceptable Baseline	Pass / Fail	Notes/Results
T001	Zach	Start-up VM and login to OS with admin account to verify OS install is functional	VM starts up and login is successful	Pass	Start-up and login both successful.
T002	“”	Test internet connectivity by pinging google.ca, nscc.ca, and bing.ca using terminal	All websites respond within a reasonable period.	Pass	All websites responded under 50ms
T003	“”	Ping Window Server from CentOS terminal to test connectivity.	CentOS VM can successfully ping Windows Server	Pass	Ping successful.
T004	“”	Perform 5 failed logins to Windows 2016 server. Using a Net172 computer, verify Splunk is detecting and monitoring the Windows 2016 server.	Splunk alerts group email account regarding failed logins.	Pass	Email notifications received.
T005	“”	Using a Net172 computer, verify Zabbix is detecting and monitoring the Windows 2016 server based on traffic created during T003.	Zabbix is detecting and monitoring the Windows 2016 server.	Pass	Zabbix detected ping activity performed in T003.

Install and Change Management Log

Install and Change Management: Windows Server 2016

Install Report for Leafcutter Group
ISEC3700

Student Information

Student Name	Leafcutter Group
Student Number	w0223600
Course Name	ISEC3700

Reporting Form

Export as PDF

Install Information

Operating System	Windows Server 2016	Version	1803
64 or 32 Bit	64 Bit		
Hostname	LeafcutterBee		
Hard Drive(s)	Hard Drive 1: 40 GB		

Static Configuration

IP Address	162.16.136.73
Subnet Mask	255.255.252.0
Gateway	172.16.136.250
Primary DNS	172.16.136.3
Secondary DNS	172.16.136.2

RAM	16GB
# of Processors	4
Network Configuration	Static
Issues	No issues reported
Steps to Resolve Issues	No issues reported
List of Attachments	Activity_Plan_and_Test_Plan.docx Naming Convention v24.9.19.docx

Figure 1 Install Log

Change Log Report for Leafcutter Group
ISEC3700

Student Information

Student Name	Leafcutter Group
Student Number	w0223600
Course Name	ISEC3700

Reporting Form

Export as PDF

Change Log Information

Date	11/5/2019
Assignment Number	1
Changes / Modifications	- Administrator password: Passw0rd - Created backup admin CBruce - CBruce password: Passw0rdCB - Timezone set to Americas/Halifax (AST) - Performed all critical updates. - Disabled Windows Updates - Activated using NSCC KMS Server - Setup auditing on object access. - Downloaded and installed the following software: VMWAre Workstation Pro Notepad++ 7Zp Google Chrome Splunk Universal Forwarder Zabbix Agent - Opened ports on firewall: 8000, 10050 TCP - Disabled shutdown and restart menu - Hid VMWare from system tray
Issues	No issues reported
List of Attachments	Activity_Plan_and_Test_Plan.docx

Figure 2 Change Log

Install Report for Leafcutter Group
ISEC3700

Student Information

Student Name	Leafcutter Group
Student Number	w0223600
Course Name	ISEC3700

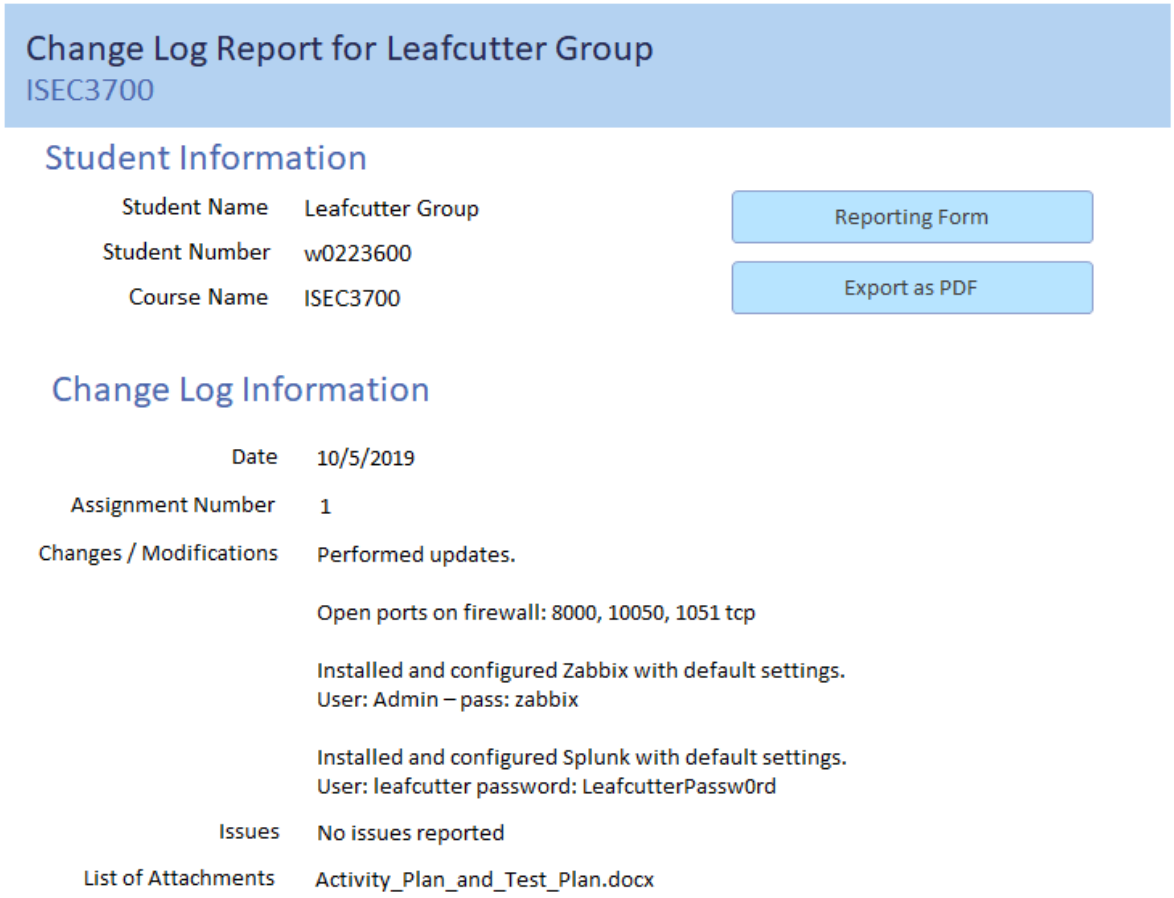
Reporting Form

Export as PDF

Install Information

Operating System	CentOS	Version	7
64 or 32 Bit	64 Bit		
Hostname	leafcutter.zabbix		
Hard Drive(s)	Hard Drive 1: 40 GB		
RAM	4GB		
# of Processors	4		
Network Configuration	DHCP		
Issues			
Steps to Resolve Issues			
List of Attachments	Activity_Plan_and_Test_Plan.docx Naming Convention v24.9.19.docx		

Figure 3 Install Log



Change Log Report for Leafcutter Group
ISEC3700

Student Information

Student Name	Leafcutter Group
Student Number	w0223600
Course Name	ISEC3700

Reporting Form

Export as PDF

Change Log Information

Date	10/5/2019
Assignment Number	1
Changes / Modifications	Performed updates. Open ports on firewall: 8000, 10050, 1051 tcp Installed and configured Zabbix with default settings. User: Admin – pass: zabbix Installed and configured Splunk with default settings. User: leafcutter password: LeafcutterPassw0rd
Issues	No issues reported
List of Attachments	Activity_Plan_and_Test_Plan.docx

Figure 4 Change Log

Auditing Research and Setup

Auditing in Windows Server, or specifically audit policy, is how the system determines what information will be tracked by the system. Said information is then made available in the system's security log for analysis. For this reason, it is important to have audit policy configured – especially in the scenario of our honeypot, where security analysis is required.

There are nine main policies:

- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

In addition to the main policies, there are advanced audit policies that can be accessed for further control. Policies have two possible settings: success and failure. Enabling a policy with success means that any successful events will be logged, while enabling a policy with failure will log any failed events.

While setting up an auditing policy is helpful in analyzing security events, it is also important to understand what auditing policies a system requires. An audit policy that covers too many events will lead to the collection of significant data – the more data there is, the more difficult it is to analyze. This means that audit policies should be configured to collect meaningful data while avoiding things that clutter the log without adding value.

(Melnik, 2018)

Setup

Based on the requirements of the honeypot, we have identified the need to audit object access. This will allow us to enable auditing on specific files and folders so that we can review who has attempted to access them. This information can then be viewed using one of our monitoring software, Splunk.

We will access the object policies by navigating to the Local Security Policy, selecting Audit Policy, and enabling both "Success" and "Failure" for the Audit Object Access policy. At a future point, when it is determined which files or folders specifically require auditing, we will enable auditing for those files and folders.

As the project progresses, we expect to enable additional audit policies if a) the need arises; and, b) the data is not already being logged by Splunk.
(Solarwinds, 2017)

Software Research

Zabbix

General Information

Zabbix , created by Alexaei Vladishev, is an open source-monitoring software. It's a program that records the statuses and conditions of an interconnected devices, such as networks or cloud services. It then provides an easy-to-use web interface for users to monitor their systems as well as provide alerts based on event occurrences, allowing users to quickly respond to any issues. Zabbix is capable of monitoring small and large networks alike, and supports most popular operating systems including Windows and Linux

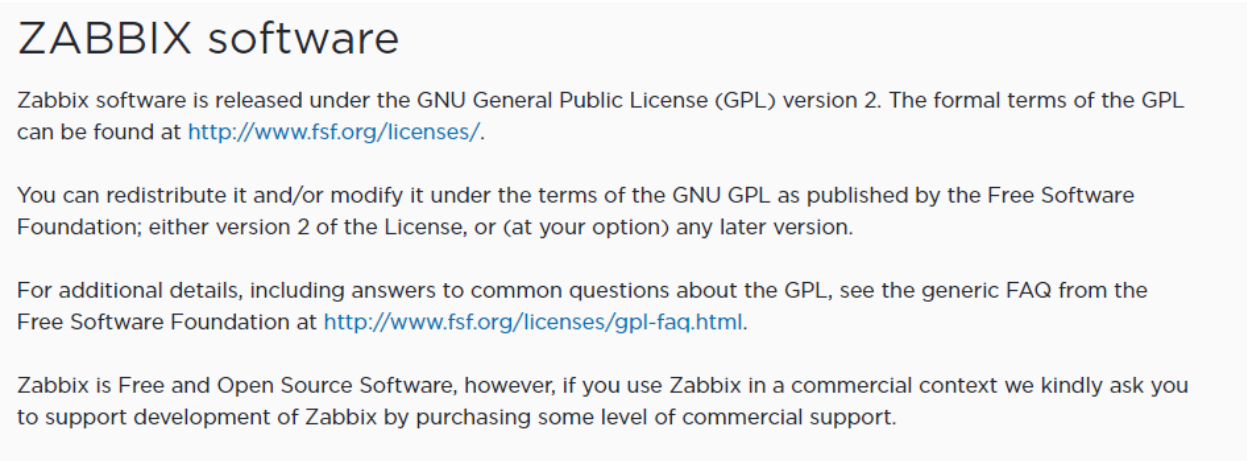
While some checks can be performed without an agent, it is recommended that an agent is installed for complete monitoring functionality, such as monitoring for CPU load or network utilization. Based on Zabbix's extensive feature list, including extensive system monitoring, audit logs, user authentication, templates, and email notifications, Zabbix will be an asset in tracking activity that takes place on our honeypot.

Our setup will have Zabbix located on our CentOS server, acting as the Zabbix host, while an agent will be installed on our Windows Server.

(Wikipedia, 2019)

Copyright Information

Zabbix is a GNU Version 2 software. This allows for the commercial use of this software. Complete information on the terms of GNU General Public License V2 can be found at http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.



ZABBIX software

Zabbix software is released under the GNU General Public License (GPL) version 2. The formal terms of the GPL can be found at http://www.fsf.org/licenses/.

You can redistribute it and/or modify it under the terms of the GNU GPL as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

For additional details, including answers to common questions about the GPL, see the generic FAQ from the Free Software Foundation at http://www.fsf.org/licenses/gpl-faq.html.

Zabbix is Free and Open Source Software, however, if you use Zabbix in a commercial context we kindly ask you to support development of Zabbix by purchasing some level of commercial support.

Figure 5 License information from https://www.zabbix.com/license

Splunk

General Information

Splunk, simply put, is a data analytics software that is used to read machine data. Splunk comes with its own searching language to help find specific information that would otherwise be difficult to read or understand. In addition to the searching, there is an astronomical number of features, such as the innovative dashboards.

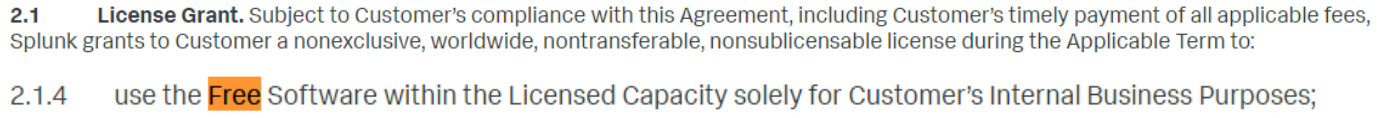
Our setup will have Splunk located on our CentOS server, acting as the Splunk host, while the Splunk Forwarder will be installed on our Windows Server. We will then use Splunk to forward specific data from our Windows Server to our CentOS server. Currently, Splunk is configured to forward all windows activity (anything you can view in event viewer), with the possibility of configuring custom file monitoring which we will be exploring in the upcoming assignments.

One feature of Splunk that we are utilizing is triggered alerts, which will notify us when there is a login attack happening on our server. We will be diving deeper into this alert system to send emails for any successful logins from workstations that are not native to our group (Anything that isn't POD7).

(All information was provided from Zach Slaunwhite, certified Splunk power user, and his personal experience with the software)

Copyright Information

Splunk contains a free version of the software with a limit of 500MB ingestion per day that can be used for internal business use. This allows for commercial use in an educational environment. Complete License information can be found at https://www.splunk.com/en_us/legal/splunk-software-license-agreement.html


2.1 **License Grant.** Subject to Customer's compliance with this Agreement, including Customer's timely payment of all applicable fees, Splunk grants to Customer a nonexclusive, worldwide, nontransferable, nonsublicensable license during the Applicable Term to:

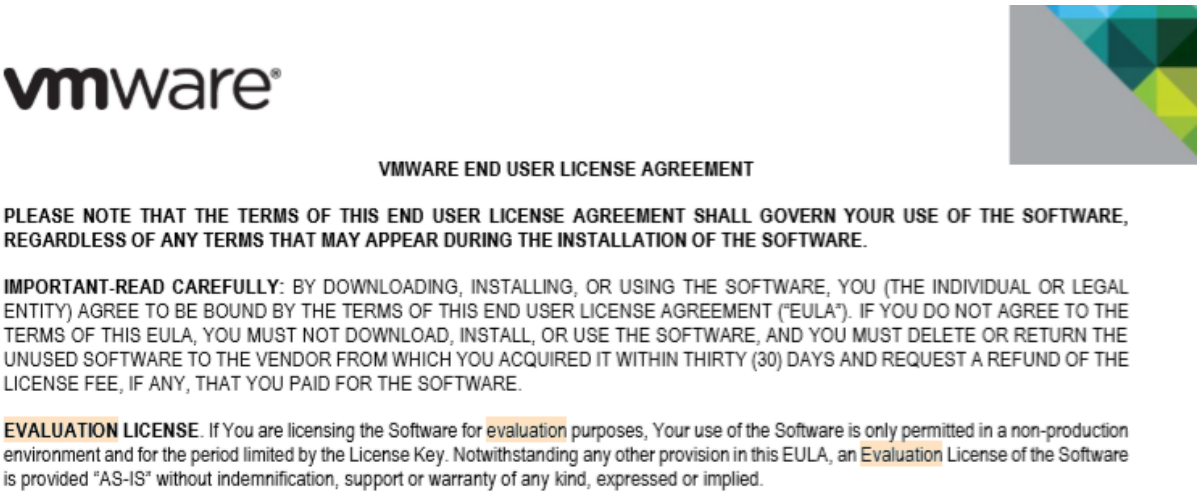
2.1.4 use the Free Software within the Licensed Capacity solely for Customer's Internal Business Purposes;

Figure 6 Splunk Software License Agreement

Additional Software Copyright Information

VMware Workstation Pro

Description: Virtualization software



VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

Figure 7 VM Ware EULA

Further information can be found at:
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf

Notepad ++
Description: Text editor.

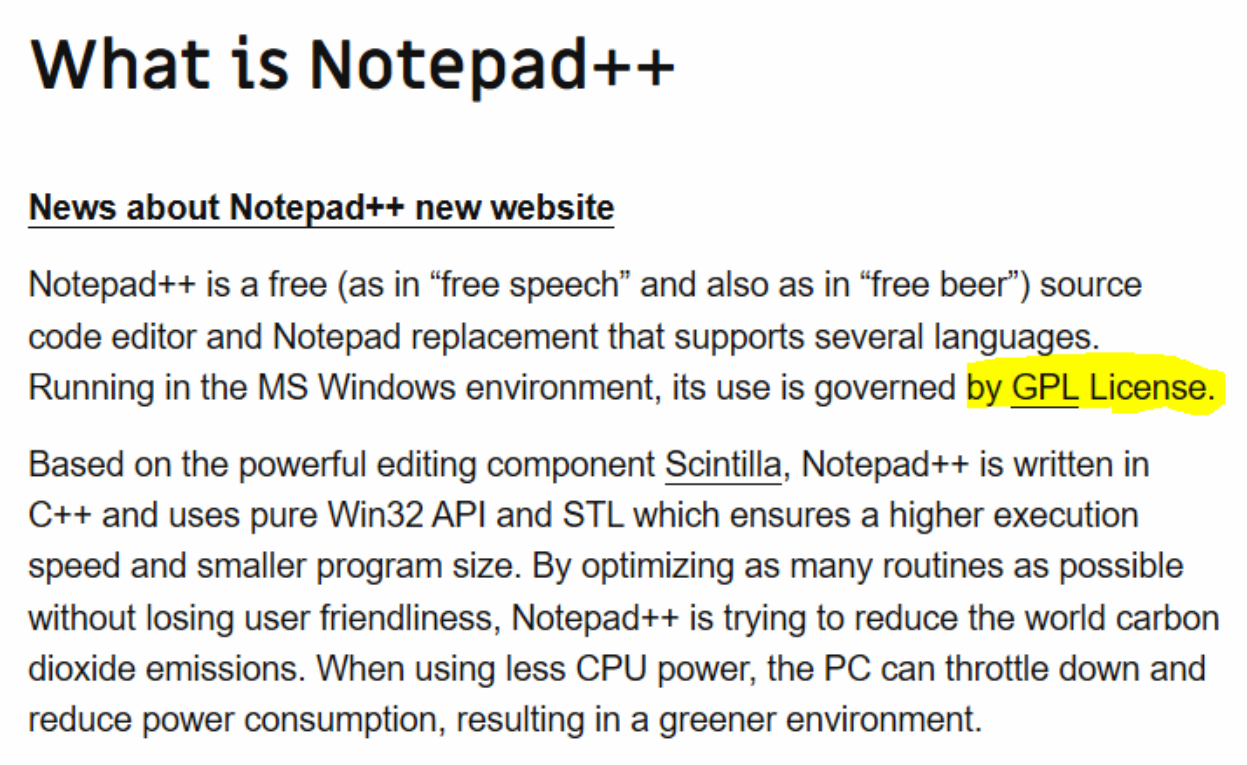


Figure 8 Notepad++ Official Website

Additional information can be found at: https://www.gnu.org/licenses/gpl-3.0.html.

7Zip

Description: File Archiver

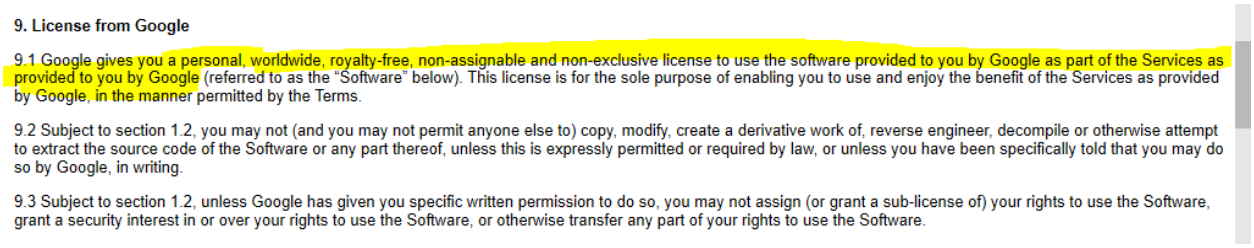
```
GNU LGPL information
--------------------

  This library is free software; you can redistribute it and/or
  modify it under the terms of the GNU Lesser General Public
  License as published by the Free Software Foundation; either
  version 2.1 of the License, or (at your option) any later version.
```

Figure 9 7Zip License Information

Additional Information can be found at: https://www.7-zip.org/license.txt and https://www.gnu.org/licenses/lgpl-3.0.en.html.

Google Chrome



9. License from Google

9.1 Google gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software provided to you by Google as part of the Services as provided to you by Google (referred to as the "Software" below). This license is for the sole purpose of enabling you to use and enjoy the benefit of the Services as provided by Google, in the manner permitted by the Terms.

9.2 Subject to section 1.2, you may not (and you may not permit anyone else to) copy, modify, create a derivative work of, reverse engineer, decompile or otherwise attempt to extract the source code of the Software or any part thereof, unless this is expressly permitted or required by law, or unless you have been specifically told that you may do so by Google, in writing.

9.3 Subject to section 1.2, unless Google has given you specific written permission to do so, you may not assign (or grant a sub-license of) your rights to use the Software, grant a security interest in or over your rights to use the Software, or otherwise transfer any part of your rights to use the Software.

Figure 10 Google Chrome License Information

Additional information can be found at: https://www.google.com/intl/en_sg/chrome/privacy/eula_text.html.

Update on Software/Configuration

RealVNC

We have added RealVNC software so that we may remote into our honeypot from outside the school network. We are utilizing a free 30-day trial period.

A. VNC SERVER ENTERPRISE EDITION END USER LICENCE AGREEMENT

PLEASE READ THIS AGREEMENT CAREFULLY. IN ORDER TO USE THE VNC SERVER ENTERPRISE EDITION SOFTWARE ("THE SOFTWARE"), YOU MUST FIRST ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT. BY USING ALL OR ANY PORTION OF THE SOFTWARE YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE THEN DO NOT USE THE SOFTWARE. BY USING ANY UPDATED VERSION OF THE SOFTWARE WHICH MAY BE MADE AVAILABLE, YOU ACCEPT THAT THE TERMS OF THIS AGREEMENT APPLY TO SUCH UPDATED SOFTWARE.

In this Agreement "Host" means the computer on which the Software is to be installed.

In this Agreement "Desktop" means a graphical user interface, whether accessible via a console attached to the Host, via the Software, or by any similar means.

You require a licence key for each Desktop that is to be made accessible using the Software.

1. Limited trial Period

A version of the Software is available for a limited trial period as set out in the Website. It will perform for only a limited period of time. THE LIMITED TRIAL SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY WARRANTY OR LIABILITY TO YOU WHATSOEVER.

More information on licensing can be found here:
https://archive.realvnc.com/products/vnc/documentation/4.6/win/licenses.pdf

White Hat

Intrusion Detection Plan

Our team will be utilizing the event viewer, which will be forwarded to a virtual machine running Splunk. With Splunk we will be able to isolate specific attacks, have alerts set up to send emails every time there is a successful login, and craft advanced search queries required for gathering data.

In addition to installing Splunk on a VM, there must be a Splunk Universal Forwarder installed on the Honeypot to establish the communication of data being captured.

Our initial intention was to use Zabbix monitor system health. However, there was no attacks performed that would impact system health and therefore trigger notifications from Zabbix. As a result, this section will not include any analysis using the Zabbix software.

Example of Searches Executed

Search One

The following search scans for all successful logins using the Windows Event code 4624, while excluding all logins from IP addresses assigned to our groups Pod in D316.

```
index=* Account_Name!=SYSTEM Account_Name!=DWM* Account_Name!=*SERVICE* (sourcetype="WinEventLog:System" OR source="WinEventLog:Security") (EventCode=4624) NOT (Source_Network_Address=127.0.0.1 OR Source_Network_Address=- OR Source_Network_Address=172.16.136.239 OR Source_Network_Address=172.16.136.237 OR Source_Network_Address=172.16.136.238) | eval loginID=mvindex(Logon_ID,-1) | eval account=mvindex(Account_Name,-1) | table _time,account,EventDesc,Source_Network_Address,loginID
```

Search Two

From the previous search, we are able to gather the time each login occurred, and through Splunk we are able to perform the following search to see all activity and isolate the results based on the time of each attack.

```
index=* Account_Name!=SYSTEM Account_Name!=LEAFCUTTERBEE$ NOT "C:\\Windows\\System32\\lsass.exe" NOT "EventCode=4798"  NOT "EventCode=4690"  NOT "C:\\Windows\\System32\\svchost"  EventDesc!="The Windows Filtering Platform has allowed a connection"  EventDesc!="The Windows Filtering Platform has permitted a bind to a local port" EventDesc!="The Windows Filtering Platform blocked a packet"  EventDesc!="The Windows Filtering Platform has blocked a connection" | table _time,Account_Name,EventDesc,Process_Name,Source_Network_Address,Source_Work*
```

Example of successful login

_time	account	EventDesc	Source_Network
2019-12-04 12:58:37	Administrator	An account was successfully logged on	172.16.136.101
2019-12-04 12:58:36	Administrator	An account was successfully logged on	172.16.136.101
2019-12-04 12:58:34	Administrator	An account was successfully logged on	172.16.136.101
2019-12-03 07:43:55	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:43:54	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:43:53	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:32:25	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:32:24	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:32:22	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:15:03	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:15:02	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:15:00	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:09:10	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:09:09	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:09:07	BruceOrca	An account was successfully logged on	172.16.138.75
2019-12-03 07:06:12	Administrator	An account was successfully logged on	172.16.138.75
2019-12-03 07:06:11	Administrator	An account was successfully logged on	172.16.138.75
2019-12-03 07:06:10	Administrator	An account was successfully logged on	172.16.138.75
2019-11-29 07:42:44	Administrator	An account was successfully logged on	172.16.136.228
2019-11-29 07:42:43	Administrator	An account was successfully logged on	172.16.136.228

All successful login attacks

Date	Account Logged In	Source IP Address
12-10-19 15:23	Administrator	172.16.136.226
12-9-19 15:11	Administrator	172.16.136.224
12-5-19 11:46	Administrator	172.16.136.214
12-4-19 17:23	Administrator	127.0.0.1
12-4-19 16:59	Administrator	127.0.0.1
12-4-19 16:29	Administrator	172.16.136.101
12-4-19 16:13	CBruce	127.0.0.1
12-4-19 16:07	CBruce	127.0.0.1
12-4-19 16:05	CBruce	127.0.0.1
12-4-19 12:58	Administrator	172.16.136.101
12-3-19 7:43	BruceOrca	172.16.138.75
12-3-19 7:32	BruceOrca	172.16.138.75
12-3-19 7:15	BruceOrca	172.16.138.75
12-3-19 7:09	BruceOrca	172.16.138.75
12-3-19 7:06	Administrator	172.16.138.75
11-29-19 7:42	Administrator	172.16.136.228

From the table above, we can deduce the logon and logoff times which and have been separated by the IP Address of the attack. For the purposes of this assignment, we have isolated our monitoring to remote access only, ignoring local log-on attempts by the KVM as a honeypot would not be accessible by this method. Due to the time constraints, we were only able to analyze select attacks.

Attack One

Intrusion Start Time:	2019-12-03 7:06
Intrusion End Time:	2019-12-03 7:46
IP of intruder:	172.16.138.75
Workstation Name:	INWSD311100
Details of attack:	The intrusion begins by a login to the account "Administrator" at 7:06 am. The intruder proceeds to open the server manager, followed by opening the computer management tool. The intruder proceeded to navigate to "Local Users and Groups" followed by the "Users" OU. They then proceeded to create a User named "Bruce Orca" with the SAM account name "BruceOrca". After creating the account, BruceOrca was than added to the group "Administrators" as well as had "Remote Desktop" enabled. The intruder proceeded to log off the Administrator's account and sign in to the new BruceOrca. At 7:10, the intruder signed off. At 7:15, the intruder signed back into BruceOrca. The intruder proceeds to open Computer management again and modified "BruceOrca" by removing the display name and again, signing off. At 7:32 the intruder signed back into "BruceOrca". The intruder once again opened Computer management and modified the "DefaultAccount" user to be set to enabled. The intruder proceeded the give the DefaultAccount a Password. The DefaultAccount was than added to the "Power Users" group. The intruder than carries on to sign off at 7:33AM. The indruder signs back into BruceOrca at 7:43AM and opens up windows explorer and modifies the "Desktop" properties. The intruder changed the security settings by adding "BruceOrca" to inherit the settings from Administrator. The intruder than opens the file "C:\Users\Administrator\Desktop\bleepBloop\Surprise!.txt". Next the intruder opened the "Test" folder located on the desktop followed by the folder "BleepBloop". The intruder finally opens the "Test" folder and opens a text file called "Blah.txt". At approximately 7:45, the intruder signed off and did not return.

Attack Two

Intrusion Start Time:	2019-12-09 15:11
Intrusion End Time:	2019-12-09 15:13
IP of intruder:	192.168.136.224
Workstation Name:	INWSD31614
Details of attack:	The intruder logged in, and opened up google chrome. This day, when logging into the server, the browser was open to "https://geekprank.com/hacker/" in fullscreen mode. This indicated the user did not sign off and left the account logged in.

Attack Three

Intrusion Start Time:	2019-12-05 11:45
Intrusion End Time:	2019-12-05 11:48
IP of intruder:	172.16.136.214
Workstation Name:	INWSD31604
Details of attack:	The intruder logged into "Administrator", once logged in they created a folder on the desktop and named it "Good Day" and saved the image "514da3b75f97c.jpeg" to this folder. They then proceeded to make this image the background image for the desktop user "Administrator".

Attack Four

Intrusion Start Time:	2019-12-10 15:23
Intrusion End Time:	2019-12-10 15:30
IP of intruder:	172.16.136.226
Workstation Name:	INWSD31616
Details of attack:	The Intruder logged into "Administrator" and opened up "notepad.exe" followed by saving the file as "destiny2.txt". The intruder then opened up "internet explorer", then opening "Google Chrome". The intruder than created a folder named "Good Day" on the desktop and saved the image "243789.png" to the picture folder. They then opened up the desktop system settings and modified the Desktop background to "243789.png".

Recommendations

Based on our attacks, we have a number of hardening recommendations from a “white hat” perspective. Please note that our recommendations assume we’re hardening an actual server deployed on a production environment.

Meaningful Logs. The production of logs is essential, being able to analyze data is a must for identifying vulnerabilities within your system. The first thing any system administrator should do is configure auditing and log management.

Analysis Software. Splunk has proven to be a useful component for our honeypot analysis, this is highly recommended if there are no other monitoring systems. It’s free for limited amounts of data!

Password Policy. Enabling a password policy that forces the users to change passwords frequently, as well as requiring strong passwords.

Disable Admin Account. A crucial change that all system administrators should make is disabling the default administrator account. From the data analyzed, this one the primary target for other teams. The next best recommendation would be creating custom domain groups with limited privileges based on the needs of the User.

Limit RDP Access. If you know which IP addresses will be remoting into the computer, limiting the scope of addresses that can connect through RDP.

Protect System from Changes Using Group Policy. From observation, a common change made to from computer was the desktop wallpaper. In group policy, it is possible to reset the desktop background when signing in. This is recommended to prevent any NSFW (Not Safe for Work) images from being saved as the background.

Black Hat

Planning

Acquire Credentials

Before undertaking our attacks, our initial reconnaissance will involve gathering information on each honeypot and their respective teams. Using social engineering tactics, we will attempt to deduce which honeypot belongs to which group. During this phase, we will also acquire the login credentials for both the Administrator and any additional accounts we can gather.

Exploratory Attacks

As the final portion of our reconnaissance, we will perform attacks to gather information. These attacks will be used to retrieve info on software, system configuration, and any other pertinent information.

Setup a Hidden User Account with Admin Privileges

During attacks, we will setup an account with admin privileges that is hidden using the registry (the only place the user will appear is in "local user and groups"). We can then use this account to perform future attacks. We believe this is beneficial in that we have another set of credentials if, for some reason, we are unable to use the credentials gathered during reconnaissance.

Cosmetic System Changes

We intend to make several cosmetic system changes to test how well the other honeypot systems are detecting our movement. *We will refrain from making any changes that risk compromising the system's security or health.*

Attacker IP Masking

We have developed an approach to attacking that we believe will partially mask our attacker IP. When performing attacks, we will start by performing an initial attack on a single honeypot (Honeypot #1). From Honeypot #1, we will mount an attack on a second honeypot (Honeypot #2). From Honeypot #2, we will mount an attack on a third honeypot, and so forth. When analysis occurs on honeypot #2 or #3, they'll see the preceding honeypot as the originating attacker instead of IP of the system we're using to perform attacks.

Results of Reconnaissance

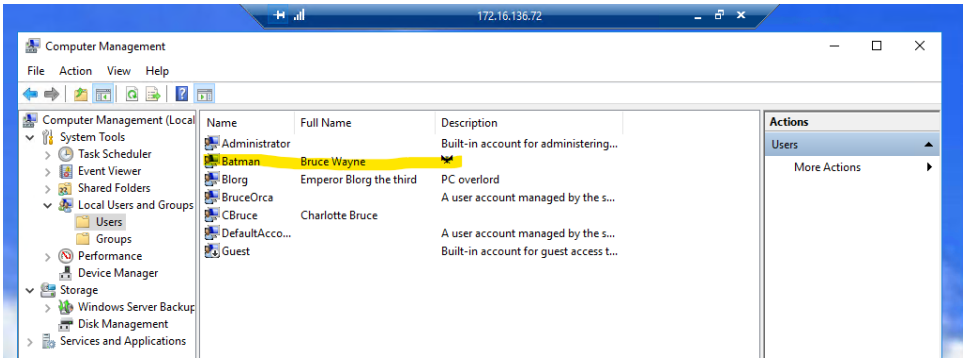
Honeypot Name	Honeypot IP	Suspected Group Members	Software Used	Credentials (user/password)
Honey	172.16.136.72	- Mitch J. - Courtney H. - Nick L - Nick W.	- 7Zip - HoneyBOT - Notepad ++ - Npcap - SolarWinds	- Administrator/Passw0rd - CBruce/Passw0rdCB - Batman/IAmBatman
Flower	172.16.136.74	- Kaelan W. - Nicholas H. - Kelvin T.	- 7Zip - Google Chrome - Network Monitor - Npcap - SoftPerfect - VNC Server - Wireshark	- Administrator/Passw0rd - CBruce/Passw0rdCB - Batman/IAmBatman
Bumble	172.16.136.75	- Tom M. - Robert L. - Joshua B.	- 7Zip - Google Chrome - ManageEngine - Network Monitor - NPcap - Oracle VM Virtual Box - VNC Server	- Administrator/Passw0rd - CBruce/Passw0rdCB - Batman/IAmBatman
Mason	172.16.136.76	- Sergio M. - Jessey H. - Gordon M. - Erin C.	- 7Zip - Notepad ++ - Google Chrome - UltraVNC - PRTG	- Administrator/Passw0rd - CBruce/Passw0rdCB - Batman/IAmBatman
Mining	172.16.136.77	- Troy K. - Kien O. - Griffin W.	- 7Zip - Network Monitor - Google Chrome - Notepad++ - OSSEC - Putty - VNC Server - Wireshark	- Administrator/Passw0rd - CBruce/Passw0rdCB - Batman/IAmBatman

Attacks Performed

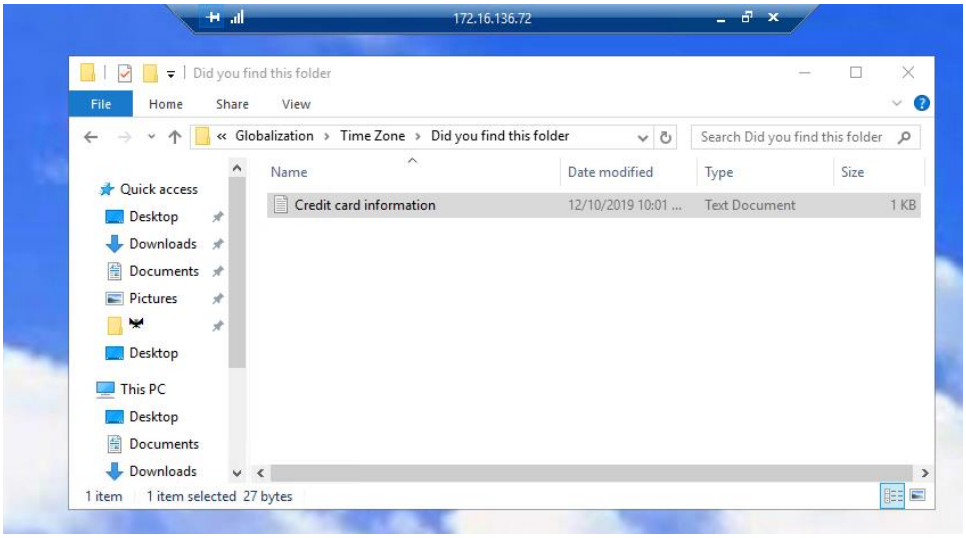
Team Honey

IP: 172.16.136.72

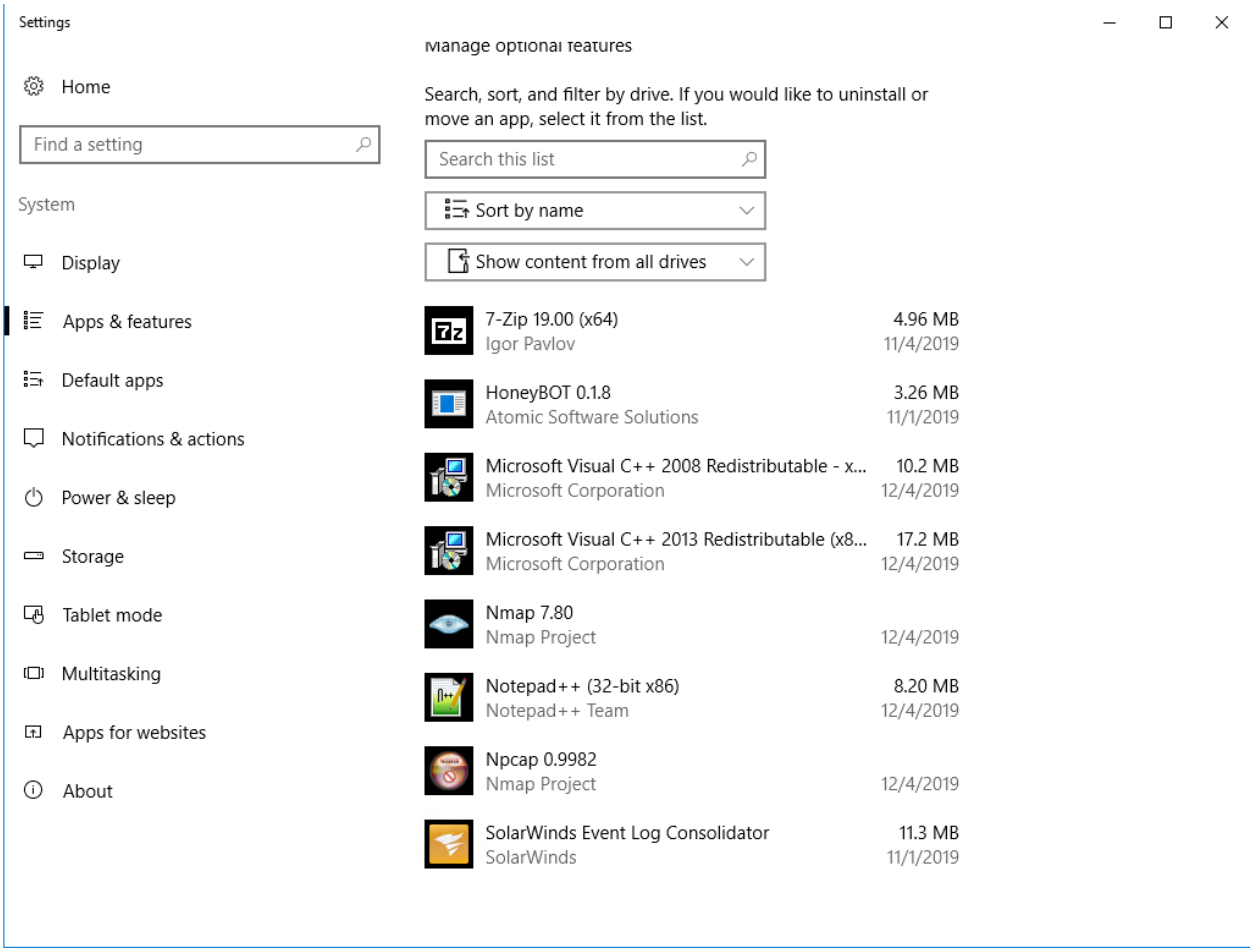
Date	Time	Attacker IP	Port	Protocol
12/04/2019	4:30pm	172.16.136.73	3389	RDP
Details				
• Created user Batman – pass IAmBatman • Added to Administrators group • Folder on CBruce desktop with Batman picture in it • Folder on Administrator desktop with Batman picture in it • Changed registry key to hide user “Batman” (still can be seen on local user and groups though)				



Date	Time	Attacker IP	Port	Protocol
12/10/2019	9:57	172.16.136.73	3389	RDP
Details				
• Create “Credit card information.txt” text file on C:\Windows\Globalization\Time Zone\Did you find this folder • Accessed “How To Setup Auditing Without DC.pdf” on Administrator’s desktop • Accessed .zip file on C:\Scripts password was “Passw0rd”				

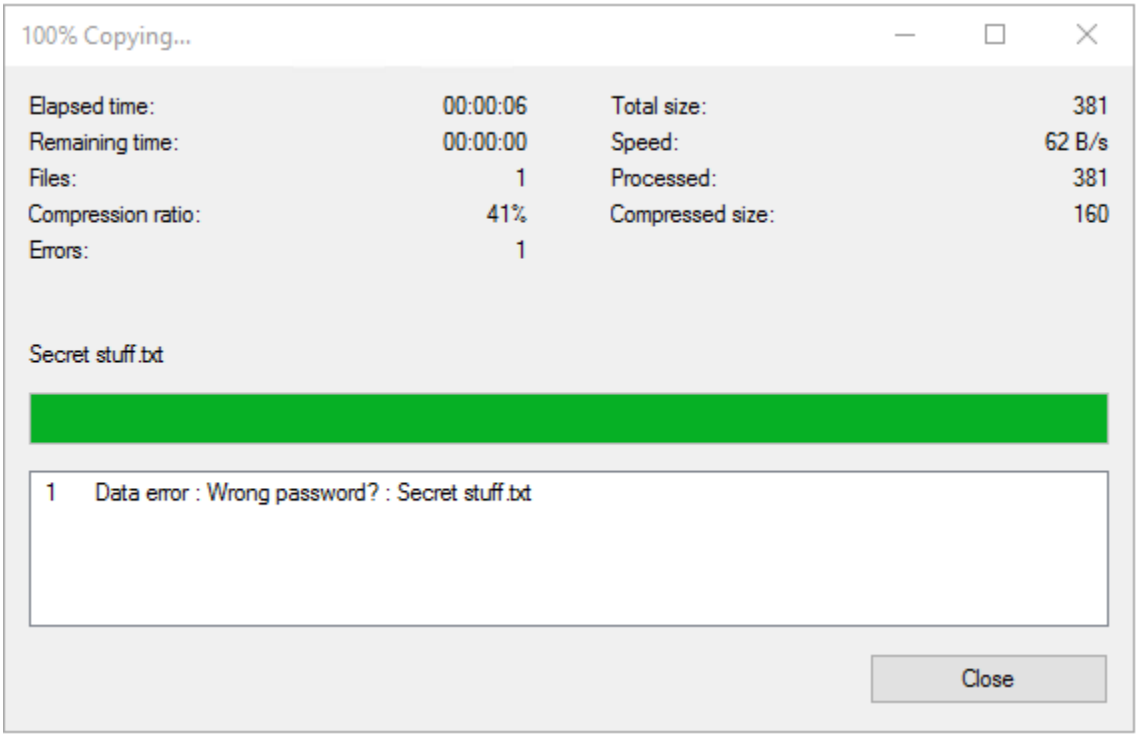


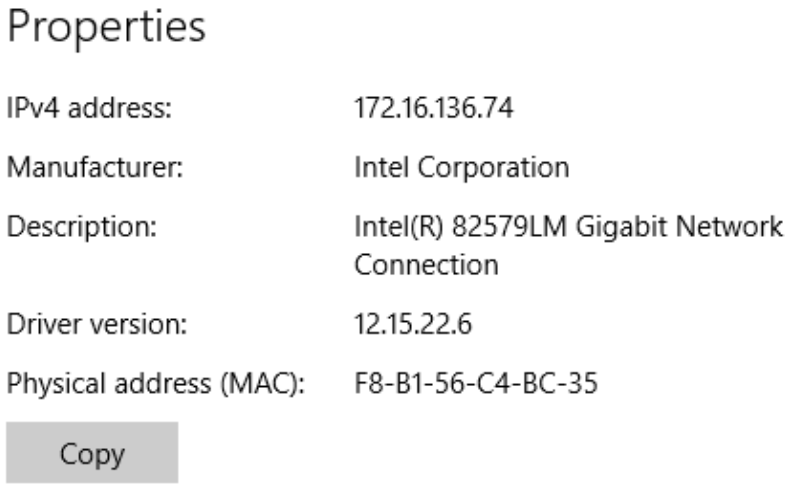
Date	Time	Attacker IP	Port	Protocol
12/10/2019	2:44 PM	172.16.136.238	3389	RDP
Details				
• Logged in with Administrator account • Information gathering to explore system and collect data on software installed				



Team Flower
IP: 172.16.136.74

Date	Time	Attacker IP	Port	Protocol
11/20/2019	4:00 PM	172.16.136.238	3389	RDP
Details				
• Accessed How to Audit Without a DC document • Tried to access C:\Scripts\Smile.7z • Entered several wrong passwords to access Smile.7z. • Accessed connection properties				

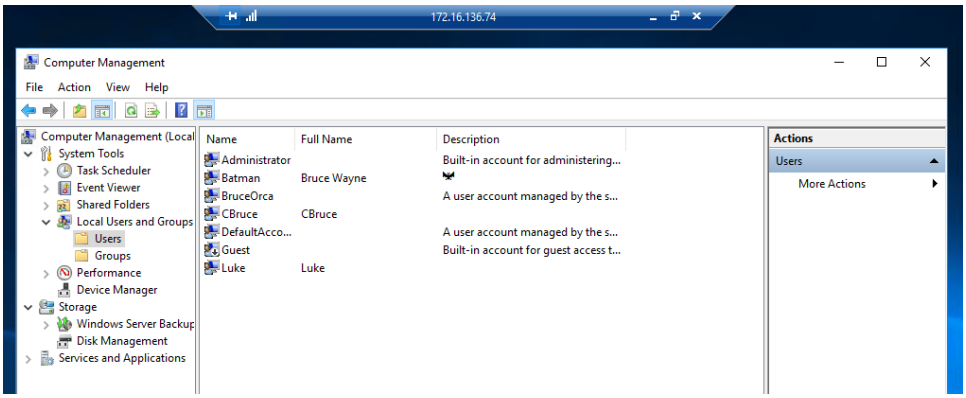




Date	Time	Attacker IP	Port	Protocol
12/04/2019	11:30am	172.16.136.237	3389	RDP

Details

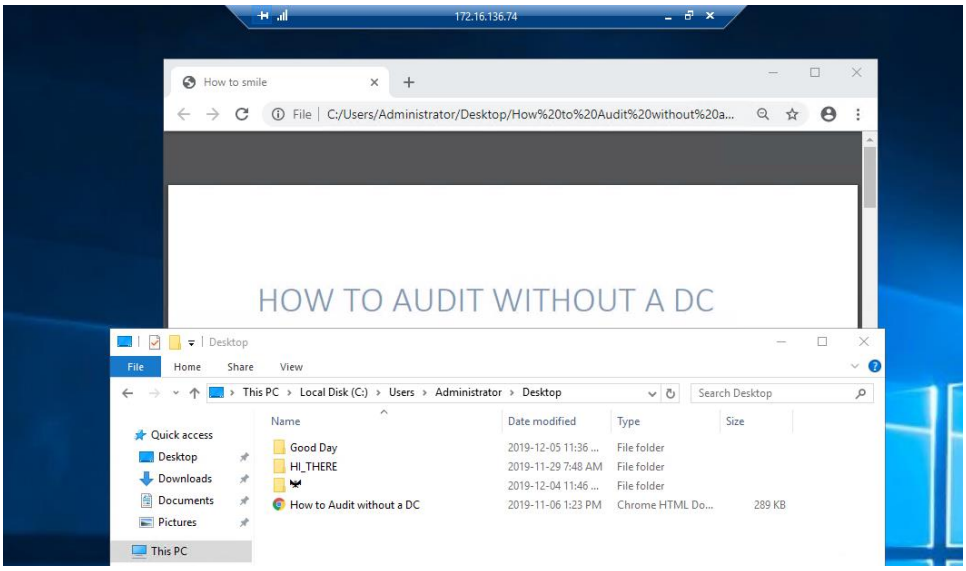
- Created user Batman – pass IAmBatman
- Added to Administrators group
- Folder on Cbruce desktop with Batman picture in it
- Folder on Administrator desktop with Batman picture in it
- Changed registry key to hide user “Batman” (still can be seen on local user and groups though)



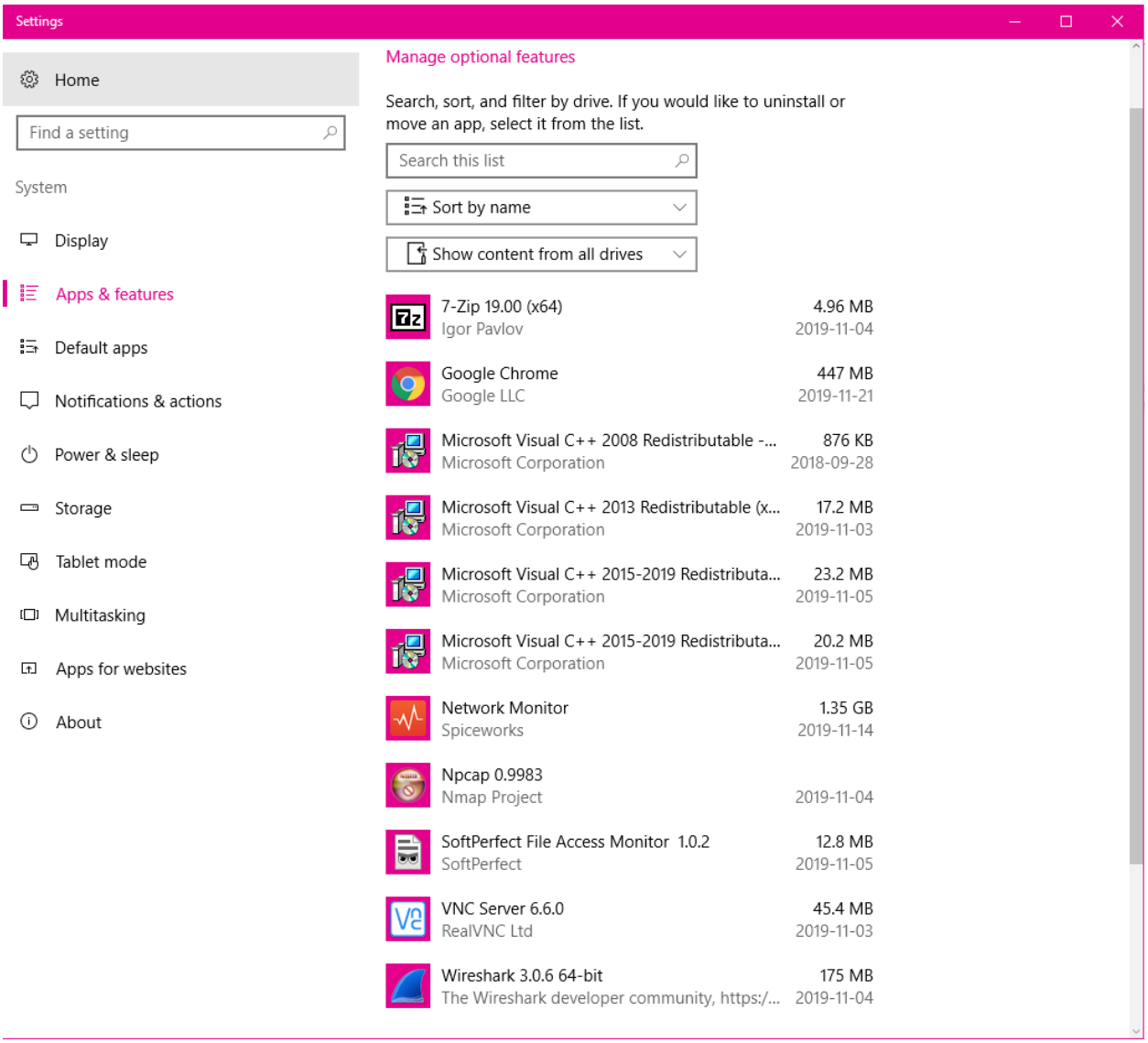
Date	Time	Attacker IP	Port	Protocol
12/10/2019	10:17am	172.16.136.237	3389	RDP

Details

- Create “Credit card information.txt” text file on C:\Windows\Cluster\en-US\Did you catch this
- Accessed .7z file on C:\Scripts document - couldn’t find the password for the file
- Accessed “How To Audit Without DC.pdf” on Administrator’s desktop



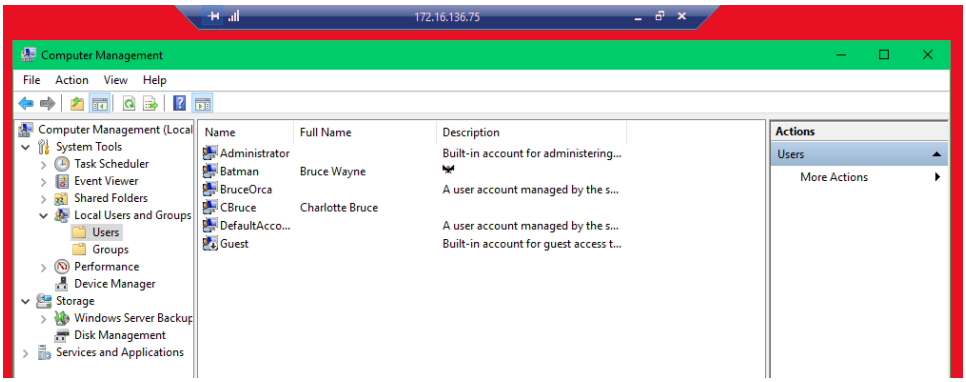
Date	Time	Attacker IP	Port	Protocol
12/10/2019	2:41 PM	172.16.136.238	3389	RDP
Details				
• Logged in with Administrator account • Information gathering to explore system and collect data on software installed				



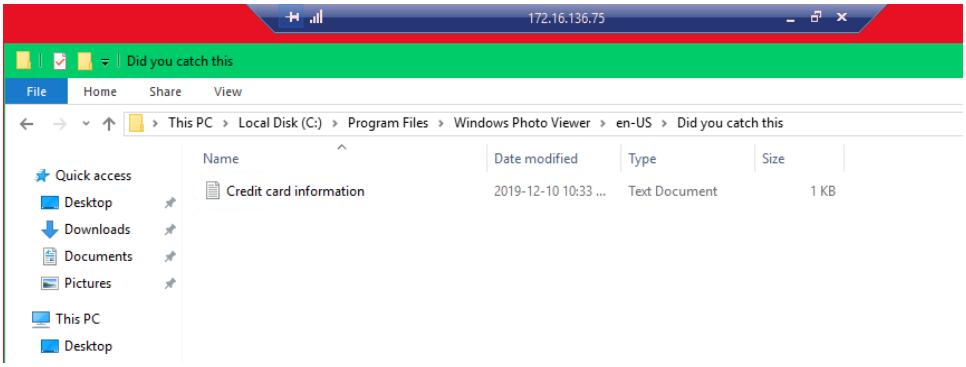
Team Bumble

IP: 172.16.136.75

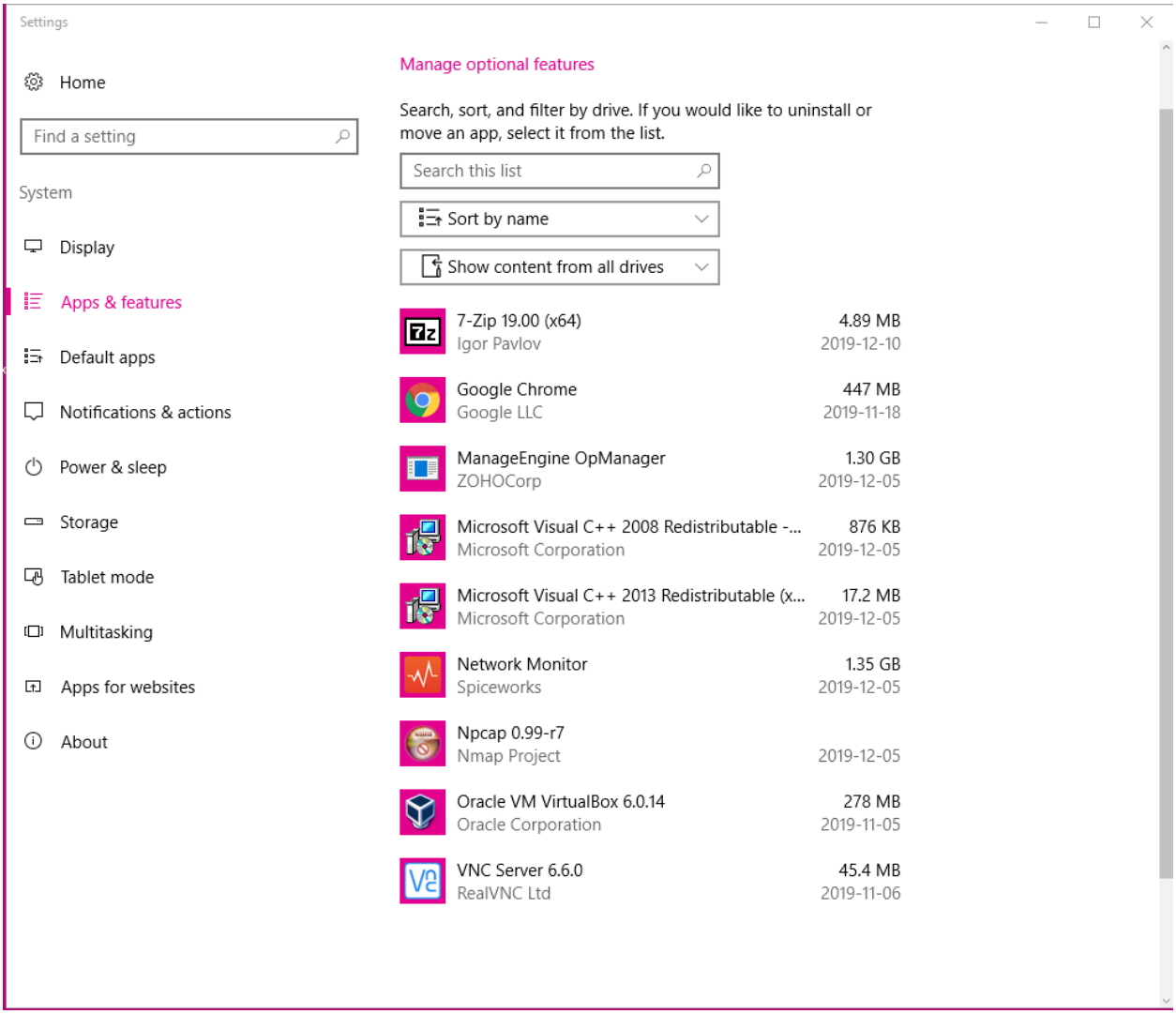
Date	Time	Attacker IP	Port	Protocol
12/04/2019	5:10pm	172.16.136.73	3389	RDP
Details				
• Created user Batman – pass IAmBatman • Added to Administrators group • Folder on Cbruce desktop with Batman picture in it • Folder on Administrator desktop with Batman picture in it • Changed registry key to hide user “Batman” (still can be seen on local user and groups though)				



Date	Time	Attacker IP	Port	Protocol
12/10/2019	10:30am	172.16.136.237	3389	RDP
Details				
• Create “Credit card information.txt” C:\Program Files\Windows Photo Viewer\en-US\Did you catch this • Accessed .zip file on C:\Scripts - couldn’t find the password for the file • Accessed “Audit Policy PDF.pdf” on Administrator’s desktop				

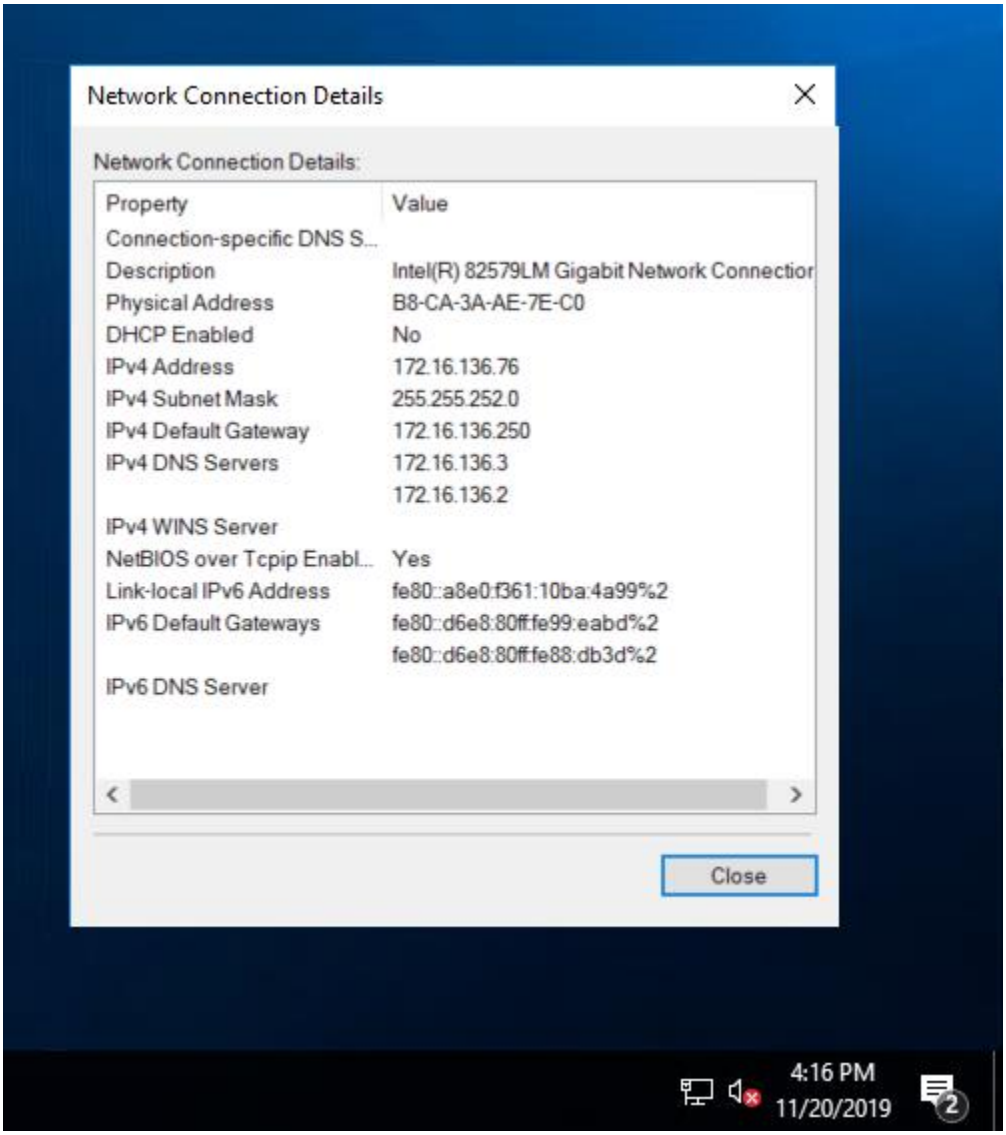


Date	Time	Attacker IP	Port	Protocol
12/10/2019	2:24 PM	172.16.136.238	3389	RDP
Details				
• Logged in with Administrator account • Information gathering to explore system and collect data on software installed				



Team Mason
IP: 172.16.136.76

Date	Time	Attacker IP	Port	Protocol
11/20/2019	4:16pm	172.16.136.238	3389	RDP
Details				
• Viewed network configuration details • Accessed How to Audit Without a DC document				

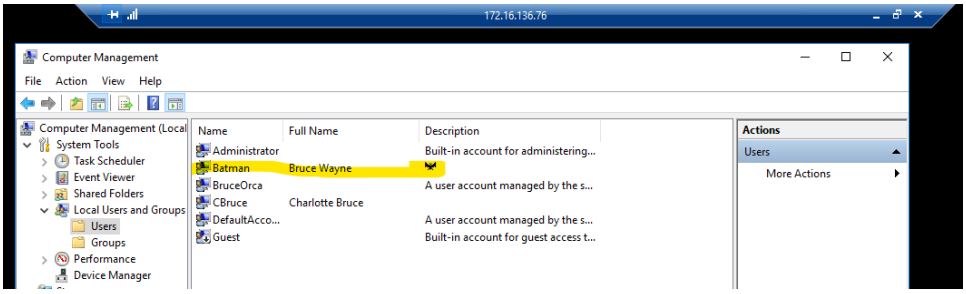


Date	Time	Attacker IP	Port	Protocol
12/04/2019	5:27pm	172.16.136.73	3389	RDP
Details				

- Created user Batman – pass IAmBatman
- Added to Administrators group
- Folder on CBruce desktop with Batman picture in it
- Folder on Administrator desktop with Batman picture in it
- Changed registry key to hide user “Batman” (still can be seen on local user and groups though)

12/05 - Logged from 172.16.136.73 (Leafcutter HoneyPot)

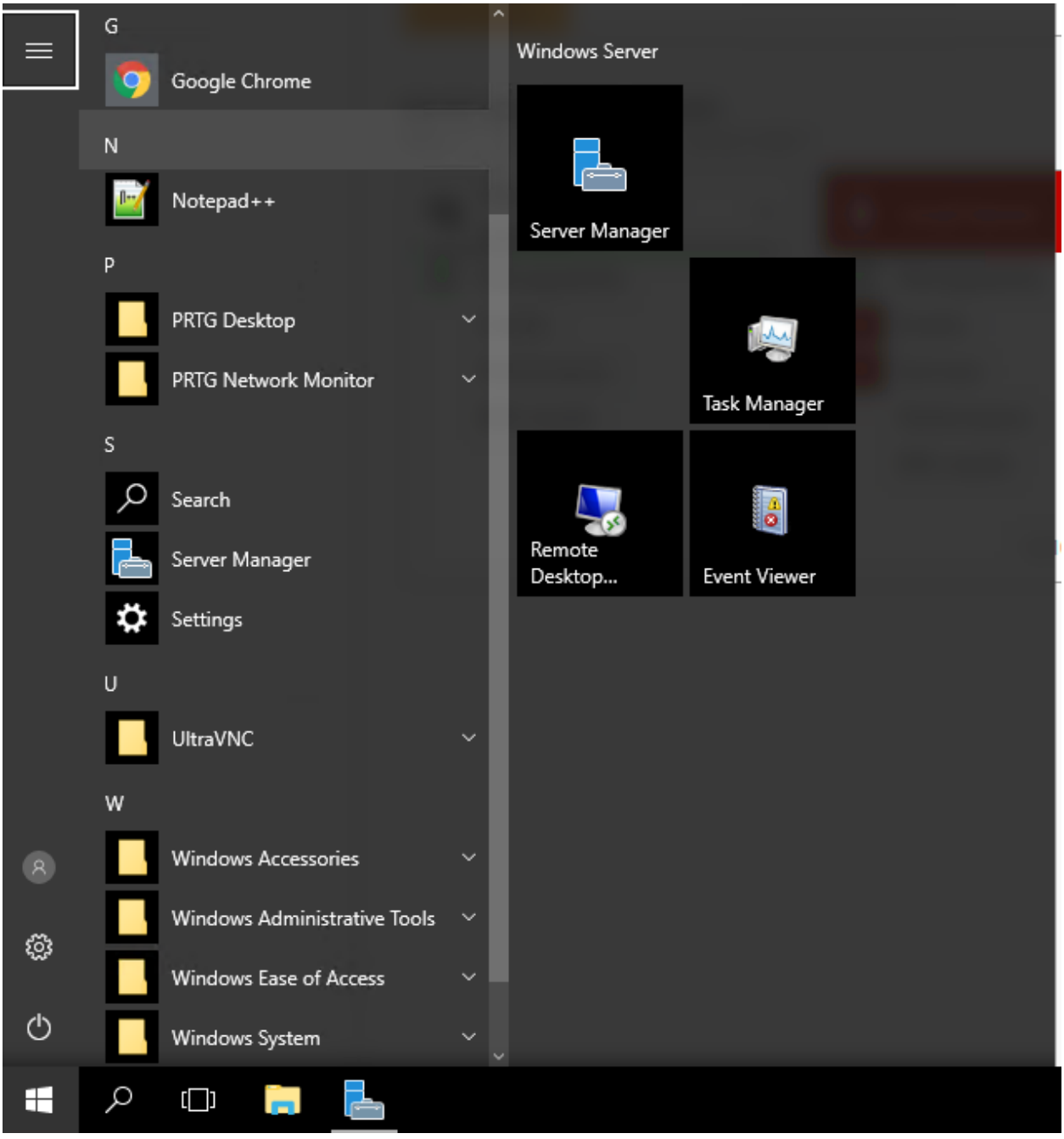
- Changed system colors
- Added hundreds of icons to desktop (does it create a log for it?)
- Hid Batman home folder
- Changed group policy to block personalization of the system (colors, themes, mouse pointer, etc.)



Date	Time	Attacker IP	Port	Protocol
12/10/2019	10:42am	172.16.136.75	3389	RDP
Details				

- Create “Credit card information.txt” C:\Program Files (x86)\Common Files\Services\Did you catch this
- Accessed .zip file on C:\Scripts – file is not password protected

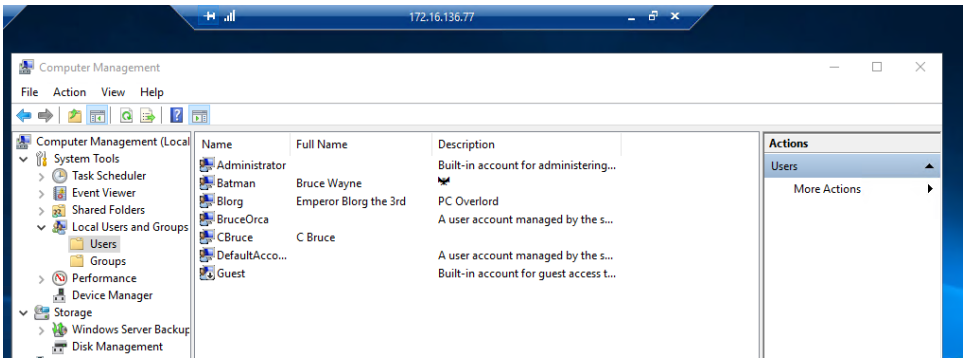
Date	Time	Attacker IP	Port	Protocol
12/10/2019	3:10 PM	172.16.136.238	3389	RDP
Details				
• Logged in with Batman account • Information gathering to explore system and collect data on software installed				



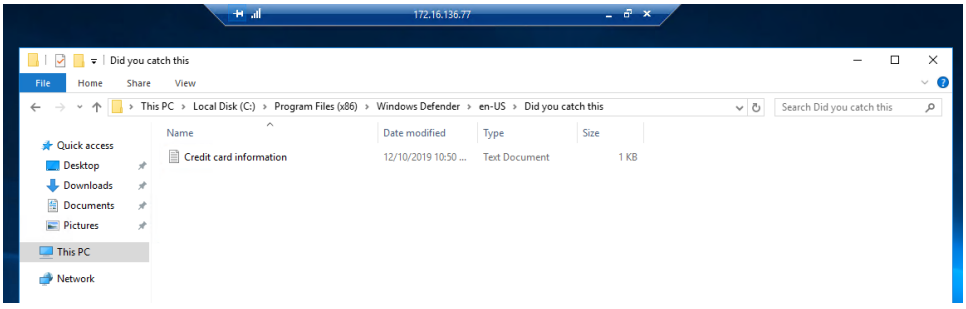
Team Mining

IP 172.16.136.77

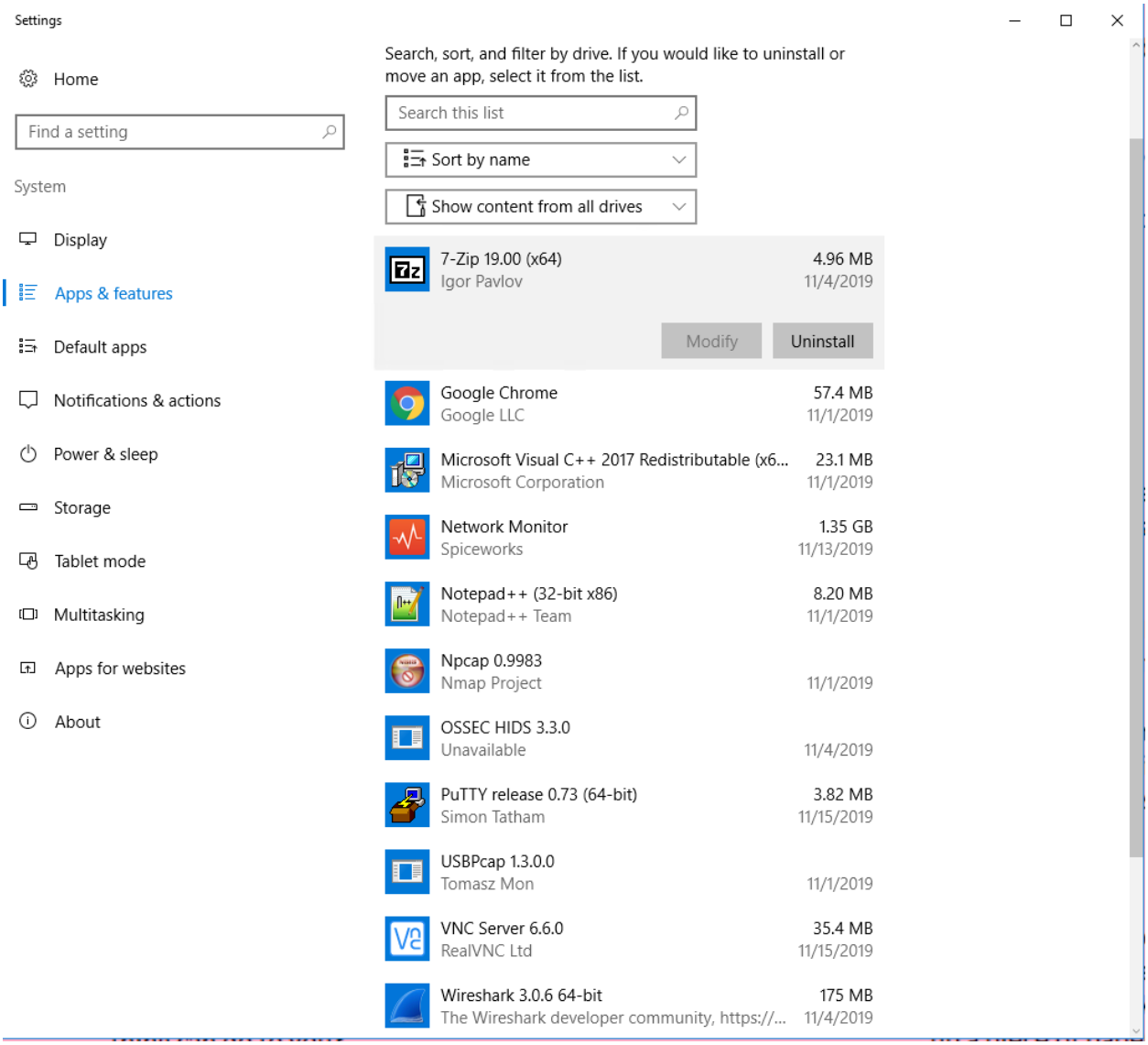
Date	Time	Attacker IP	Port	Protocol
12/04/2019	6:00pm	172.16.136.76	3389	RDP
Details				
• Created user Batman – pass IAmBatman • Added to Administrators group • Folder on CBruce desktop with Batman picture in it • Folder on Administrator desktop with Batman picture in it • Changed registry key to hide user “Batman” (still can be seen on local user and groups though)				



Date	Time	Attacker IP	Port	Protocol
12/10/2019	10:48am	172.16.136.76	3389	RDP
Details				
• Create “Credit card information.txt” C:\Program Files (x86)\Windows Defender\en-US\Did you catch this • Accessed .zip file on C:\Scripts - couldn’t find the password for the file				



Date	Time	Attacker IP	Port	Protocol
12/10/2019	2:14 PM	172.16.136.238	3389	RDP
Details				
• Logged in with Administrator account • Information gathering to explore system and collect data on software installed				



Recommendations

Based on our attacks, we have a number of hardening recommendations from a “black hat” perspective. Please note that our recommendations assume we’re hardening an actual server deployed on a production environment.

Limit physical access. Limit - as much as possible - physical access to the machine or room where it’s stored. This will prevent a variety of physical attacks that can be performed by malicious parties.

Disable administrator account. Renaming and also disabling this account is good practice, as you don’t want the default account with full privileges to be used.

Control logon hours. Determine which users require necessary access outside of regular working hours. All other users that do not require access outside of working hours should be limited by group policy.

Limit or disable RDP Access. Only allow users with network level authentication to access remotely. If there’s no need for remote connect to that server, completely disable RDP. To further secure RDP connection, make sure to use a VPN so only tunneled connections are allowed.

Proper monitoring software. During infiltration, we noticed several honeypots that lacked monitoring software capable of tracking movement across their system in a meaningful way. We would recommend the use of more robust software and, in the case of an actual production scenario, enterprise-grade versions of said software.

Train users to reduce effectiveness of social engineering. We were able to deduce the personal identities of the honeypot administrators by using a variety of social engineering tactics. Our recommendation is that administrators take greater care in protecting sensitive information that may be used in a malicious attack.

Take action after an attack. We noticed on several servers that none of the modifications made by attackers were not addressed or resolved. This means the system is still vulnerable. We recommend that immediate action be taken as soon as an administrator becomes aware of an attack.

References

Melnik, J. (2018, August 23). *Auditing Windows Systems*. Retrieved from Netwrix: https://blog.netwrix.com/2018/08/23/auditing-windows-server/

Solarwinds. (2017). *Enable File Auditing in Windows*. Retrieved from Solarwinds : https://support.solarwinds.com/SuccessCenter/s/article/Enable-File-Auditing-in-Windows

Wikipedia. (2019, October 22). *Zabbix*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Zabbix

Appendix A: Team Rubrics

Adriano

Criteria	Adriano	Alex	Mohammed	Zach
Attendance	2	2	2	2
Submission deadline	2	2	2	2
Quality of Work	2	2	2	2
Communication	2	2	2	2
Participation	2	2	2	2

Alex

Criteria	Adriano	Alex	Mohammed	Zach
Attendance	2	2	2	2
Submission deadline	2	2	2	2
Quality of Work	2	2	2	2
Communication	2	2	2	2
Participation	2	2	2	2

Mohammed

Criteria	Adriano	Alex	Mohammed	Zach
Attendance	2	2	2	2
Submission deadline	2	2	2	2
Quality of Work	2	2	2	2
Communication	2	2	2	2
Participation	2	2	2	2

Zach

Criteria	Adriano	Alex	Mohammed	Zach
Attendance	2	2	2	2
Submission deadline	2	2	2	2
Quality of Work	2	2	2	2
Communication	2	3	2	2
Participation	2	2	2	2

Appendix B: Work Logs

Adriano Valenga Carneiro

Time spent on project:	12 hours
Details of work completed:	Attended meetings with group. Did the attacks. Assisted in final edits. Assisted in final recommendations. Provided research for planning and recommendations.

Alex Kelly

Time spent on project:	12 Hours
Details of work completed:	Attended group meetings. Undertook black hat reconnaissance including social engineering and information gathering. Performed a series of attacks for information gathering purposes. Wrote Black Hat Planning and Recommendation sections. Compiled and performed final edits on document.

Mohammed Hussain

Time spent on project:	10
Details of work completed:	Attended group meetings and coordinate with Zack and other group members roles and took on the white hat role and monitoring black hat activity. Set up auditing and data analysis software on the Honeypot and VM monitoring the Honeypot. Most time was spent analyzing the data captured.

Zach Slaunwhite

Time spent on project:	**15~ Hours**
Details of work completed:	Attended group meetings, finalized group members roles and took on the white hat role and monitoring black hat activity. Set up auditing and data analysis software on the Honeypot and VM monitoring the Honeypot. Most time was spent analyzing the data captured.

Appendix C: Team Charter

Members

Adriano Carneiro – Primary Team Lead
Alex Kelly – Secondary Team Lead
Mohammed Hussain – Team Member
Zach Slaunwhite – Team Member

Structure

The team will be led by our primary lead, Adriano Carneiro. A secondary lead, Alex Kelly, has been assigned as backup.

Team Lead Responsibilities

The team lead will act as the glue holding the team together. He is responsible for setting the pace, offering encouragement, motivating the team, and keeping communication flowing. The team lead will also ensure team members are meeting goals based on project-specific timelines.
It is the team lead's responsibility to ensure deadlines are being met. In situations where a team member is unable to meet a deadline, the team lead will coordinate with the group to ensure deliverables are completed within the project's timeline.
The team lead will review submitted work to ensure project requirements have been met. If additional work is required, a team discussion will take place to ensure said work is completed. The team lead will also be responsible for putting the final assignment documentation together, as well as submitting said document to the correct drop box on Brightspace. Final submissions will take place prior to the SAAD1002 class on Thursdays.

Team Member Responsibilities

Team Contribution

Team members are expected to contribute to all aspects of a project. From attending meetings to the final revision of deliverables, team members must spend a fair share of time researching, compiling, and creating documentation.

Individual Work and Deadlines

It's the members responsibility to complete their assigned part of the project. Assigned work must be completed on the day prior to the project's due date. Members will upload completed work into the OneDrive folder created for the group, as a means of centralizing all work created. Team members may contact the team lead to arrange for additional resources in completing their assigned tasks. If a team member is unable to complete their assigned work for any reason, the team lead must be informed immediately.

Individual Work Logs

Team members are responsible for logging their time spent during weekly activities, as well as describing the work performed during the project. Individual work logs will also be uploaded to the OneDrive folder.

Quality of Work

Individual work contributions are expected to be of acceptable quality as determined by the team lead. Acceptable quality is defined as meeting all outcomes based on project requirements, in addition to any outcomes specified by the team.

Communication Efforts

It is the member's responsibility to ensure proper communication is maintained throughout all projects. In the event of extraordinary circumstances, team members will make every effort possible to communicate the situation to their peers to ensure proper action can be taken. If, for any reason, a team member fails to communicate during an extended period or maintains absence from meetings/classes without explanation, it's the team leader's responsibility to try and communicate with said team member(s). In the event no communication can be established, marks will be deducted from the rubric, and the member's name will not be added to that part of the project.

Meetings

Meeting Guidelines

Meetings will take place a minimum of once per week when a project is active. To best utilize time, the team will attempt to schedule meetings within the following time periods:

- Between classes on Mondays, Wednesdays, Thursdays.
- Class labs scheduled by the faculty member who assigned the project.

Meeting frequency may increase or decrease at the team's discretion, as required by on-going projects. In some cases, meetings may take place online through Discord voice or text communication. Team members are expected to attend all meetings.

Project Initiation

Once a project is assigned, an initial meeting will take place at the team's earliest availability. During this meeting, the team will begin planning the project and delegating individual tasks through discussion. A meeting schedule for the project, based on the Meeting Guidelines, will be developed at this time.

Final Review

When applicable, the team will convene in-class, on the project's due date, to finalize deliverables for submission. In situations where the team cannot meet in-class for a final review, alternate plans will be decided upon.

Decision Making

Decisions, unless specified otherwise within this charter, will be made as a team. When a decision is required, the team will discuss options and attempt to reach unanimous consensus. If unanimous consensus is not possible, discussion will continue until a solution is proposed that has majority support. I think we're good since it's covered in conflict resolution. If it gets to a point where we need to involve faculty, it has probably become a conflict.

Conflict Resolution

At the beginning of each meeting, team members will have an opportunity to voice their issues. Once an issue has been identified, the team will discuss and evaluate the issue. Next, the team will try to mediate and remedy the issue through dialog and/or action. Any required actions will be decided upon using the methods outlined in Decision Making. In the extreme case that an issue cannot be resolved internally - despite the group's best efforts - said issue will be elevated to the relevant faculty member.

Other Communication Channels

Outside of class meetings, communication will primarily take place using the following channels:

- Discord for informal and/or time-sensitive communication.
- Group Email for formal and/or important communication.

Team members may use their own discretion when deciding which channel to use for their communication. However, all communication relating to the project will take place where the entire group can participate. One-on-one communication regarding the project will be avoided to ensure all team members are on the same page.

Charter Amendments

As our team evolves, we recognize that our approach to teamwork and project management may shift and change. Resultantly, charter amendments may occur to reflect these changes. Team members may propose a written amendment to the team charter during our weekly team meeting. The proposal will be put to a vote and, if approved by majority rule, the team will begin work on preparing a final draft of the amendment. Once the final draft has been created and approved, the amendment will be added to the charter.