CTF Final Document:

Cover Page

Network Map

**Marketing Division – 10.1.8.1**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

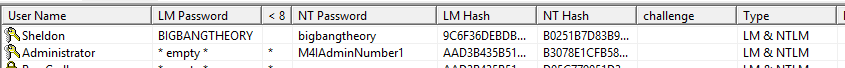
How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| Administrator | Admin | M4IAdminNumber1 |
| Sheldon |  | bigbangtheory |
| HarryPotter |  |  |
| BearGrylls |  |  |
| sneakers |  |  |



**Machine Division – 10.1.8.101**

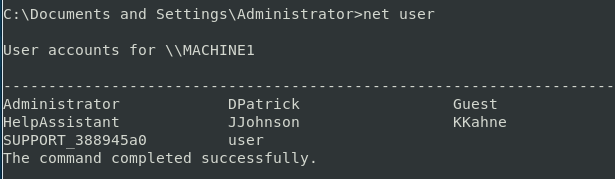
How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

* After using an SSH login with the Administrator account, we ran the “net user” command, showing the below output:



How did you learn passwords?

* To learn the Administrator password, we leveraged the cracked password for Marketing1’s Administrator, and used the hint below from the Twitter profile:



How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| Administrator | Admin | M4IAdminNumber2 |
| DPatrick |  |  |
| JJohnson |  |  |
| KKahne |  |  |
| user |  |  |

**Music Division – 192.168.2.1**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| doors | User | PeopleAre5trange |
| Penny |  |  |
| Pinkfloyd |  |  |
| root |  | \*uses password in all-words.txt |

**Management Division – 192.168.2.101**

How did you find the target?

* We inspected the page source of main.m4i.local using “ctrl u”. In the page source, two photos were pulled from remote sources, one from the Movie and one from the Management division shown below:



How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Movie Division – 192.168.3.1**

How did you find the target?

* We inspected the page source of main.m4i.local using “ctrl u”. In the page source, two photos were pulled from remote sources, one from the Movie and one from the Management division shown below:



How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Military Division 192.168.3.101**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Medical Division – 172.22.22.1**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Meteorology Division**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Mitnick Division – 192.168.3.201**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Marconi Division**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Make Division**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Table of all usernames and passwords:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Division** | **Username** | **Account Type** | **Password** |
|  |  |  |  |  |
|  |  |  |  |  |

**Supplemental Questions:**

1. List the restaurants Dr. Evil visits frequently
2. What is the password learned from the Heartbeat Server

**Source Code:**

**General Observations:**

* You are required to keep a log of time spent on this assignment and include the log in this appendix.
* How long (in wall clock hours; not man hours) did it take to complete the project excluding the report?
* How long (in wall clock hours; not man hours) did it take to prepare the report?
* Was it an appropriate length final assignment considering the time allotted?
* What corrections and or improvements do you suggest for this project?
  + Please be specific, and if you add new material, give the exact wording/instructions you would give future students in the new project handout. Feel free to cross out and edit text to make minor corrections/suggestions.