The Cyber Kill Chain

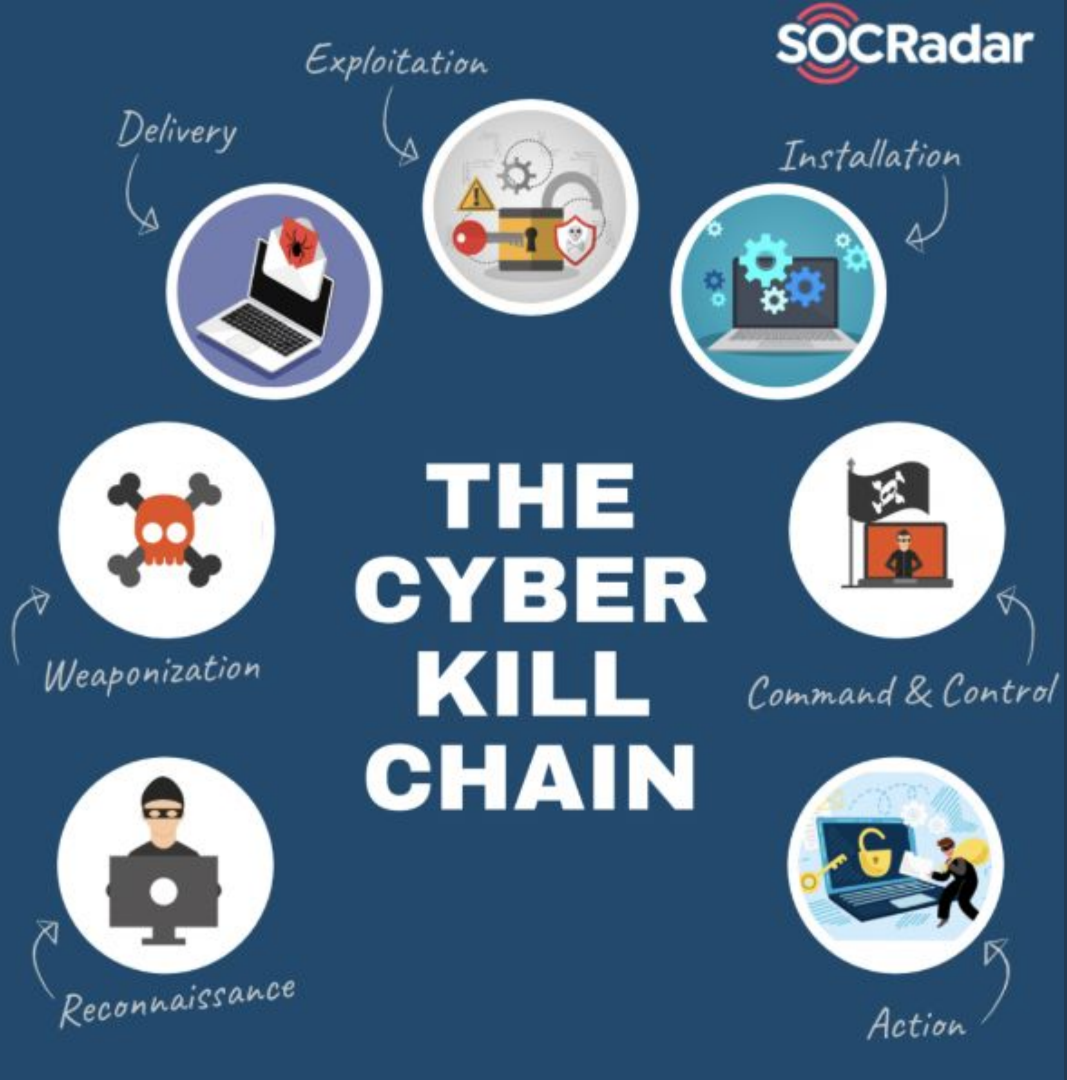
CSA Cyber Kickstart
Defend and hack!!

8 PHASES OF THE
CYBER KILL CHAIN

1. Reconnaissance
2. Intrusion
3. Exploitation
4. Privilege Escalation
5. Lateral Movement
6. Obfuscation / Anti-forensics
7. Denial of Service
8. Exfiltration

SOCRadar

THE CYBER KILL CHAIN



Reconnaissance

Weaponization

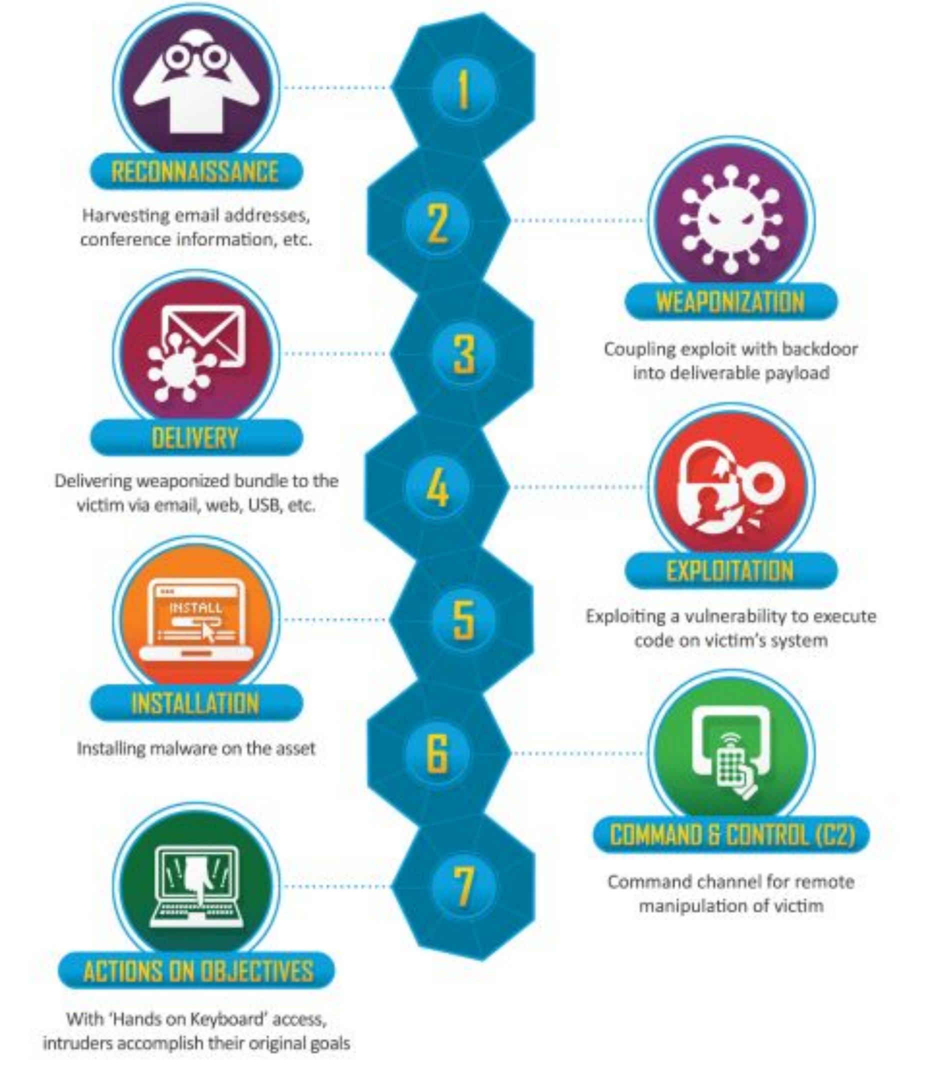
Delivery

Exploitation

Installation

Command & Control

Action



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

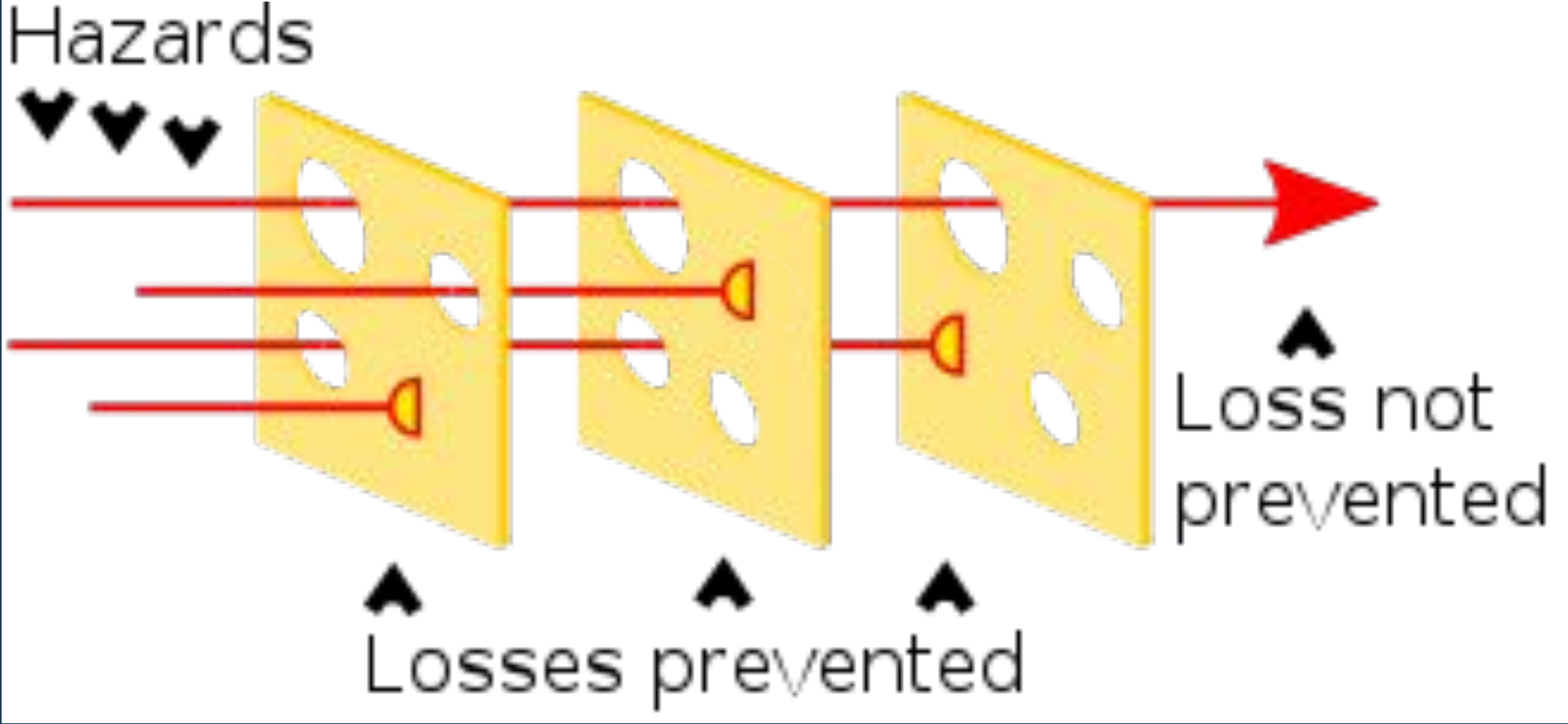
With 'Hands on Keyboard' access, intruders accomplish their original goals

8 PHASES OF THE

CYBER KILL CHAIN

1. Reconnaissance
2. Intrusion
3. Exploitation
4. Privilege Escalation
5. Lateral Movement
6. Obfuscation / Anti-forensics
7. Denial of Service
8. Exfiltration

Defense in Depth



Indicators of Compromise

“Pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network.”

Like residue from an attack.

IP addresses

Emails

Log details

etc.

Malware

Scripts/codes

Hashes

C2 Domain Names

cisa.gov/uscert/ncas/alerts/aa22-249a

1 Reconnaissance

WHY???

Passive (OSINT):

- Harvesting email address
- IP address ranges
- Domain names
- Company style guides/logos
- Employee names
- Server types (Shodan.io)

Active:

- Port scanning
- Website enumeration
- Physical reconnaissance
- Fingerprinting operating systems
- Fingerprint software

1 Reconnaissance

Practice

2 Intrusion & Weaponization

Based on the recon!

- Choose your attack vector.....
  - Phishing email
  - USB drive
  - Smishing
  - Vishing
  - Drive-by-compromise
  - Supply Chain Compromise
  - Physical access

3 Exploitation & Delivery

- What is being "exploited" here....
  - A person?
  - A website?
  - A device (server/asset?)
  - A supplier?

The weapon has been specifically designed for this exploit!

Subtle difference between exploitation and delivery? (According to me, Anna)

nvd.nist.gov/vuln/detail/CVE-2017-0148

hacker voice

“WE’RE IN.”

4 Privilege Escalation

Privilege escalation often requires either:

A.) Another exploit

B.) Pivoting to another account/device

You need *admin* credentials (almost always) to deploy malware or overtake system processes.

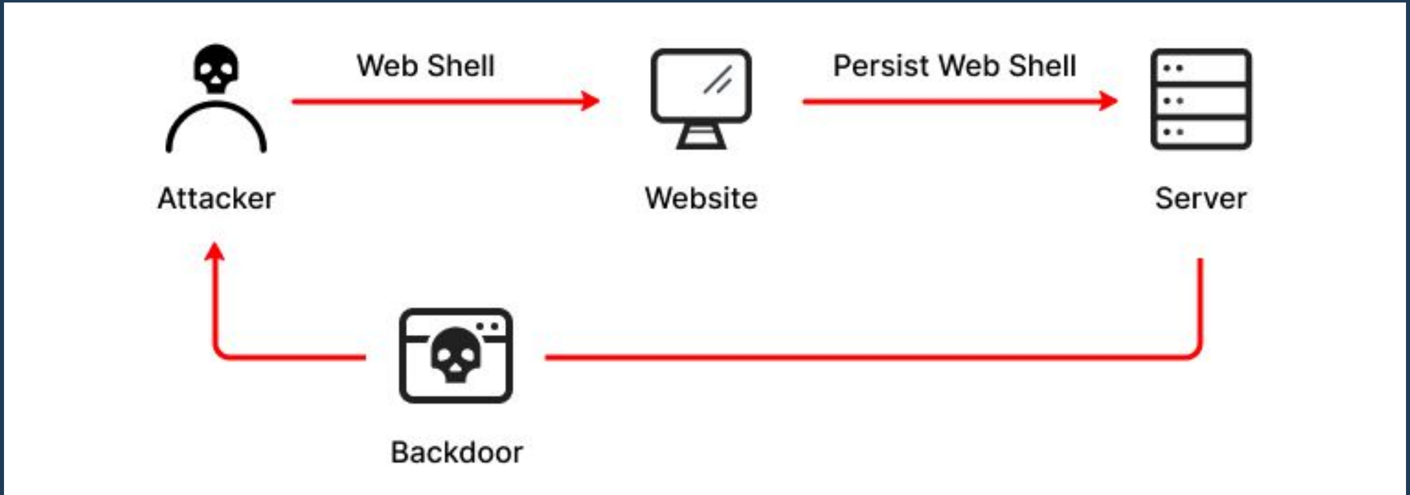
makeuseof.com/what-is-the-cve-2021-4034-polkit-privilege-escalation-vulnerability/

****

Persistence

Once you GET IN.. you need a way to get BACK in.

- WebShell
- New User Account
- Another vulnerability
- Backdoor
- Rootkit



**** Persistence

What was the persistence mechanism?

bash_history_persistence.txt

5 Lateral Movement

Move to another device/asset

Could be looking for something specific!

- Domain Controller
- Specific User host
- Sensitive Information
- File Share

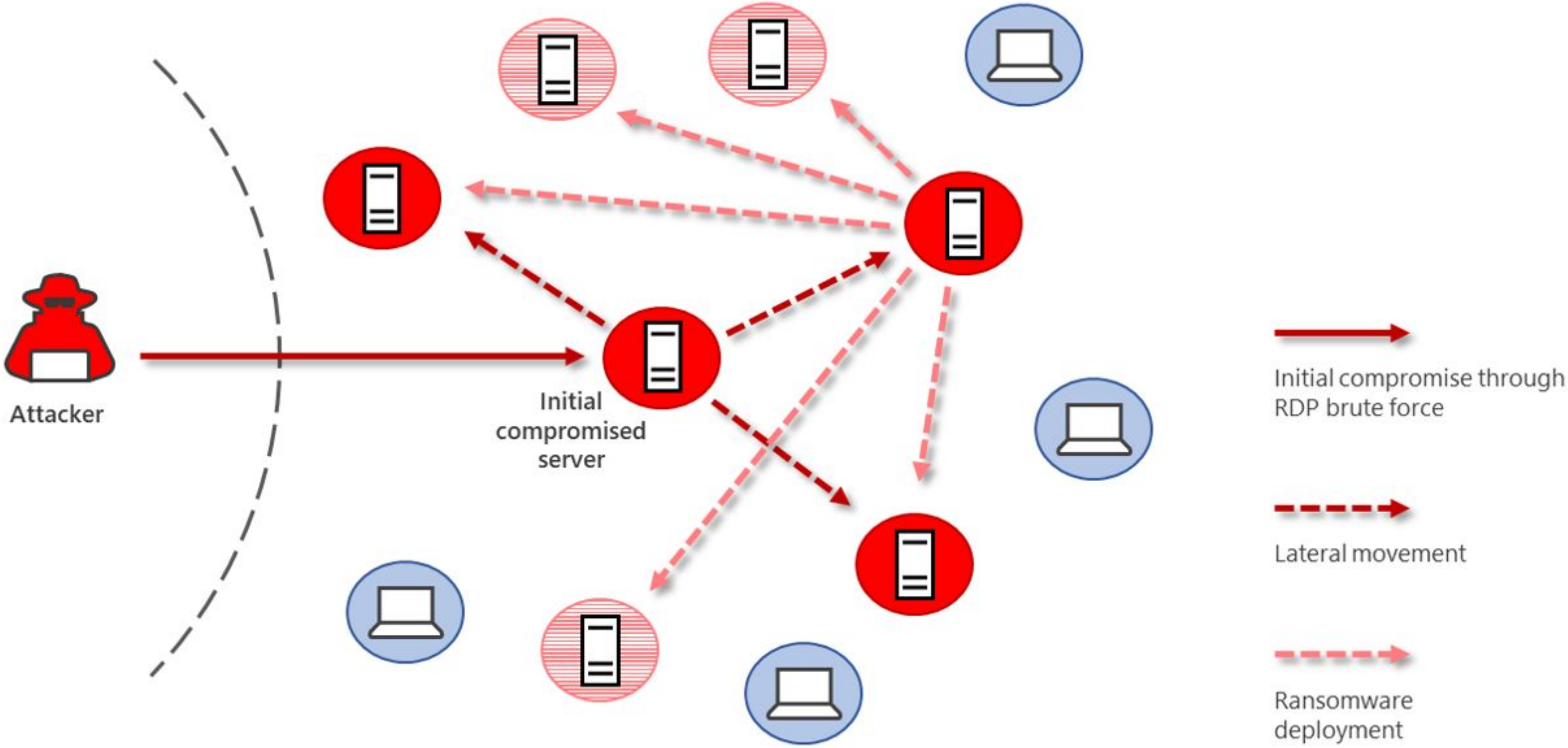
Repeat the cycle from the compromised host:

- Recon (scan other hosts)
- Weaponization (develop new exploit)
- Exploit (deliver malicious payload)
- Access new device

5 Lateral Movement

What were the hosts reaching out to each other? What was the action?

capture_recon.txt



Attacker

Initial compromised server

Initial compromise through RDP brute force

Lateral movement

Ransomware deployment

6 Obfuscation / Anti-forensics

Hide the IOCs!!!!

- Attack from VPN
- Delete exploitation tools
- Modify timestamps
- Delete logs
- Delete exfiltrated data
- Encrypt data

7 Denial of Service

- DoS attack
- Locked out authorized users
- RansomWare
- Wiper Malware (see: Russian and Ukraine!)

thehackernews.com/2022/12/russian-courts-targeted-by-new-crywiper.html

6 Obfuscation / Anti-forensics

What were the obfuscation techniques?

bash_history_obfuscation.txt

8 Exfiltration

The bad actors stole your data 😔

- Email
- Cloud upload (Box, Google Drive, etc.)
- Physical drives
- Web requests
- SMB shares
- Dumpster Diving

Data theft is usually held against the company for money (ransom/extortion).

Will likely be sold on the DarkWeb for profit.