Threats and Countermeasures

Lecture 10:
Credential Access / Discovery

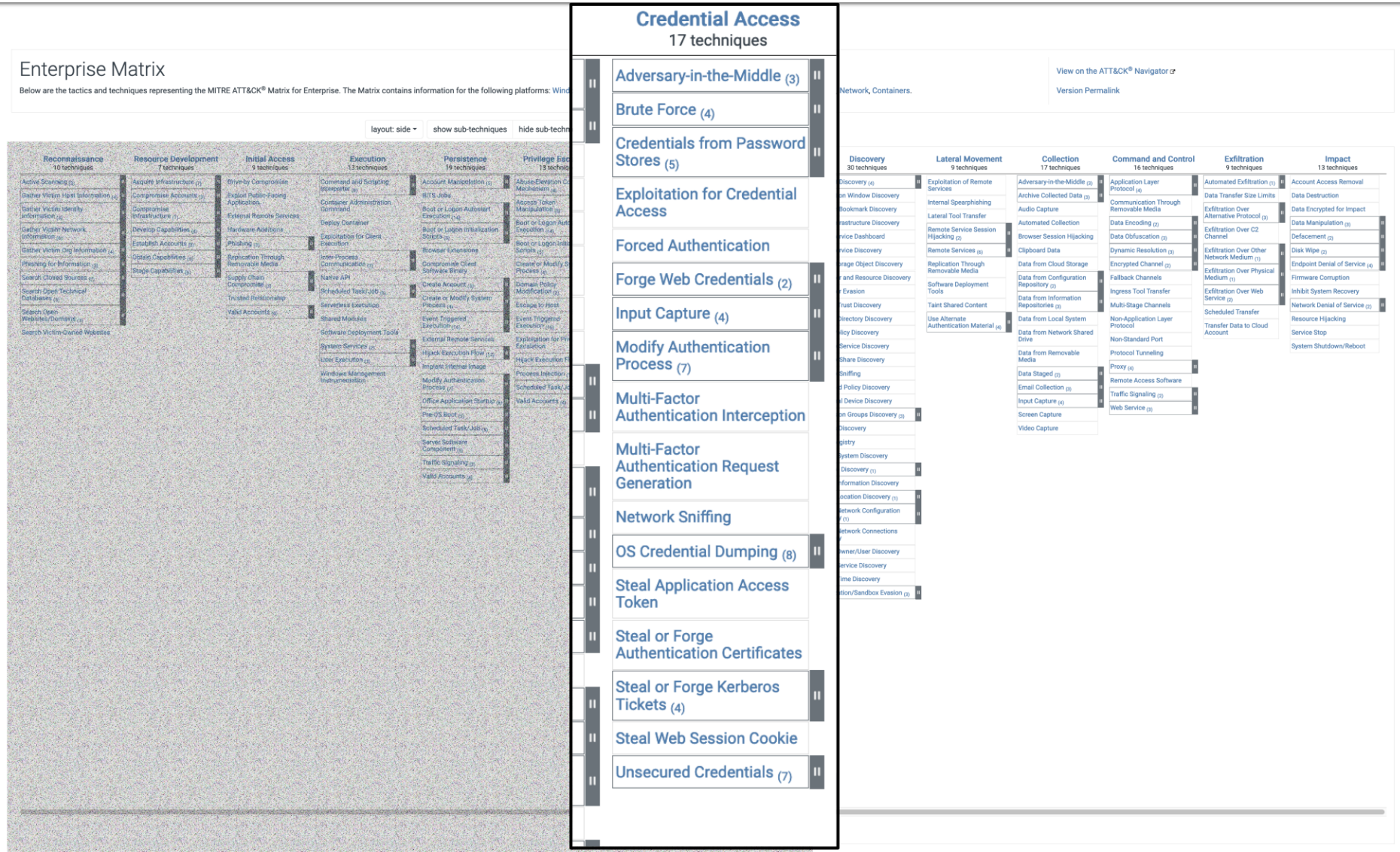
COMP-5830/-6830
Spring 2025

Threats and Countermeasures

Lecture 10:
Credential Access

COMP-5830/-6830
Spring 2025

MITRE ATT&CK


Enterprise Matrix
Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms:
View on the ATT&CK® Navigator
Version Permalink
layout: side
show sub-techniques
Reconnaissance
10 techniques
Resource Development
7 techniques
Initial Access
9 techniques
Execution
13 techniques
Persistence
19 techniques
Discovery
30 techniques
Lateral Movement
9 techniques
Collection
17 techniques
Command and Control
16 techniques
Exfiltration
9 techniques
Impact
13 techniques
Credential Access
17 techniques
Adversary-in-the-Middle (3)
Brute Force (4)
Credentials from Password Stores (5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Modify Authentication Process (7)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Unsecured Credentials (7)

Credential Access (MITRE)

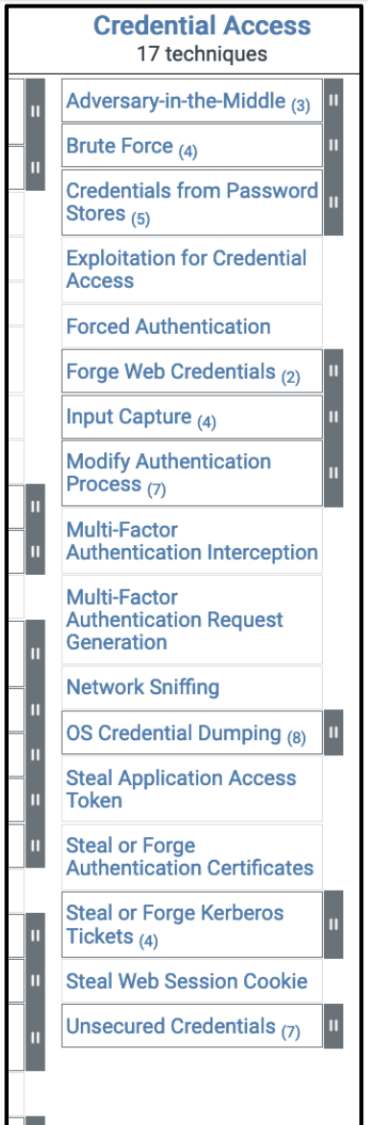
- Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

Credential Access
17 techniques

- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (7)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Unsecured Credentials (7)

Credential Access (simplified)

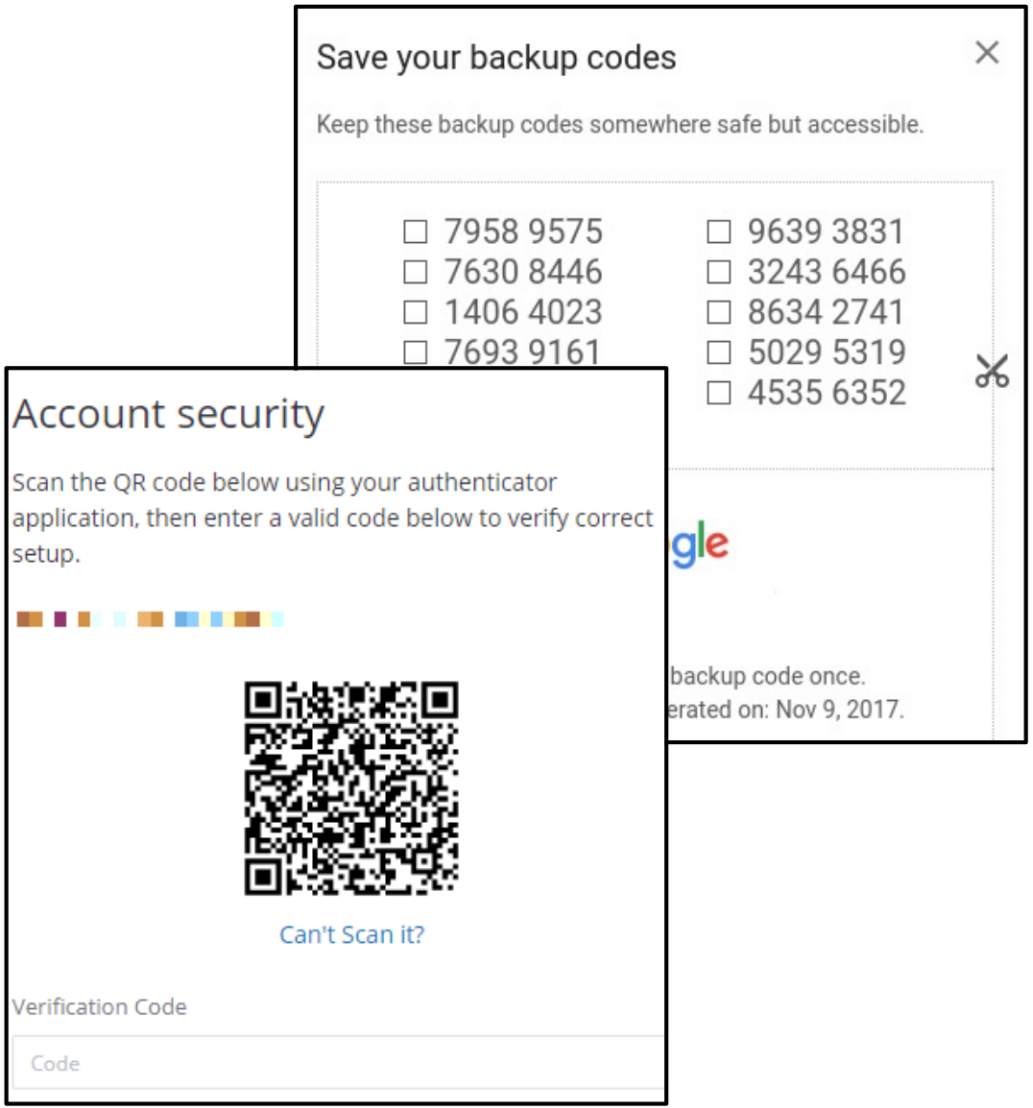
- **GOAL**: Obtain additional valid credentials
  - Usernames, passwords, MFA codes, etc
- Sample mechanisms:
  - Keylogger (HW or SW)
  - OS-store dump
  - Token manipulation
  - MitM



Types of Credentials

User-Related

- OS logon
- Web Service/API
- MFA codes
- Reset-Mechanisms



Types of Credentials

User-Related

- OS logon
- Web Service/API
- MFA codes
- Reset-Mechanisms

Device/Infra-Related

- Trusted Platform Module (TPM) access
- Device Creds
- Network Access Creds
  - 801.1X, MAC filters, etc.

Input/Output Capture

- Humans often type their credentials (logon, web apps, password manager, etc.)
- Obtain via:
  - Keyloggers
  - GUI Input Capture
  - Web Portal Capture
  - Cred API Hooking

MitM Attacks

- Many communication protocols lack secure channels or authentication
  - ARP, DNS, DHCP, etc.
- Can be abused to force a device to communicate through an attacker-controlled system to collect information and perform malicious activities
- Examples of MITM attacks include:
  - Server Message Block (SMB) Relay
  - Address Resolution Protocols (ARP) Cache Poisoning
  - DHCP Server Spoofing

ARP Protocol

The **Address Resolution Protocol (ARP)** allows hosts to map IP ←→ MAC addresses.

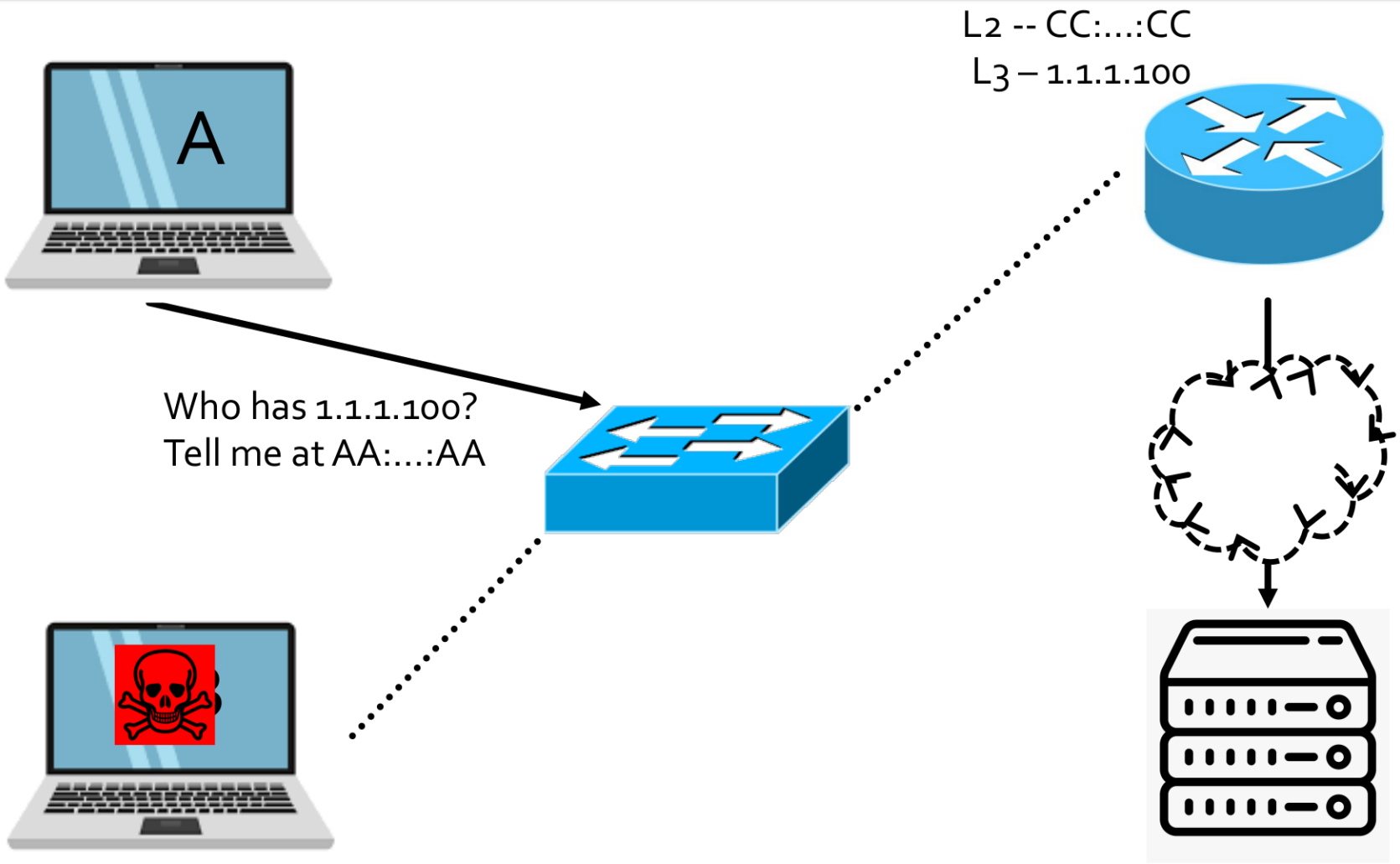
- ARP Announcements
  - “I have IP 1.1.1.1 and my MAC is XX:X…X:XX”
- ARP Probe
  - “What MAC is associated with 1.1.1.1?”
- L2 Default gateway
  - The host to send to if not on local network

ARP Poisoning/Spoofing

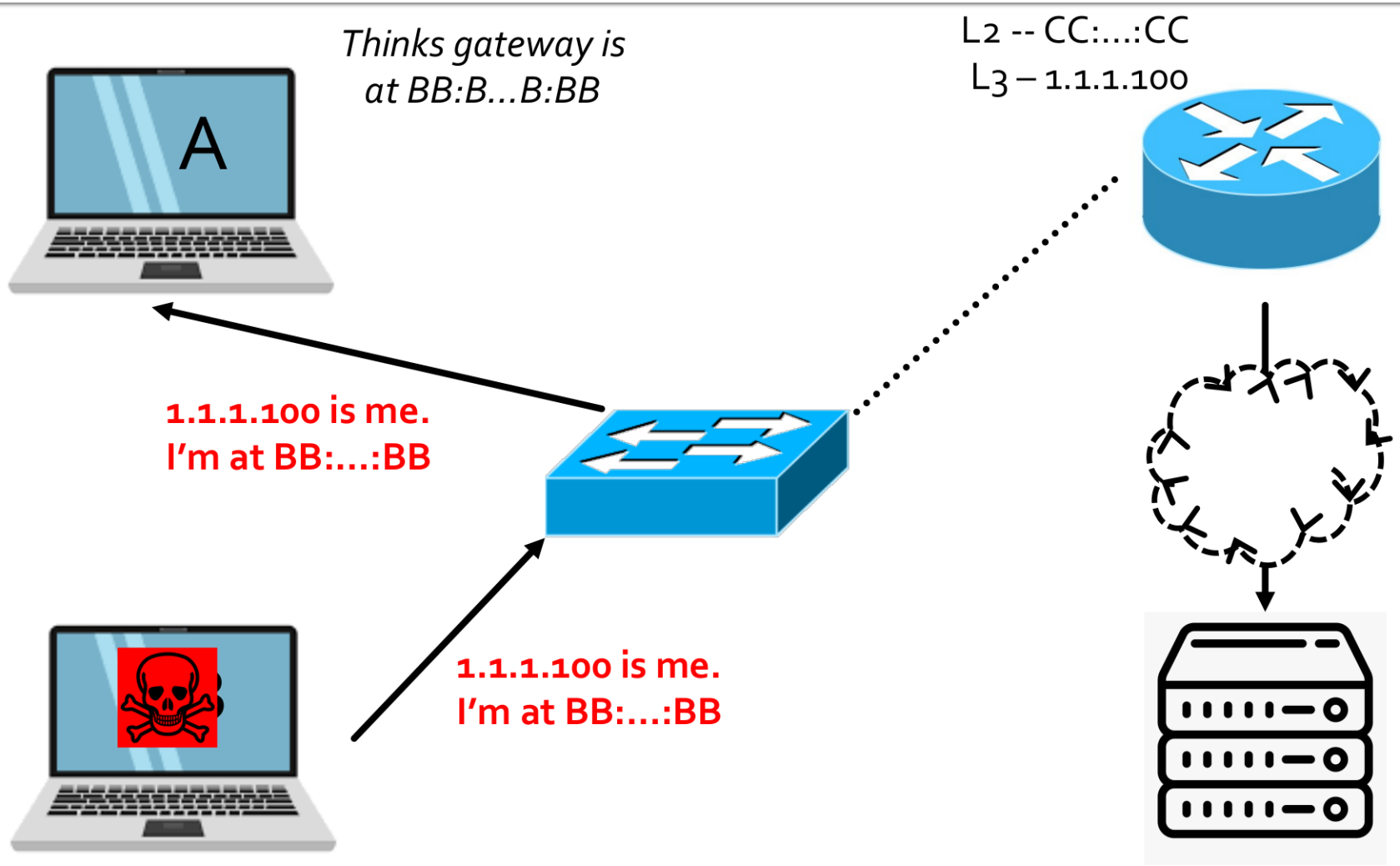
ARP Poisoning/Spoofing Attacks are a set of techniques used to misdirect traffic on the network.

- Malicious actor on local network
- Can be used to:
  - DoS another client
  - Cause network thrashing
  - Intercept traffic

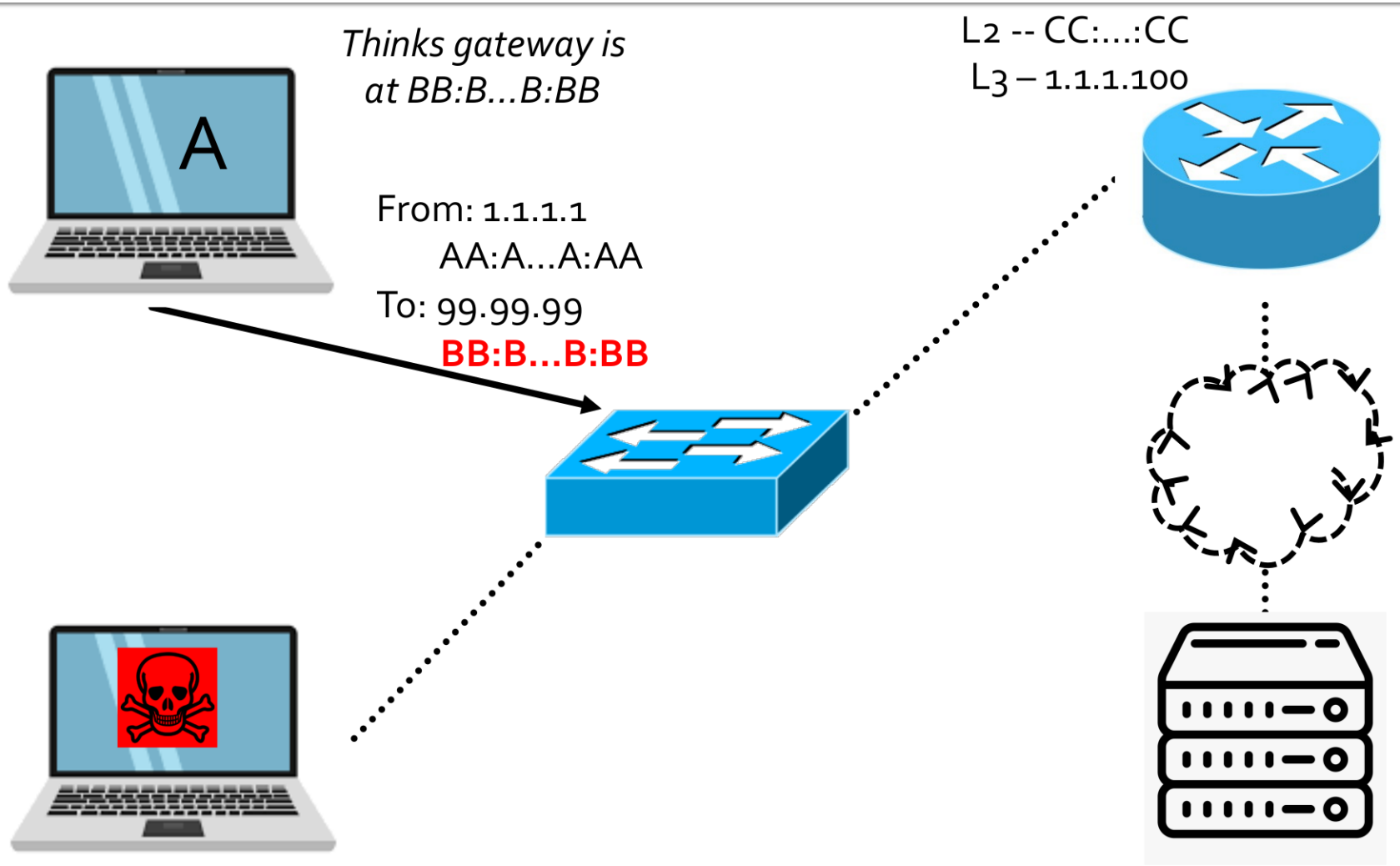
ARP Poisoning/Spoofing



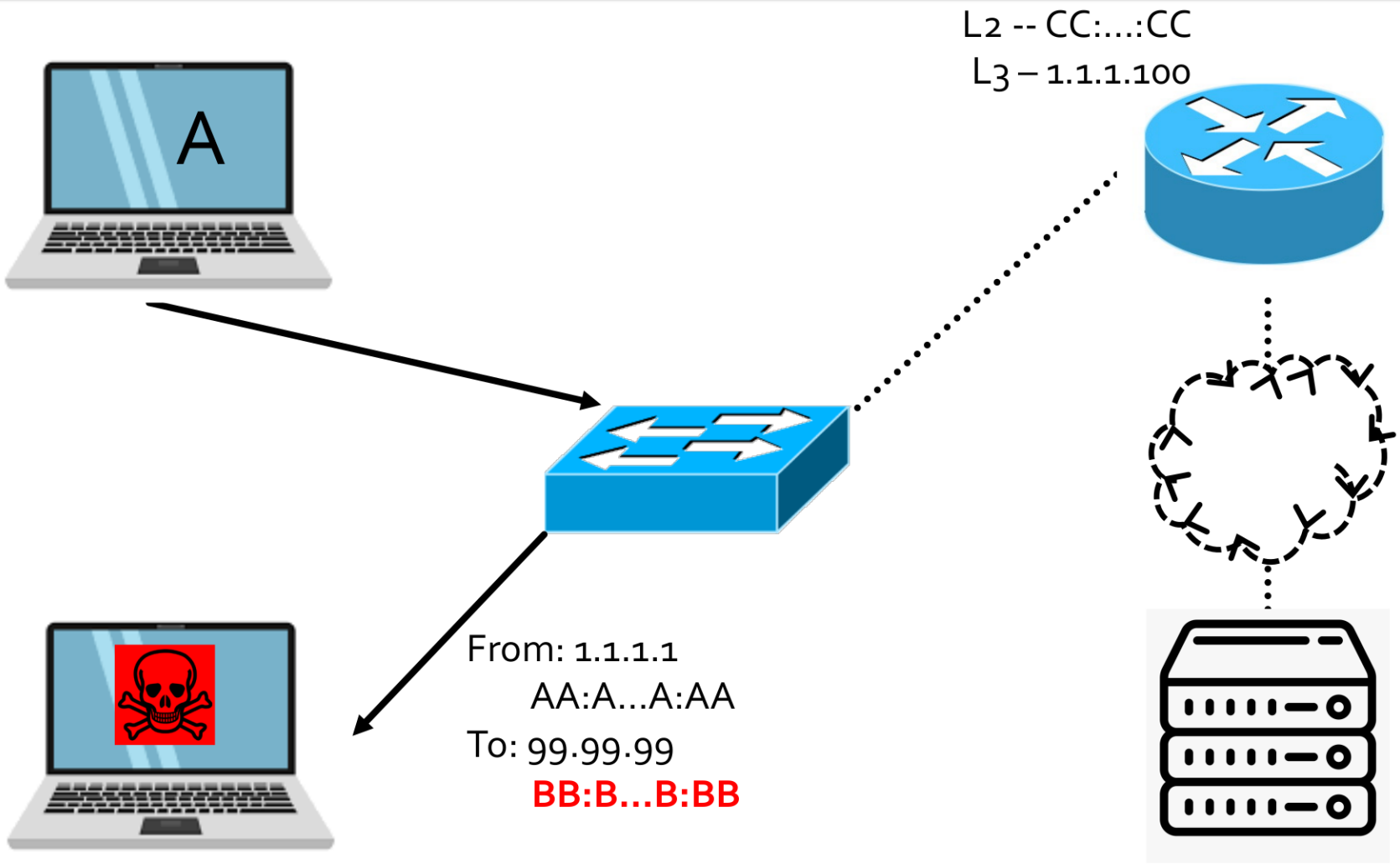
ARP Poisoning/Spoofing



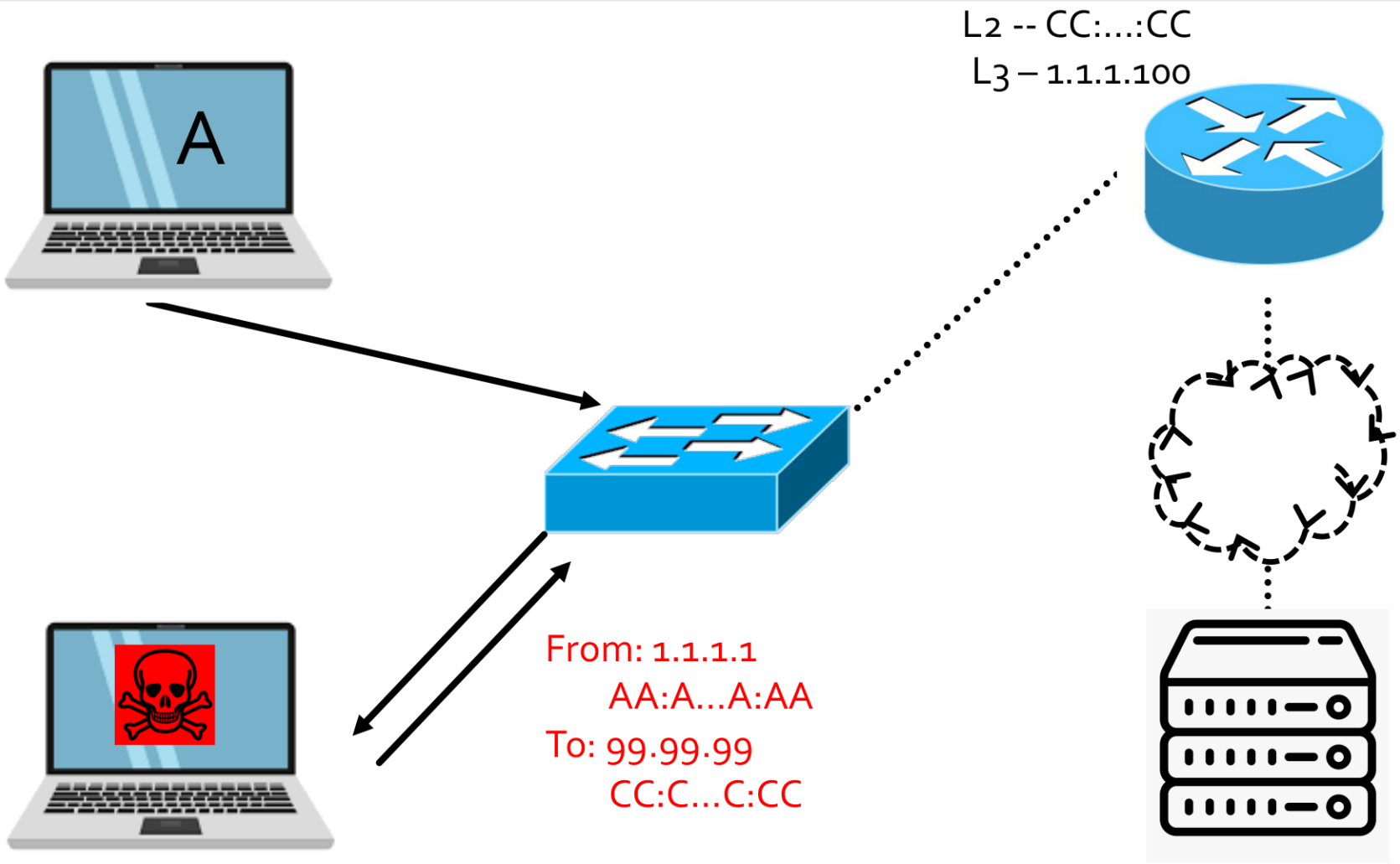
ARP Poisoning/Spoofing



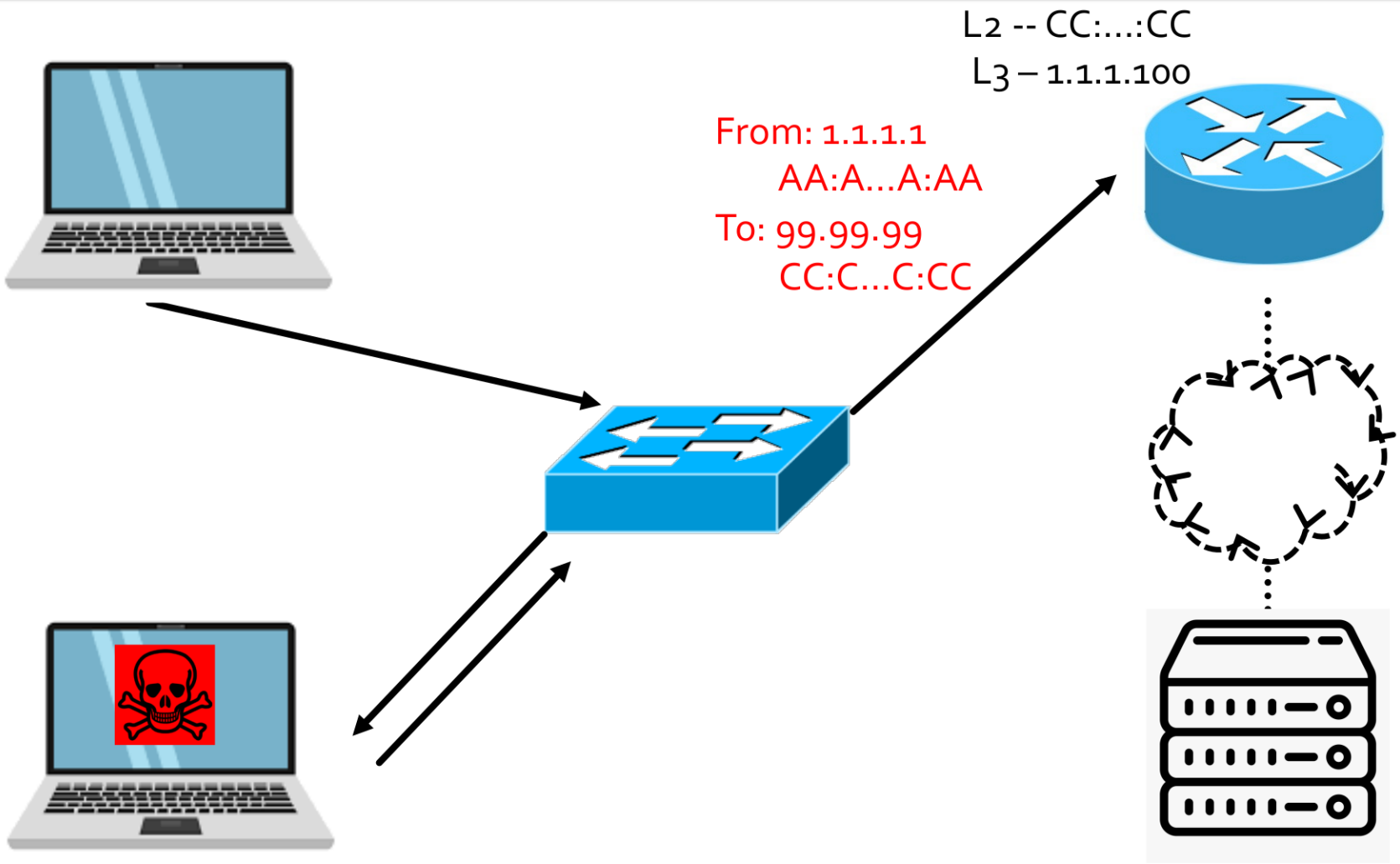
ARP Poisoning/Spoofing



ARP Poisoning/Spoofing

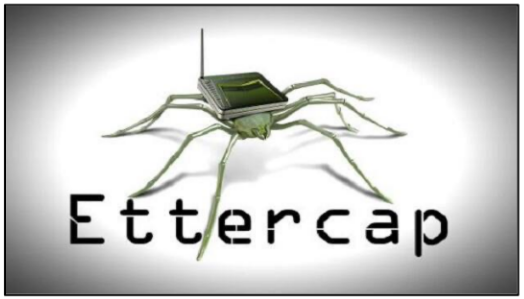


ARP Poisoning/Spoofing



Useful Tools

- Ettercap
  - Older, Ethernet-focused



- Bettercap
  - Newer, WiFi-focused

- Yersinia
  - Generic L2-interaction framework (more/different protocols)

Brute-Force Password Attacks

- Required: Input Corpus + Validation Oracle

Brute-Force Password Attacks

- Required: Input Corpus + Validation Oracle

Online

- Password Guessing
- Credential Stuffing
- Password Spray
- …

Brute-Force Password Attacks

- Required: Input Corpus + Validation Oracle

Online

- Password Guessing
- Credential Stuffing
- Password Spray
- …

Offline

- Password/Hash "cracking"

Dumping OS Stores

- Different OSes store in different locations and/or multiple locations
  - In "*files*" stored on-disk
  - In-memory
  - OS's internal "keychain"
  - Securityd Memory

Dumping OS Stores

- Linux (`/etc/passwd` + `/etc/shadow`)
- Windows (Security Acct Manager (SAM))
- Tools
  - Mimikatz
  - pwdump
  - volatility
  - etc.

Threats and Countermeasures

Lecture 10: Discovery

COMP-5830/-6830
Spring 2025

MITRE ATT&CK

Discovery
30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery

MITRE ATT&CK

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

layout: side | show sub-techniques | hide sub-techniques | help

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques

MITRE ATT&CK

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

layout: side | show sub-techniques | hide sub-techniques | help

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques

Discovery

- Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

Discovery
30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery

Discovery (simplified)

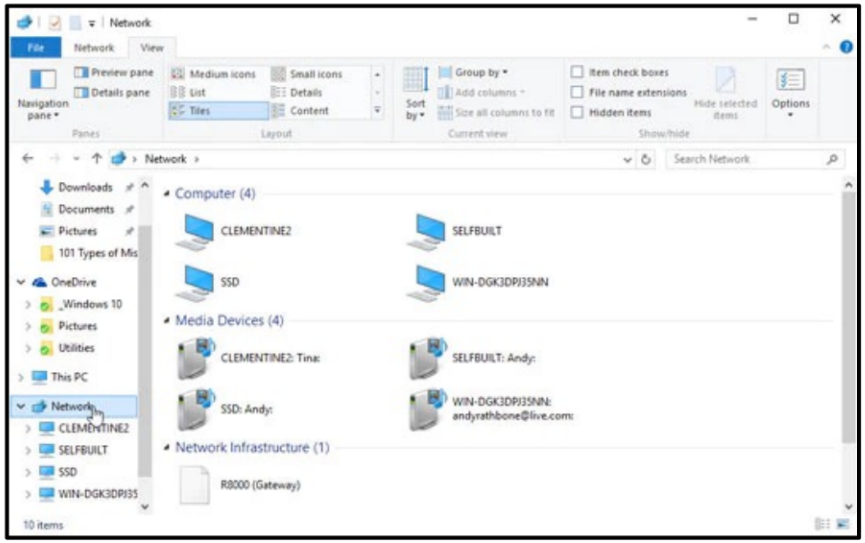
- Gain knowledge of systems/networks useful in orientating the attacker
- Explore current control/capabilities to plan follow-on actions
- Built-in OS tools are often leveraged and sufficient

Discovery
30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery

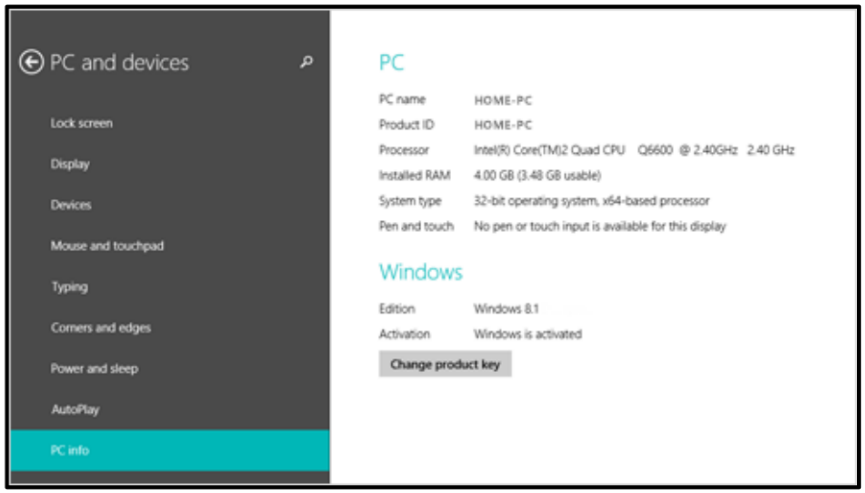
Windows OS Exploration

- Enumerate Disks

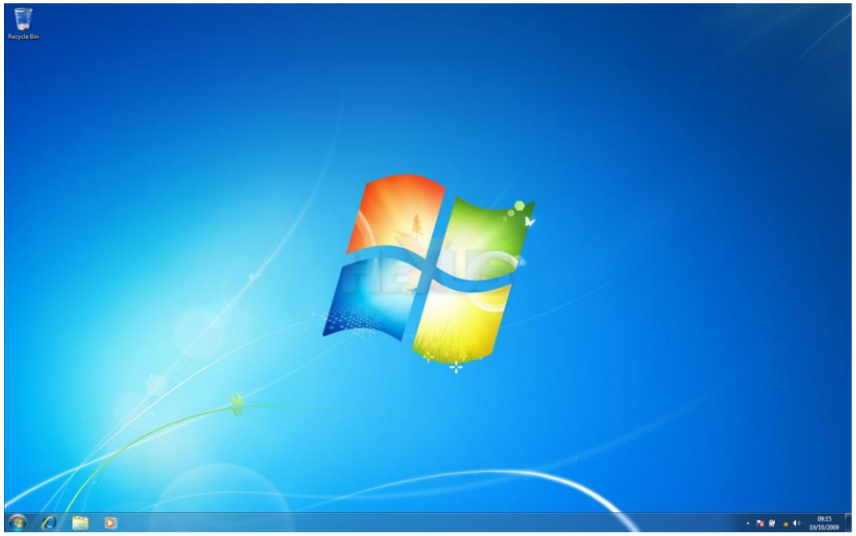


Windows OS Exploration

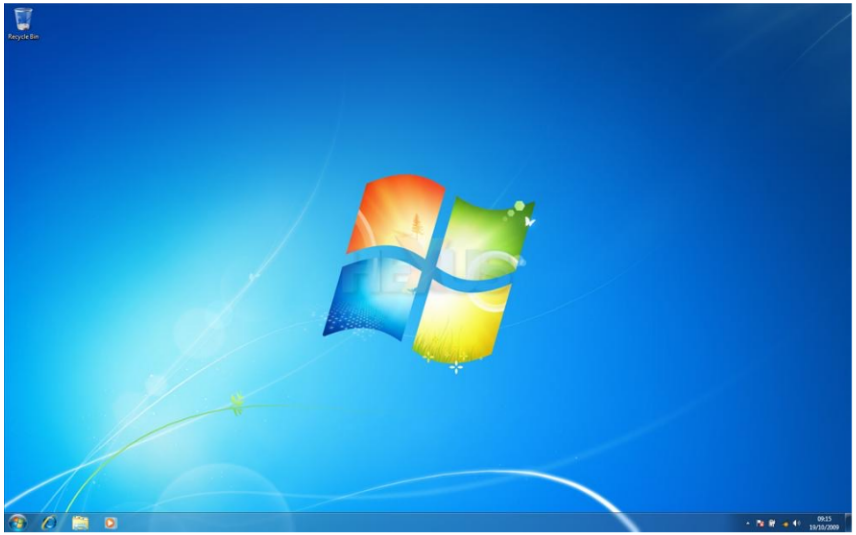
- Enumerate Disks
- Version info



Windows 7



Windows 7



Windows 8

Microsoft

Community

MA MartinGoens Created on December 4, 2012

how to make windows 8 look and act like windows 7

Recently bought a new laptop, from HP and I am so confussed with the new windows 8, I can't even use the darn thing, reminds me of the time I was stuck with an Apple Machine. Is there a way to change the screen and start up to look and behave like Windows 7?
Other wise, I'm giving this piece of junk a good toss out the window. And I don't mean Windows 8.
Thank you for any help you all can be, I just wanted a new computer not an operating system like this..

CNET

Tech Money Home Wellness Home Internet Energy Deals Sleep

Tech > Services & Software

How to make Windows 8 look like Windows 7

We reveal how to water down or ignore some of Windows 8's more controversial features and restore functionality you thought had vanished.

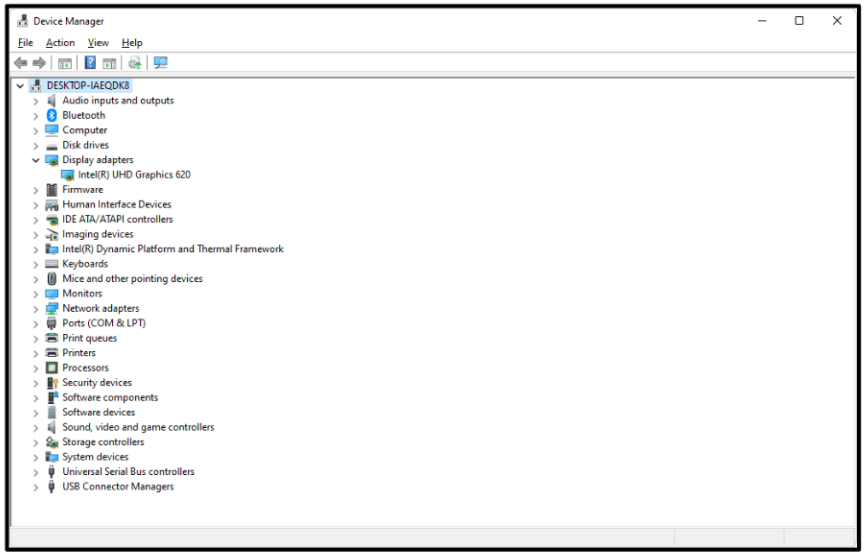
Nick Peers

Oct. 27, 2012 1:00 a.m. PT

5 min read

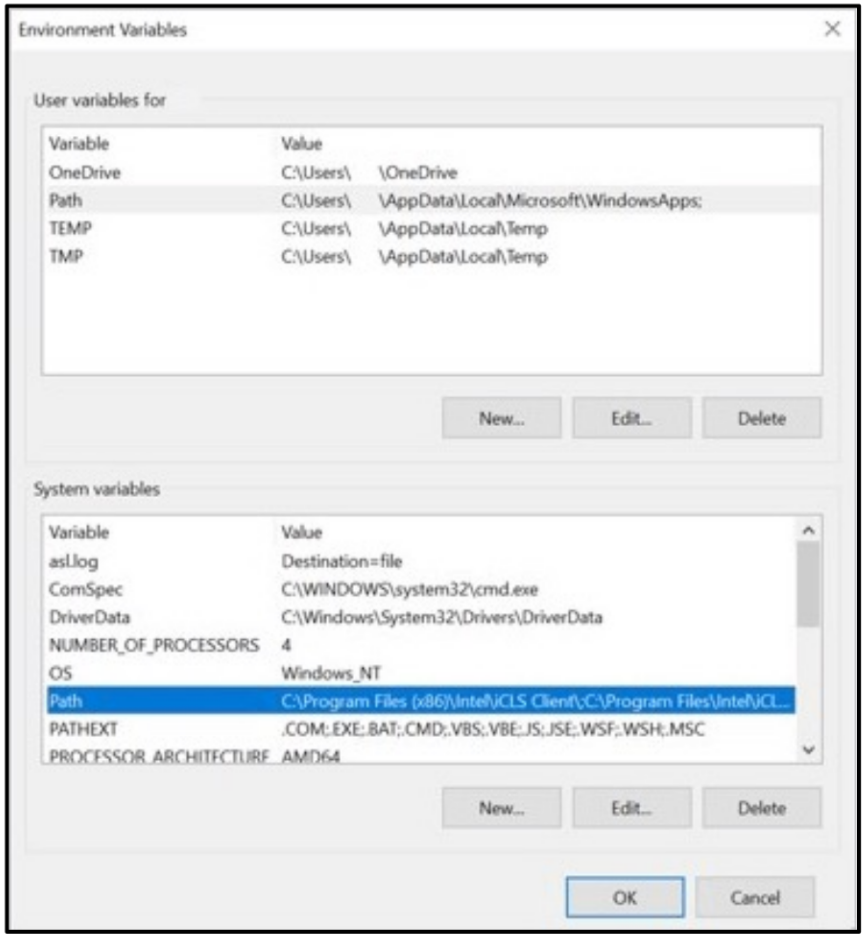
Windows OS Exploration

- Enumerate Disks
- Version info
- Device Manager



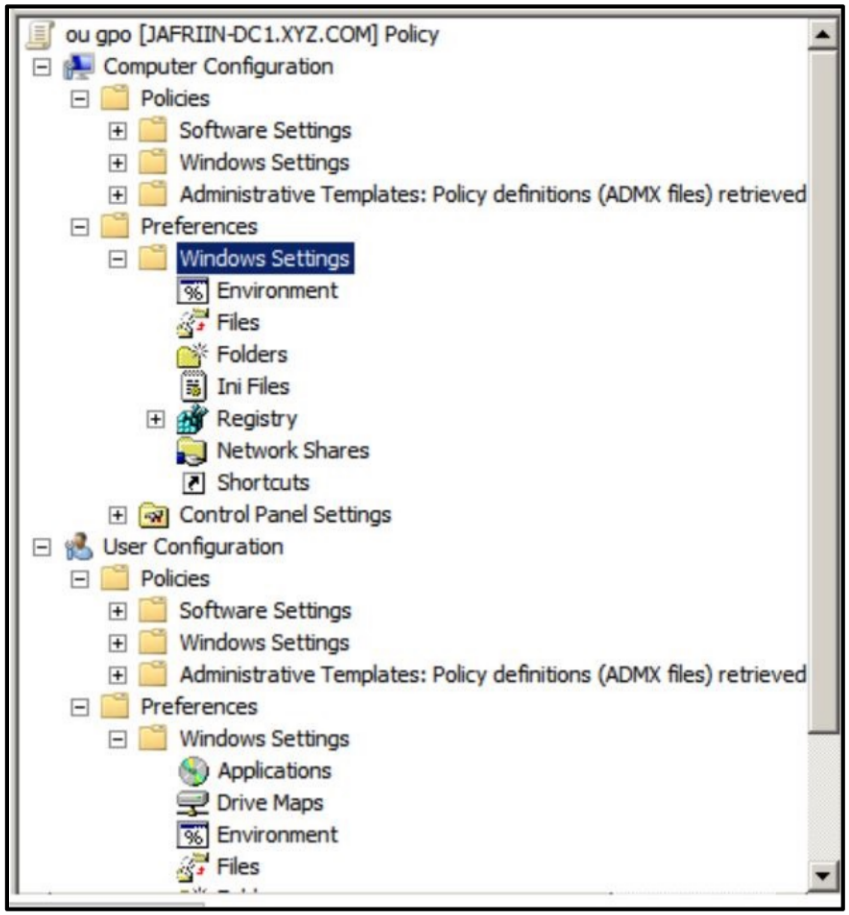
Windows OS Exploration

- Enumerate Disks
- Version info
- Device Manager
- Environment



Windows OS Exploration

- Enumerate Disks
- Version info
- Device Manager
- Environment
- Local/Group Policy



Linux OS Exploration

Linux OS Exploration

- Kernel version, architecture, etc
- `uname -a`

Linux OS Exploration

- Kernel version, architecture, etc
- Info about CPU
- Info about RAM
- Show all hardware

- `uname -a`
- `cat /proc/cpuinfo`
- `cat /proc/meminfo`
- `lshw`

Linux OS Exploration

- Kernel version, architecture, etc
- Info about CPU
- Info about RAM
- Show all hardware
- Enumerate disks & block devices

- `uname -a`
- `cat /proc/cpuinfo`
- `cat /proc/meminfo`
- `lshw`
- `lsblk -f`

Linux OS Exploration

- Kernel version, architecture, etc — `uname -a`
- Info about CPU — `cat /proc/cpuinfo`
- Info about RAM — `cat /proc/meminfo`
- Show all hardware — `lshw`
- Enumerate disks & block devices — `lsblk -f`
- Default user setttings — `/etc/skel/`

Filesystem Exploration

Explore the contents of the initially-accessed device (manually and automated).

```
find . -type f | grep -i 'XXXX'

ls -R | grep -i 'XXXX'

grep -rni 'XXXX'
```

Software Exploration

- Most organizations *templatize* their IT infrastructure
  - Default installs
  - Default configurations
  - etc.
- Anything available for use is available for exploitation/abuse
  - Locally & elsewhere*
- `ps aux`
  - Current shell session
- `sudo ps aux`
  - Current user session

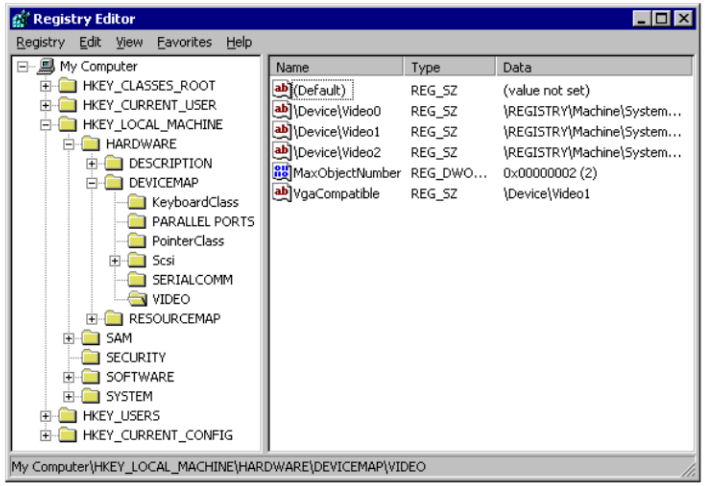
Windows Config Exploration

"[A] central hierarchal database used to store information that is necessary to configure the system for one or more users, applications, and hardware devices."

Pre-Windows 2000

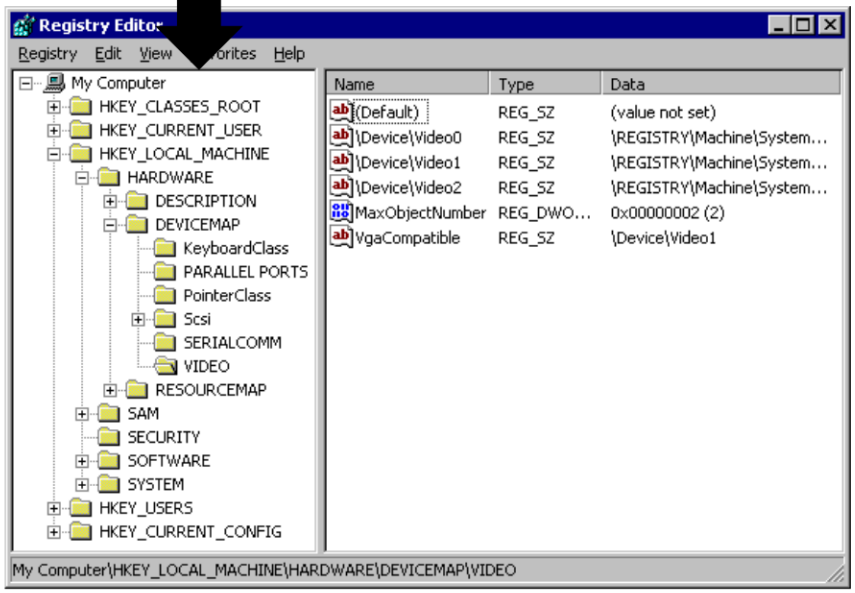
- boot.ini
- system.ini
- win.ini

Post-Windows 2000



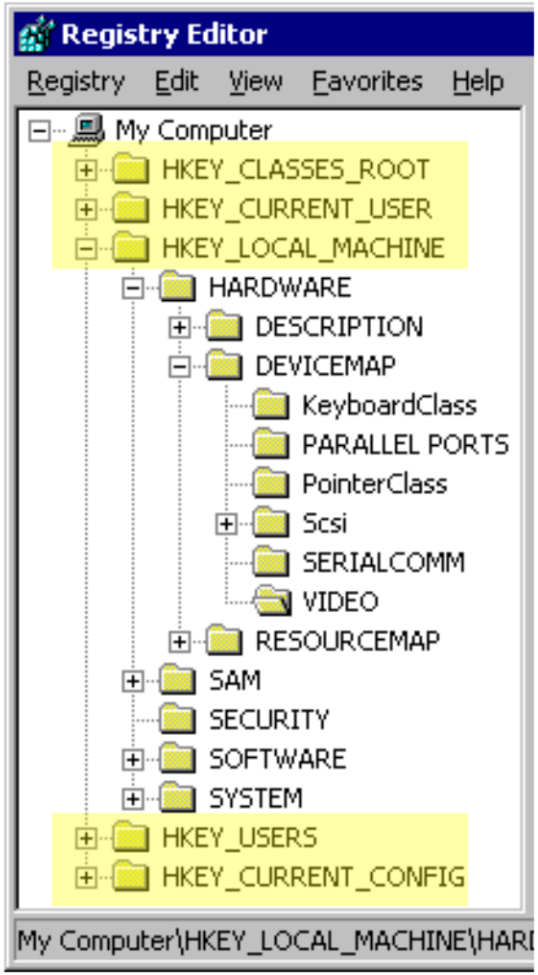
Windows Registry

- Registry keys
  - Hold multiple “values” analogous to FS directories



Windows Registry

- "Hives"
  - Logical grouping of registry key collections

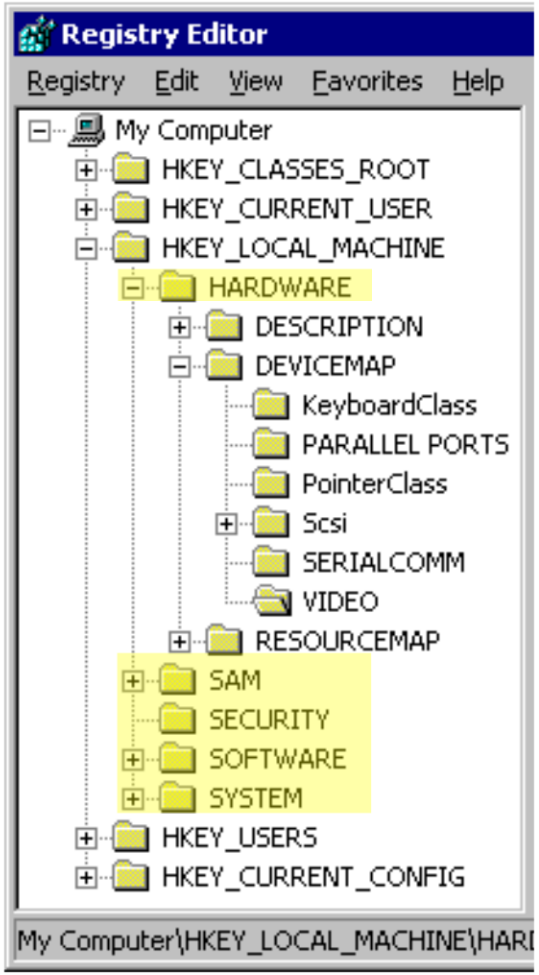


Hive Organization

- HKEY_CLASSES_ROOT (HKCR)
  - Information related to file name extensions and Object Linking and Embedding (OLE) mappings
- HKEY_CURRENT_USER (HKCU)
  - Settings for the currently logged on user
- HKEY_USERS (HKU)
  - Information of different user settings consolidated from HKCU hive
- HKEY_LOCAL_MACHINE (HKLM)
  - Information about HW and SW on the system
- HKEY_CURRENT_CONFIG (HKCC)
  - Information about current HW configurations
  - Usually empty until loaded during the boot process
  - Loads HW profiles into HKLM

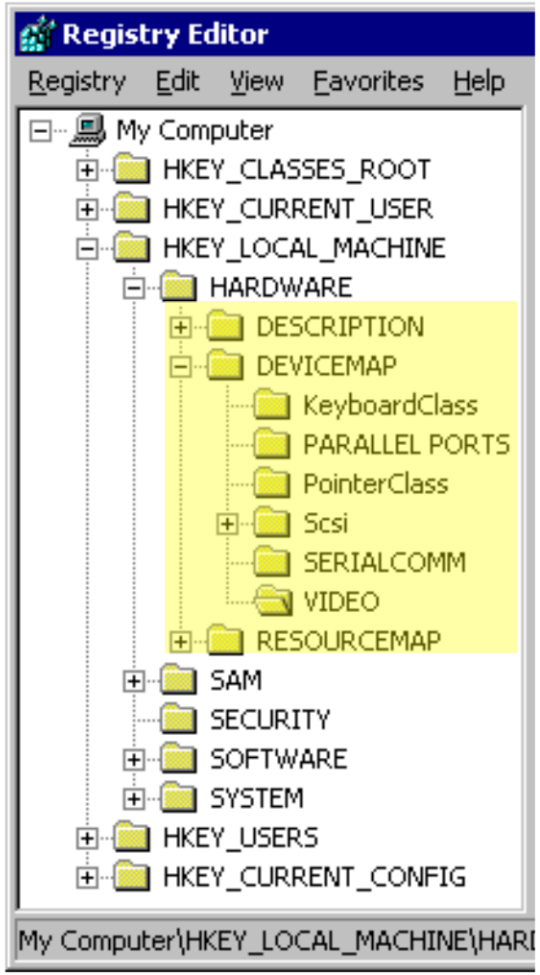
Windows Registry

- "Hives"
  - Logical grouping of registry key collections
- "Keys"



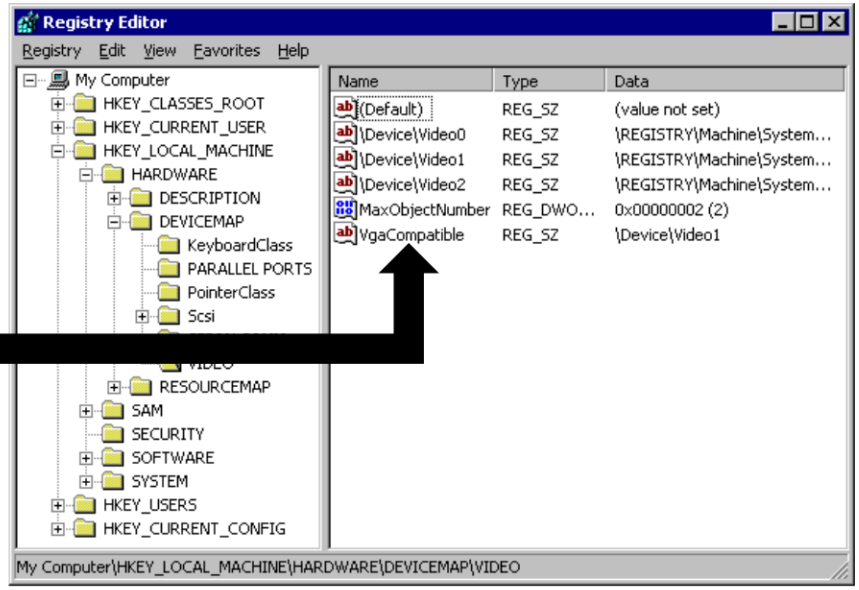
Windows Registry

- "Hives"
  - Logical grouping of registry key collections
- "Keys"
- "Subkeys"
  - Registry keys logically nested under other registry keys



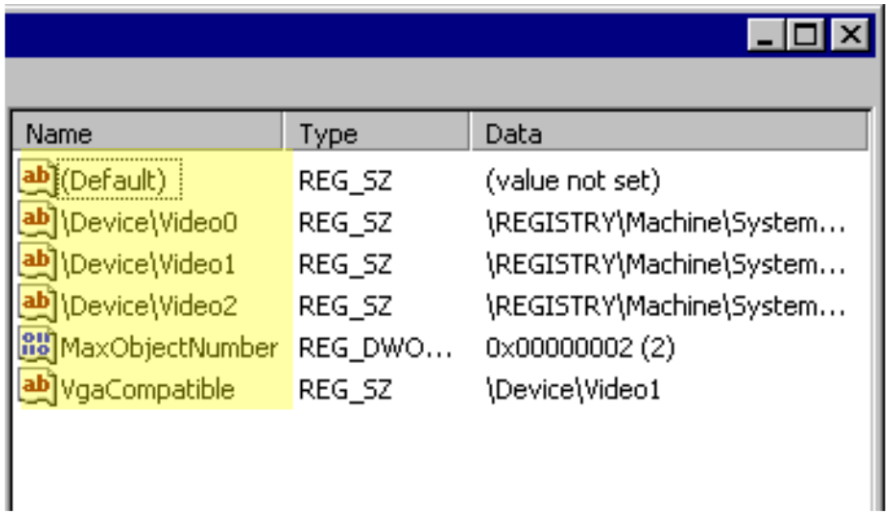
Windows Registry

- Registry keys
  - Hold multiple “values” analogous to FS directories
- Registry values
  - Hold a single, typed configuration analogous to FS files



Windows Registry

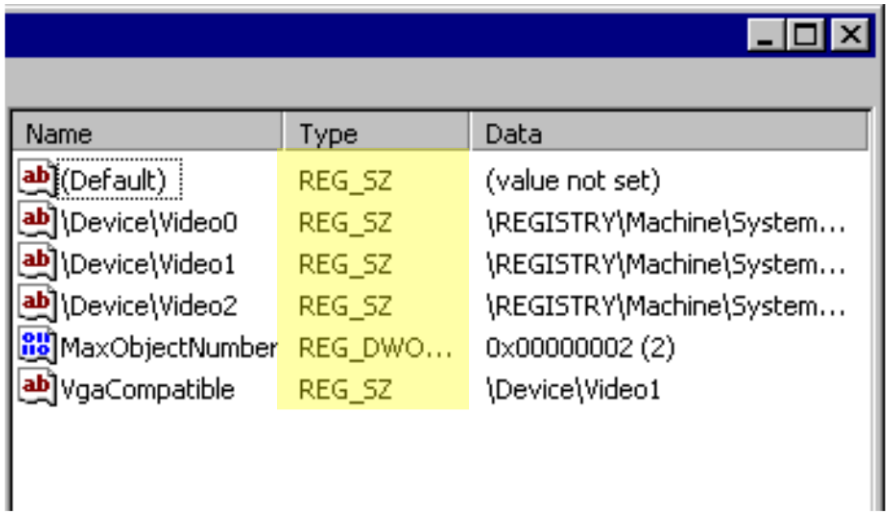
- "Key Name"
  - Lowest referenceable tree node



Name	Type	Data
(Default)	REG_SZ	(value not set)
\Device\Video0	REG_SZ	\REGISTRY\Machine\System...
\Device\Video1	REG_SZ	\REGISTRY\Machine\System...
\Device\Video2	REG_SZ	\REGISTRY\Machine\System...
MaxObjectNumber	REG_DWO...	0x00000002 (2)
VgaCompatible	REG_SZ	\Device\Video1

Windows Registry

- "Key Name"
  - Lowest referenceable tree node
- "Key Type"
  - Indicates how to interpret the contents



Name	Type	Data
(Default)	REG_SZ	(value not set)
\Device\Video0	REG_SZ	\REGISTRY\Machine\System...
\Device\Video1	REG_SZ	\REGISTRY\Machine\System...
\Device\Video2	REG_SZ	\REGISTRY\Machine\System...
MaxObjectNumber	REG_DWO...	0x00000002 (2)
VgaCompatible	REG_SZ	\Device\Video1

Windows Registry

- "Key Na
  - Lowes
    tree no
- "Key Ty
  - Indicat
    interpr

Registry value types

Article • 02/08/2023 • 7 contributors

Feedback

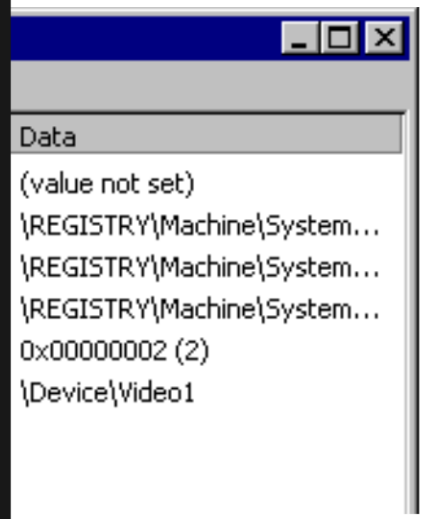
In this article

A *registry value* can store data in one of several formats, such as a string value or an integer value. When you store data in a registry value—for instance by calling the RegSetValueEx function—you can indicate the type of data being stored by specifying one of the types in the table below. When you retrieve a registry value, functions such as RegQueryValueEx use these types to indicate the type of data retrieved.

The following registry value types are defined in the winnt.h header file:

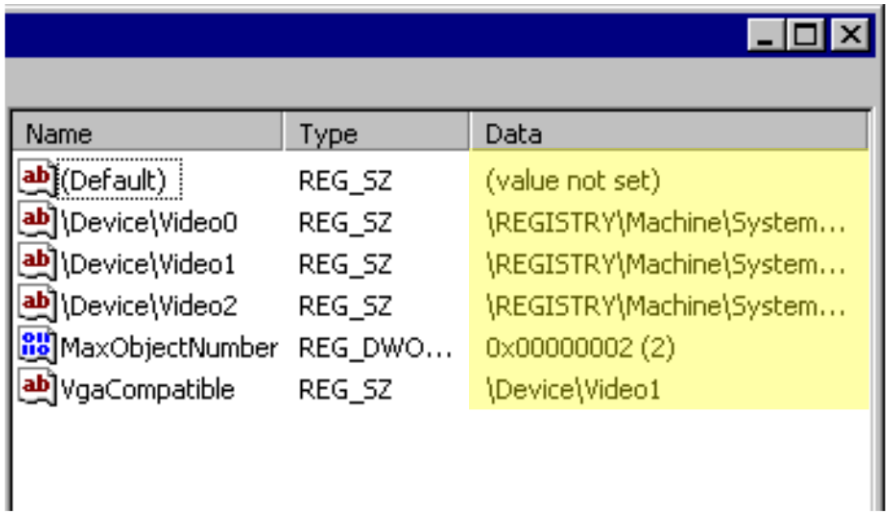
Expand table

Value	Type
REG_BINARY	Binary data in any form.
REG_DWORD	A 32-bit number.
REG_DWORD_LITTLE_ENDIAN	A 32-bit number in little-endian format. Windows is designed to run on little-endian computer architectures. Therefore, this value is defined as REG_DWORD



Windows Registry

- "Key Name"
  - Lowest referenceable tree node
- "Key Type"
  - Indicates how to interpret the contents
- "Key Data"
  - Configuration data



Name	Type	Data
(Default)	REG_SZ	(value not set)
\Device\Video0	REG_SZ	\REGISTRY\Machine\System...
\Device\Video1	REG_SZ	\REGISTRY\Machine\System...
\Device\Video2	REG_SZ	\REGISTRY\Machine\System...
MaxObjectNumber	REG_DWO...	0x00000002 (2)
VgaCompatible	REG_SZ	\Device\Video1

Linux System Config

Linux configuration is more … distributed …

Linux System Config

Linux configuration is more … distributed …

- Every app/service/etc is responsible for its own config data
- Services/Daemons nominally in /etc/
- Makes heavy use of symbolic files

```
/etc/
├── PackageKit
│   ├── PackageKit.conf
│   └── Vendor.conf
├── X11
│   ├── Xreset
│   ├── Xreset.d
│   │   └── README
│   ├── Xresources
│   │   └── x11-common
│   ├── Xsession
│   ├── Xsession.d
│   │   ├── 20dbus_xdg-runtime
│   │   ├── 20x11-common_process-args
│   │   ├── 30x11-common_xresources
│   │   ├── 35x11-common_xhost-local
│   │   ├── 40x11-common_xsessionrc
│   │   ├── 50x11-common_determine-startup
│   │   ├── 60x11-common_xdg_path
│   │   ├── 90gpg-agent
│   │   ├── 90qt-a11y
│   │   ├── 90x11-common_ssh-agent
│   │   └── 99x11-common_start
│   ├── Xsession.options
│   ├── app-defaults
│   │   ├── Editres
│   │   ├── Editres-color
│   │   ├── Viewres
│   │   ├── Viewres-color
│   │   ├── XFontSel
│   │   ├── Xfd
│   │   ├── Xmessage
│   │   └── Xmessage-color
│   ├── rgb.txt
│   ├── xkb
│   └── xorg.conf.d
├── acpi
│   ├── actions
│   │   ├── hibinit-power.sh
│   │   └── sleep.sh
```

Linux System Config

Linux configuration is more … distributed …

- Every app/service/etc is responsible for its own config data
- Services/Daemons nominally in /etc/
- Makes heavy use of symbolic files
- Home directory (`$HOME`) often used for user-specific configurations
  - $HOME/.<*app*>/
  - $HOME/.local/
  - $HOME/.config/
  - etc.

Threats and Countermeasures

Lecture 10: Discovery

COMP-5830/-6830
Spring 2024

Browser Discovery

- Browsers are excellent source of info
  - Useful for social engineering (common interests, social media, etc)
  - Internal corporate resource pages (org charts, employees, etc.)
  - Internal documentation (design docs, onboarding procedures, etc)

Browser Discovery

- Brow
  - Us
    inte
  - Int
    em
  - Int
    onl

charts,

Browser Artifacts

- Where has the user been?
- Where do they frequently go?
- What did they do when they were there?
- How did they authenticate?

Browser Data Locations

- Firefox:
  - `%userprofile%\Application Data\Mozilla\Firefox\Profiles\`
  - `%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\`
- Internet Explorer:
  - `%USERPROFILE%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\`
  - `%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\ WebCacheV*.dat`
- Chrome
  - `%USERPROFILE$\AppData\Local\Google\Chrome\User Data\`

Accessing Browser Cookies

- Firefox (and some others) use SQLite databases for storing cookies and other data

- **SQLite3 IS NOT SQL Server**
  - SQL Server is a fully-featured, datacenter-scale implementation of a SQL database engine
  - SQLite3 is SQL “minimal infrastructure” database engine which operates off of a single file

Extracting Browser Info

- Listing all tables
- `.tables`

Extracting Browser Info

- Listing all tables
- Print table schema

- `.tables`
- `PRAGMA table_info(XXXX)`

Extracting Browser Info

- Listing all tables
- Print table schema
- Extracting info from table directly

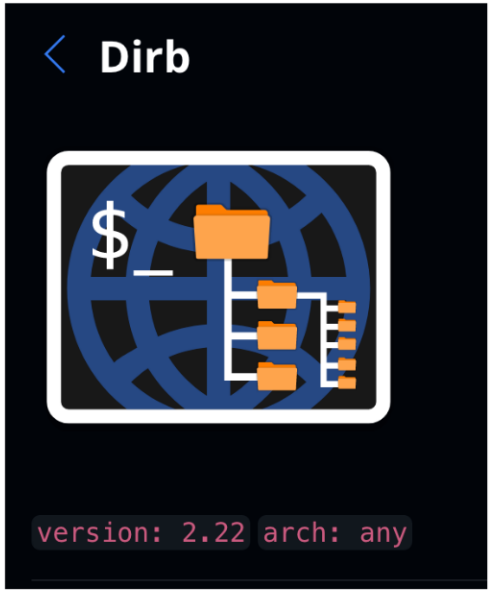
- `.tables`
- `PRAGMA table_info(XXXX)`
- *Standard SQL*

Extracting Browser Info

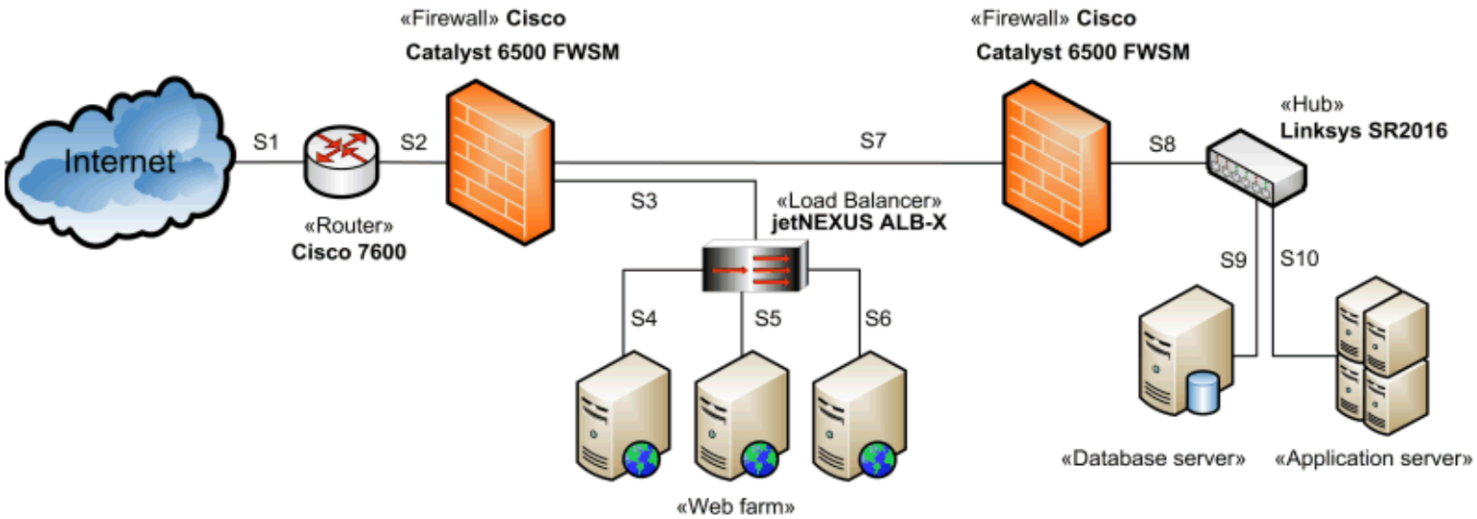
- Listing all tables
  - `.tables`
- Print table schema
  - `PRAGMA table_info(XXXX)`
- Extracting info from table directly
  - *Standard SQL*
- Dumping table data to *usable* format
  -
```
sqlite3> .mode json
sqlite3> .once out.json
sqlite3> SELECT * from XXXX;
```

Internal Network Scanning

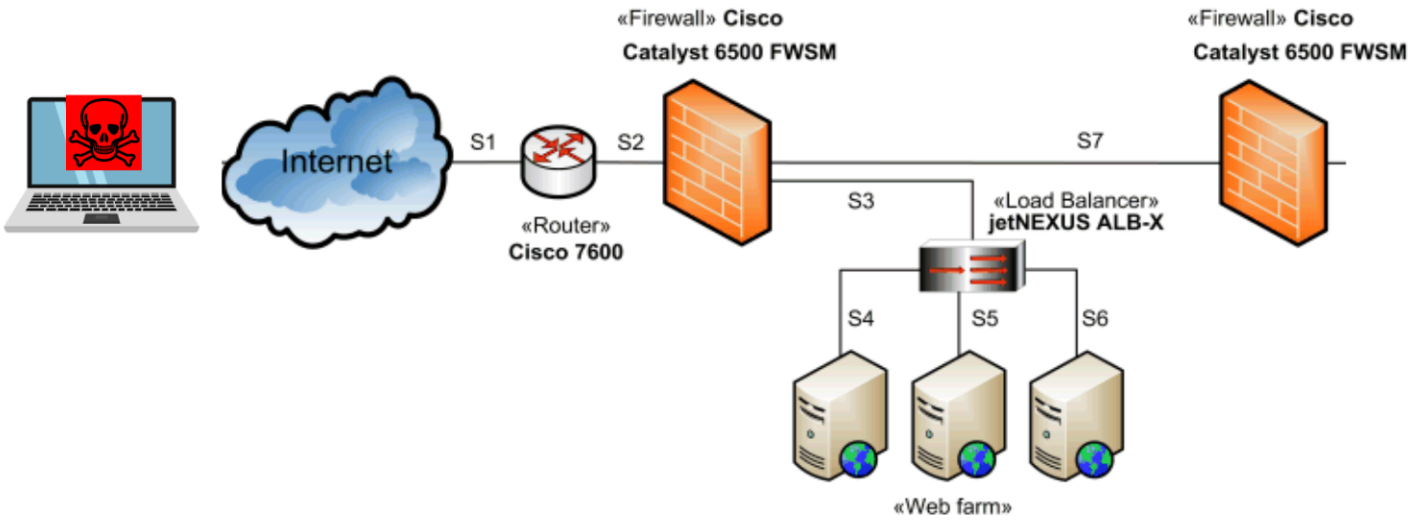
- All the same TTPs from reconnaissance but with a **different perspective.**



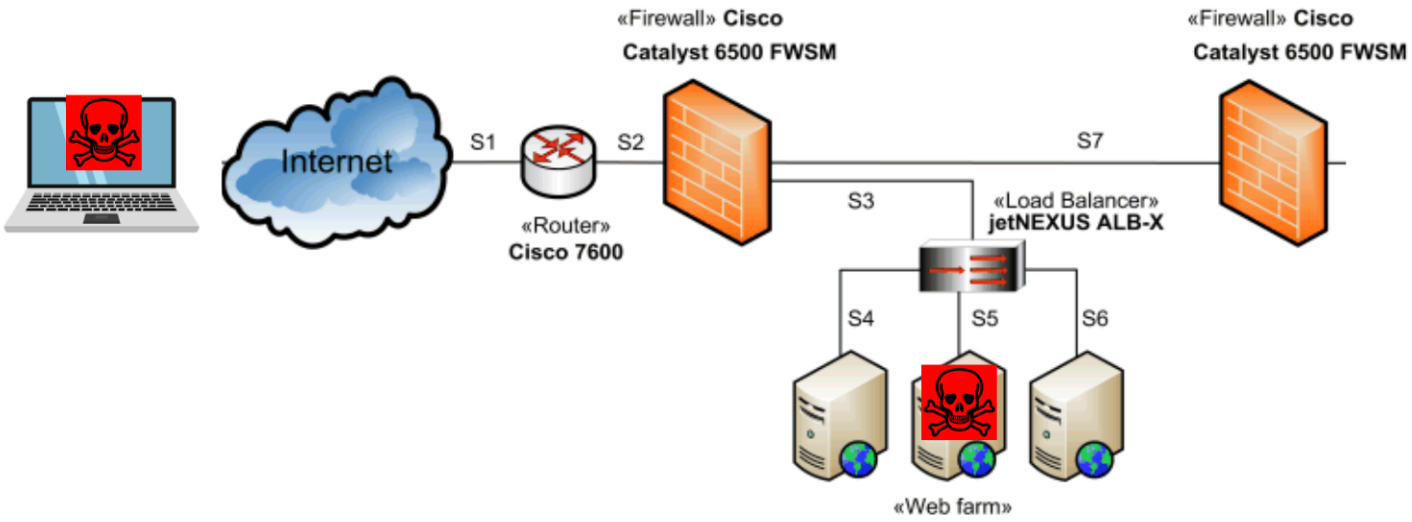
Scanning Perspective



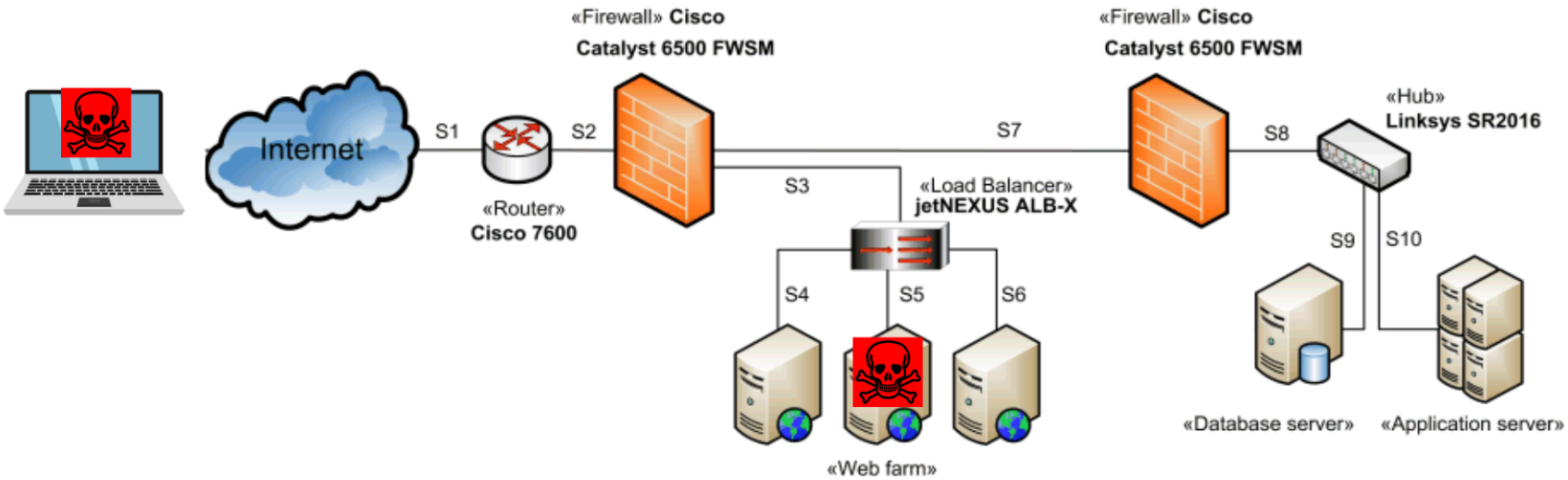
Scanning Perspective



Scanning Perspective



Scanning Perspective



Internal Network Data Collection

Internal Network Data Collection

- Active network enumeration creates risk of detection

Internal Network Data Collection

- Active network enumeration creates risk of detection
- Passive network observation does not

Internal Network Data Collection

- Active network enumeration creates risk of detection
- Passive network observation does not
- Many common tools
  - TCPDump
  - WinDump
  - Wireshark / Tshark
  - P0f
  - Network Miner

Internal Network Data Collection

- Active network enumeration creates risk of detection
- Passive network observation does not
- Many common tools
  - TCPDump
  - WinDump
  - Wireshark / Tshark
  - P0f
  - Network Miner