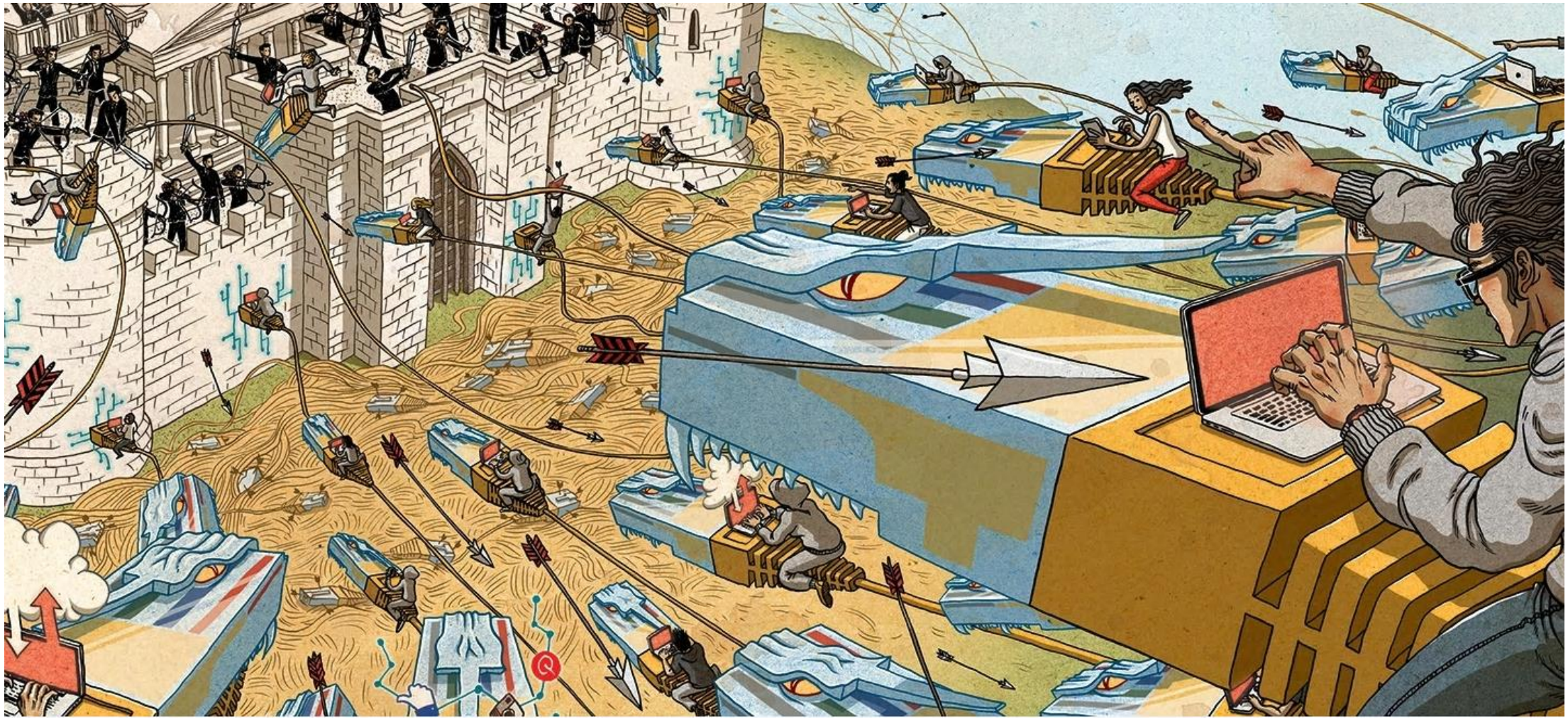


# Linux and Windows post exploitation

# Post exploitation?

- Maintaining Access
- Situational awareness
- Privilege Escalation
- Data Harvesting and Exfiltration
- Lateral movement

- Data exfiltration (J.P. Morgan, Anthem)
- Fraud (payments, SWIFT, clearing)
- Service tampering or manipulation (SEC)
- Denial of service (Sony Entertainment)

# Post exploitation?


## PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection
Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

## Enterprise ATT&CK

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control

# Prerequisites

- Motivation vs Risk
- Target related business and technical knowledge
- Experience in attacking monitored environments
- Hiding / wiping tracks

# Privilege escalation & Maintaining persistence

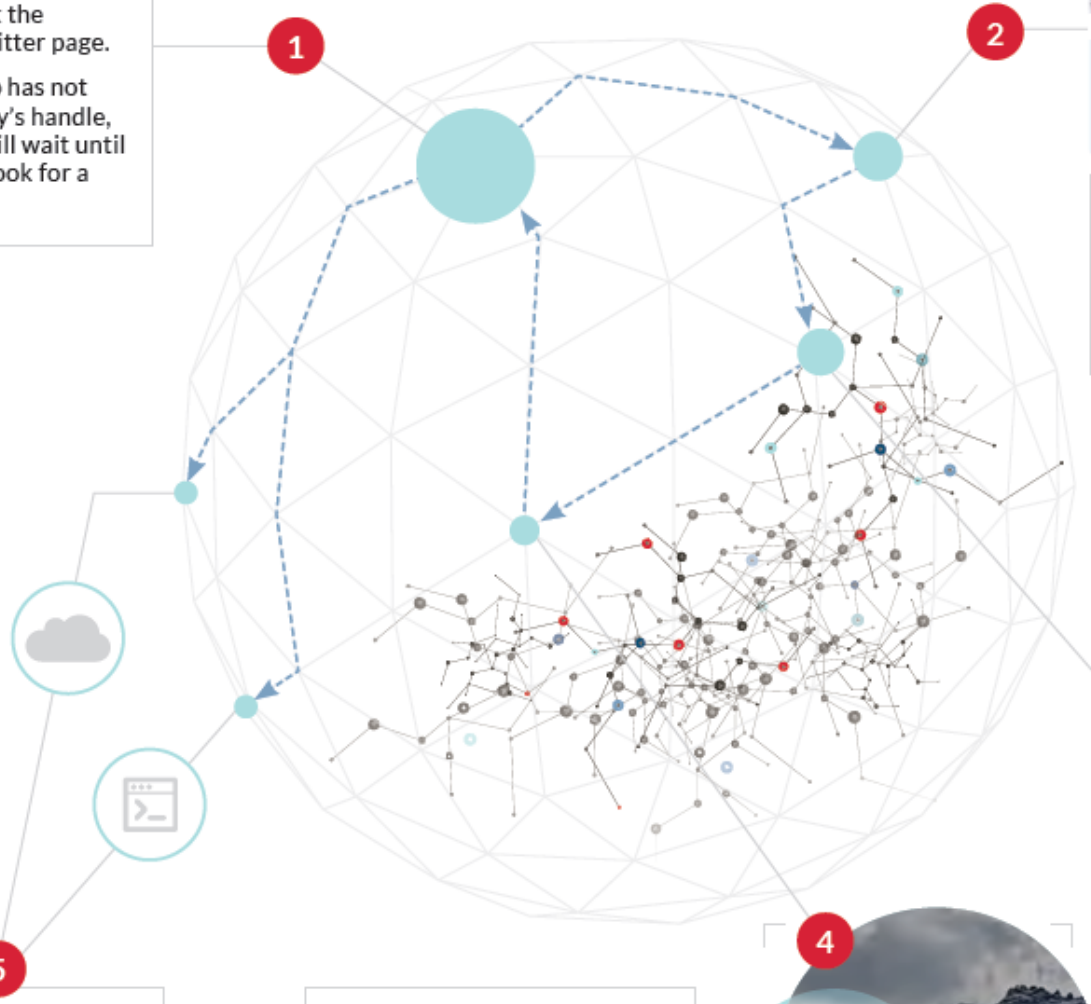
- On the host / device:
  - Modification or exploitation of services, processes, applications running or could be started with desired privileges
  - RAM, vaults, Text files (configs, logs etc) containing credentials
  - Handy IT tools left over could be reused to narrow down the search (or query databases)

- Maintaining persistence
  - C&C, backdoors (changing firmware, binaries, libs, configs, authorized SSH keys, browser extensions)

**1.** The HAMMERTOSS backdoor generates and looks for a different Twitter handle each day. It uses an algorithm to generate the daily handle, such as "234Bob234", before attempting to visit the corresponding Twitter page.

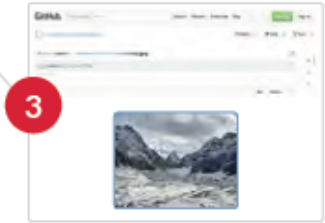
If the threat group has not registered that day's handle, HAMMERTOSS will wait until the next day and look for a different handle.







**2.** HAMMERTOSS visits the associated Twitter account and looks for a tweet with a URL and a hashtag that indicates the location and minimum size of an image file.



**3.** HAMMERTOSS visits the URL and obtains an image.

**4.** The image looks normal, but actually contains hidden and encrypted data using steganography.

HAMMERTOSS decrypts the hidden data to obtain commands.

**5.** HAMMERTOSS processes the decrypted commands, which may instruct the malware to conduct reconnaissance, execute commands via PowerShell, or upload data to a cloud storage service.

**Note:** The images are stock photography and were not used by the group.

# Privilege escalation

- Passwords attacks
  - Offline hashes cracking (JTR, Hashcat)
  - Online password guessing (Hydra, Medusa & more). Password spraying.
  - Pass the hash
- Internal discovery
  - Passive recon – files, arp tables, reuse of creds, SSH keys or Kerberos keytabs
  - Active – examine websites, scan for important ports (445, 22, 25, 110, 3389 etc. known for services you need)
  - Attacking domain resources

# Linux

- Examples of privilege escalation techniques:
  - Sudo privileges
  - Suid binaries
  - NFS share
  - Kernel or software exploit

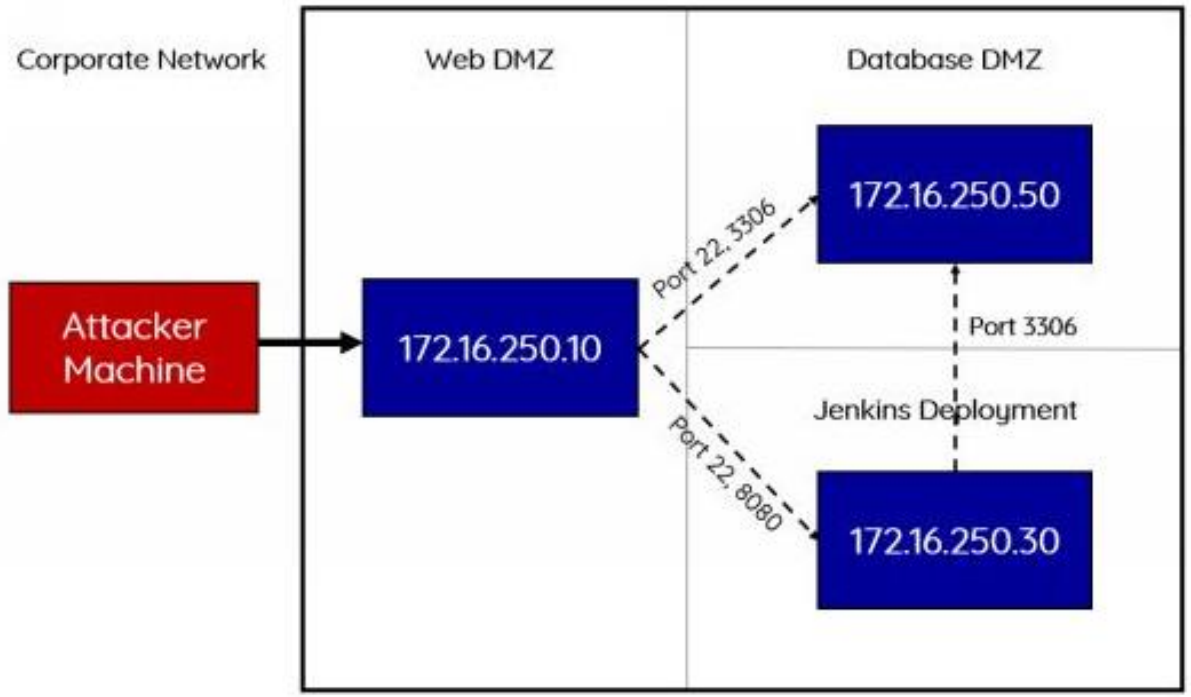
# Linux

- Hunting for credentials
  - SSH keys
  - Passwords /connection strings in config files / logs
  - Kerberos tickets

- Data harvesting
  - Business data in files
  - Local DBs
  - Useful binaries

# Demo

- THP3 charged Kali Linux
- Metasploit
- Dnscat2
- sshuttle



# Windows

- Examples of privilege escalation techniques:
  - Unquoted paths or incorrect permissions in services
  - Modifiable exe or dll being run under privileged account
  - Kernel or software exploit
  - Social engineering
  - Answer files

# Demo

- Metasploit
- Responder
- Mimikatz
- Crackmapexec
- PowerShell Empire
- BloodHound