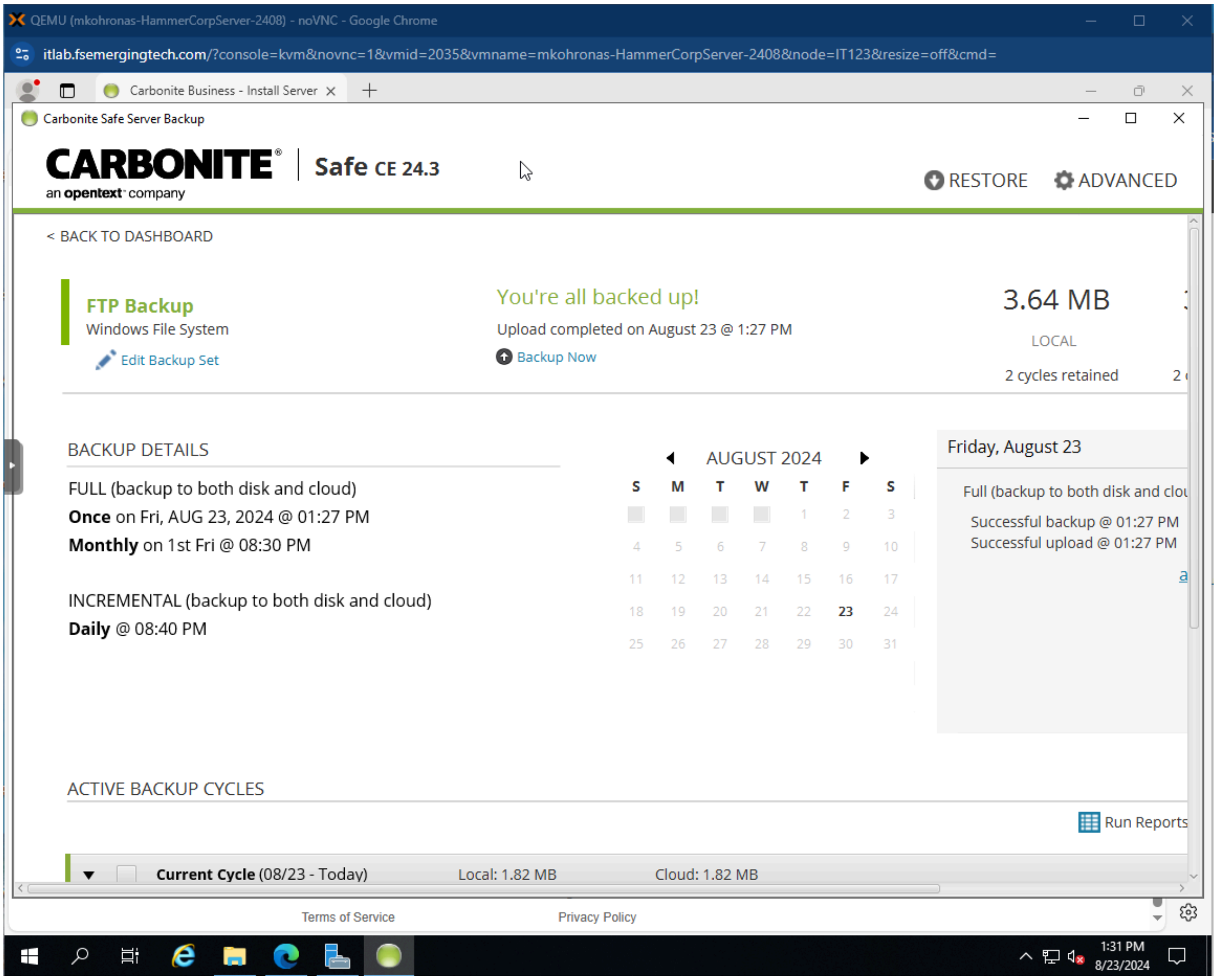
#1


QEMU (mkohronas-HammerCorpServer-2408) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=2035&vmname=mkohronas-HammerCorpServer-2408&node=IT123&resize=off&cmd=
Carbonite Business - Install Server
Carbonite Safe Server Backup
CARBONITE®
an opentext™ company
Safe CE 24.3
RESTORE
ADVANCED
< BACK TO DASHBOARD
Edit Backup Set
Backup Now
Run Reports
Terms of Service
Privacy Policy
1:31 PM
8/23/2024

FTP Backup
Windows File System

You're all backed up!
Upload completed on August 23 @ 1:27 PM

3.64 MB
LOCAL
2 cycles retained

BACKUP DETAILS

FULL (backup to both disk and cloud)
Once on Fri, AUG 23, 2024 @ 01:27 PM
Monthly on 1st Fri @ 08:30 PM

INCREMENTAL (backup to both disk and cloud)
Daily @ 08:40 PM

AUGUST 2024

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Friday, August 23

Full (backup to both disk and clou
Successful backup @ 01:27 PM
Successful upload @ 01:27 PM

ACTIVE BACKUP CYCLES

Current Cycle (08/23 - Today) Local: 1.82 MB Cloud: 1.82 MB

#2

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-23 13:49 Pacific Daylight Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:49
Completed NSE at 13:49, 0.00s elapsed
Initiating NSE at 13:49
Completed NSE at 13:49, 0.00s elapsed
Initiating NSE at 13:49
Completed NSE at 13:49, 0.00s elapsed
Initiating ARP Ping Scan at 13:49
Scanning 172.16.1.115 [1 port]
Completed ARP Ping Scan at 13:49, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:49
Completed Parallel DNS resolution of 1 host. at 13:49, 0.01s elapsed
Initiating SYN Stealth Scan at 13:49
Scanning 172.16.1.115 [65535 ports]
Discovered open port 21/tcp on 172.16.1.115
Discovered open port 80/tcp on 172.16.1.115
Discovered open port 135/tcp on 172.16.1.115
Discovered open port 139/tcp on 172.16.1.115
Discovered open port 445/tcp on 172.16.1.115
SYN Stealth Scan Timing: About 21.08% done; ETC: 13:52 (0:01:56 remaining)
Discovered open port 10090/tcp on 172.16.1.115
SYN Stealth Scan Timing: About 52.47% done; ETC: 13:51 (0:00:55 remaining)
Discovered open port 49666/tcp on 172.16.1.115
Discovered open port 5985/tcp on 172.16.1.115
Discovered open port 49667/tcp on 172.16.1.115
Completed SYN Stealth Scan at 13:51, 104.14s elapsed (65535 total ports)
Initiating Service scan at 13:51
Scanning 9 services on 172.16.1.115
Completed Service scan at 13:52, 53.77s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 172.16.1.115
Retrying OS detection (try #2) against 172.16.1.115
NSE: Script scanning 172.16.1.115.
Initiating NSE at 13:52
Completed NSE at 13:53, 40.91s elapsed
Initiating NSE at 13:53
Completed NSE at 13:53, 1.15s elapsed
Initiating NSE at 13:53
Completed NSE at 13:53, 0.00s elapsed
```

```
Nmap scan report for 172.16.1.115
Host is up (0.0033s latency).
Not shown: 65526 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ssl-cert: Subject: commonName=WMSvc-SHA2-HAMMERCORP
| Issuer: commonName=WMSvc-SHA2-HAMMERCORP
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-08-23T20:28:52
| Not valid after:  2034-08-21T20:28:52
| MD5:   7c9a:0cac:2fc2:219c:ec2e:299c:7182:5e3b
|_SHA-1: 47b5:980a:1ace:3736:f521:6cad:a6a0:e655:3c24:fcde
| ftp-syst:
|_  SYST: Windows_NT
|_ssl-date: 2024-08-23T20:53:02+00:00; 0s from scanner time.
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
10090/tcp open  unknown
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
MAC Address: BC:24:11:50:3B:0E (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (97%)
Aggressive OS guesses: Microsoft Windows Server 2019 (97%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

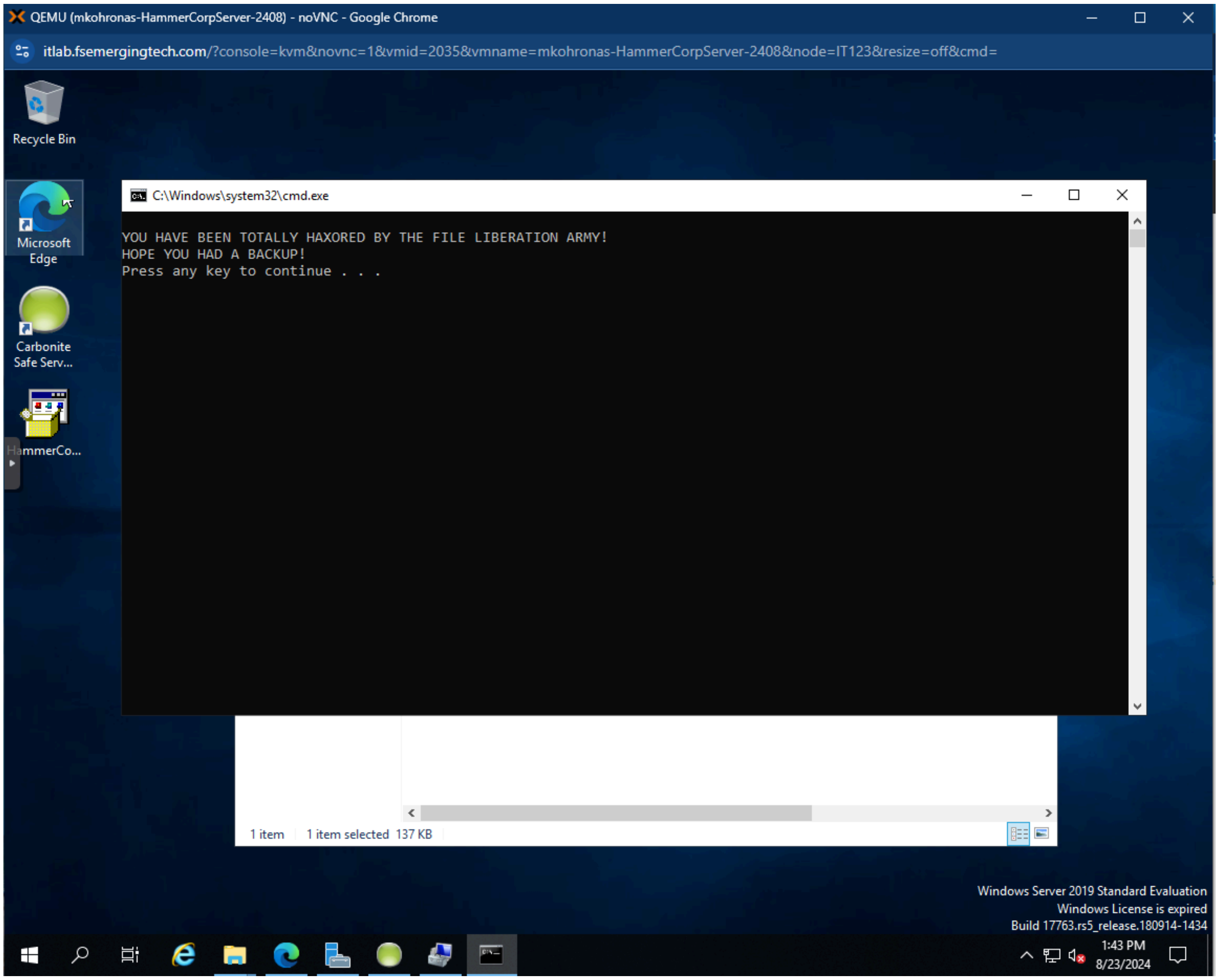
```
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: HAMMERCORP, NetBIOS user: <unknown>, NetBIOS MAC:
bc:24:11:50:3b:0e (unknown)
| Names:
|   HAMMERCORP<00>       Flags: <unique><active>
|   HAMMERS<00>          Flags: <group><active>
|_  HAMMERCORP<20>       Flags: <unique><active>
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-08-23T20:52:22
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   3.32 ms 172.16.1.115

NSE: Script Post-scanning.
Initiating NSE at 13:53
Completed NSE at 13:53, 0.00s elapsed
Initiating NSE at 13:53
Completed NSE at 13:53, 0.00s elapsed
Initiating NSE at 13:53
Completed NSE at 13:53, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 212.25 seconds
           Raw packets sent: 131214 (5.777MB) | Rcvd: 347 (15.592KB)
```

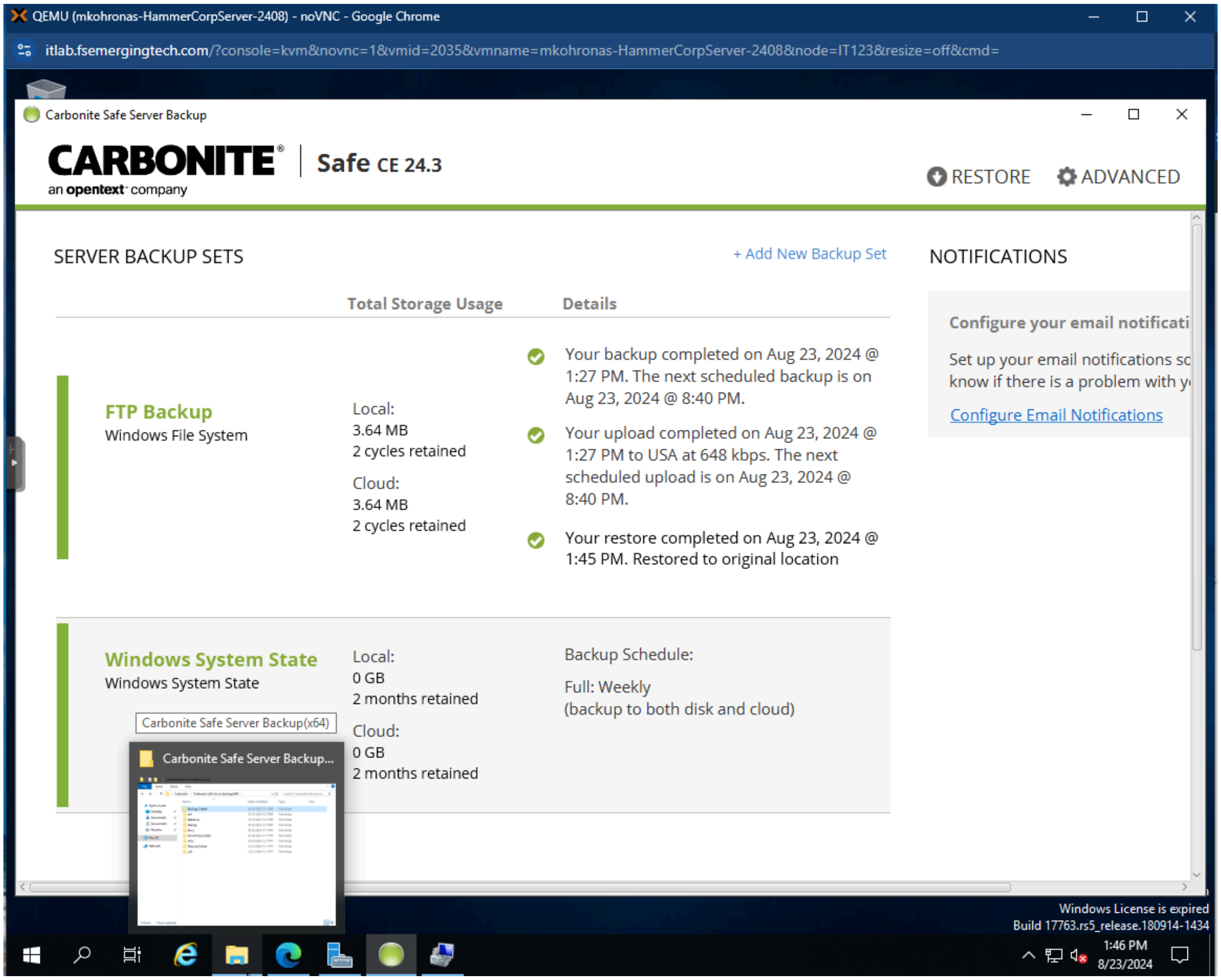
#3



QEMU (mkohronas-HammerCorpServer-2408) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=2035&vmname=mkohronas-HammerCorpServer-2408&node=IT123&resize=off&cmd=
Recycle Bin
Microsoft Edge
Carbonite Safe Serv...
HammerCo...
C:\Windows\system32\cmd.exe
1 item
1 item selected 137 KB
Windows Server 2019 Standard Evaluation
Windows License is expired
Build 17763.rs5_release.180914-1434
1:43 PM
8/23/2024

```
YOU HAVE BEEN TOTALLY HAXORED BY THE FILE LIBERATION ARMY!
HOPE YOU HAD A BACKUP!
Press any key to continue . . .
```

#4


QEMU (mkohronas-HammerCorpServer-2408) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=2035&vmname=mkohronas-HammerCorpServer-2408&node=IT123&resize=off&cmd=
Carbonite Safe Server Backup
CARBONITE
an opentext company
Safe CE 24.3
RESTORE
ADVANCED
+ Add New Backup Set
Carbonite Safe Server Backup(x64)
Carbonite Safe Server Backup...
Windows License is expired
Build 17763.rs5_release.180914-1434
1:46 PM
8/23/2024

SERVER BACKUP SETS

	Total Storage Usage	Details
FTP Backup Windows File System	Local: 3.64 MB 2 cycles retained Cloud: 3.64 MB 2 cycles retained	✓ Your backup completed on Aug 23, 2024 @ 1:27 PM. The next scheduled backup is on Aug 23, 2024 @ 8:40 PM. ✓ Your upload completed on Aug 23, 2024 @ 1:27 PM to USA at 648 kbps. The next scheduled upload is on Aug 23, 2024 @ 8:40 PM. ✓ Your restore completed on Aug 23, 2024 @ 1:45 PM. Restored to original location
Windows System State Windows System State	Local: 0 GB 2 months retained Cloud: 0 GB 2 months retained	Backup Schedule: Full: Weekly (backup to both disk and cloud)

NOTIFICATIONS

Configure your email notificati

Set up your email notifications sc know if there is a problem with y

Configure Email Notifications

1. Could you still see the files on the FTP server in your NMAP scan?

No I could not still see the files on the NMAP scan

2. What was allowing NMAP to see the FTP files?

The ability for anonymous to access the FTP files. In addition to removing “all users”

3. When you configure SSL for FTP is that SFTP or FTPS? What is the difference?

I am configuring an FTPS since SFTP is a completely different protocol. FTPS is when the command channel/data is encrypted in the FTP process. Whereas SFTP encrypts the connection that the data is being sent over overall encrypts everything. In addition to that SFTP uses SSH whereas FTPS uses TLS/SSL

4. What is the difference between explicit and implicit SSL for FTP? – Feel free to Google

Implicit SSL for FTP means that the FTP connection will always be secured with SSL. From the get go the connection is made as a secure SSL connection. Explicit SSL for FTP means that the connection could start decrypted and then request to be switched to an encrypted session

5. Why might you use IISManager accounts for FTP instead of local computer or domain accounts?

This helps separate accounts used for FTP and personal computer login. This can add an extra login step making it more secure so if someones account was breached they would need an extra set of credentials to use the FTP server. This can also help with fine-tuning and managing access control within the FTP server.

6. Name a major risk to keeping backups in the cloud.

A major risk of keeping backups in the cloud is the potential for an attacker to gain access to your backup and leaking valuable information. In addition to that if there is an issue with the cloud server you may not be able to use the backup.

7. In the Carbonite configuration for this lab what two types of backup were employed?

A cloud backup and a local backup. One on the local system and one stored in the cloud.

8. Why is it important to have two types of backup?

In case one gets corrupted or lost it is important to have redundancy which ensures availability to the backup if needed.

9. What did the file the boss sent to run on the HammerCorpServer do?

This file deleted all FTP files. Essentially losing all files and information for the business.

10. Is there anything you could do to check this file before running it? If so, what?

You can run it past virustotal to see if there is anything malicious. In addition to that noticing that the file was detected as malicious by the windows defender should have put red flags up.

#6

Lab Write Up

1. Provide a sentence or two answering the following questions:

a. What are the pros of cloud-based backups?

Having a cloud-based backup is extremely beneficial in any situation. Having a backup stored in the cloud helps ensure maximum availity of our backup. It could be stored in two different locations to ensure redundancy. If you have a backup on your local machine and get hit with ransomware or anything which wipes your files it could also affect your backup.

b. What are the cons of cloud-based backups?

By having the backup stored in the cloud it could cause some security issues. If the backup is not secured it could cause leakage of data as your backup may include sensitive information. In addition to that if there is an outage or major error on the cloud provider's side it could cause corruption or loss of your backup.

c. What are the pros of local backups?

Having a local backup is great. With a local backup you don't have to download the files back from the cloud rather you already have everything saved which could be transferred over quickly and easily. In addition to that it would save money to have it stored locally as you don't have to pay for the storage space from the cloud provider.

d. What are the cons of local backups?

Having a local backup could be a cause of a serious cybersecurity attack. If the backup isn't stored properly it could result in free access to all of the company's data. In addition to that if an attacker installs ransomware on the machine with the backup on it. It could cause the loss of the system files and the backup files both.