

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: Windows, Linux, macOS, Android, iOS, and Cloud.

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

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques
Active Scanning (2)	Acquire Infrastructure (2)	Drive-by Compromise (2)	Command and Scripting Interface (2)	Account Manipulation (2)	Abuse Elevation of Privileges (2)
Dark Web Vendors Information (2)	Exploit Public-Facing Application (2)	Exploit Public-Facing Application (2)	Container Access/Execution (2)	Boots or Logon Automation (2)	Boots or Logon Automation (2)
Dark Web Vendors Information (2)	Compromise Accounts (2)	External Remote Services (2)	Display Container (2)	Boots or Logon Initialization (2)	Boots or Logon Initialization (2)
Dark Web Vendors Information (2)	Develop Capabilities (2)	Hardware Addition (2)	Exploitation for Client Execution (2)	Browser Extensions (2)	Browser Extensions (2)
Dark Web Vendors Information (2)	Establish Accounts (2)	Phishing (2)	Inter-Process Communication (2)	Compromise Client Software Binary (2)	Client or Mobile System Processes (2)
Dark Web Vendors Information (2)	Optimize Capabilities (2)	Replication Through Removable Media (2)	Native API (2)	Create Account (2)	Domain Policy Modification (2)
Dark Web Vendors Information (2)	Supply Chain (2)	Scheduled Task/Job (2)	Scheduled Task/Job (2)	Create or Modify System Processes (2)	Escape to Host (2)
Dark Web Vendors Information (2)	Trusted Relationship (2)	Valid Accounts (2)	Serviceless Execution (2)	Event Triggered Execution (2)	Event Triggered Execution (2)
Dark Web Vendors Information (2)	Valid Accounts (2)	Shared Mailbox (2)	Software Deployment Tools (2)	External Remote Services (2)	Exploitation for Privilege Escalation (2)
Dark Web Vendors Information (2)	System Services (2)	User Execution (2)	User Execution (2)	Hijack Execution Flow (2)	Hijack Execution Flow (2)
Dark Web Vendors Information (2)	Windows Management Instrumentation (2)	Windows Management Instrumentation (2)	Windows Management Instrumentation (2)	Modify Authentication Process (2)	Process Injection (2)
Dark Web Vendors Information (2)				Office Application Startup (2)	Scheduled Task/Job (2)
Dark Web Vendors Information (2)				Pre-OS Boot (2)	Scheduled Task/Job (2)
Dark Web Vendors Information (2)				Service Software Component (2)	Traffic Signaling (2)
Dark Web Vendors Information (2)				Valid Accounts (2)	Valid Accounts (2)

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)

Network, Containers.

View on the ATT&CK® Navigator

Version Permalink

Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Discovery (2)	Exploitation of Remote Services (2)	Adversary-in-the-Middle (2)	Application Layer Protocol (2)	Automated Exfiltration (2)	Account Access Removal (2)
Discovery (2)	Internal Spearphishing (2)	Archive Collected Data (2)	Communication Through Removable Media (2)	Data Transfer Size Limits (2)	Data Destruction (2)
Discovery (2)	Lateral Tool Transfer (2)	Audio Capture (2)	Data Encoding (2)	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact (2)
Discovery (2)	Remote Service Session Hijacking (2)	Automated Collection (2)	Data Obfuscation (2)	Exfiltration Over C2 Channel (2)	Data Manipulation (2)
Discovery (2)	Remote Services (2)	Browser Session Hijacking (2)	Dynamic Resolution (2)	Exfiltration Over Other Network Medium (2)	Defacement (2)
Discovery (2)	Replication Through Removable Media (2)	Clipboard Data (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (2)	Disk Wipe (2)
Discovery (2)	Software Deployment Tools (2)	Data from Cloud Storage (2)	Fallback Channels (2)	Exfiltration Over Web Service (2)	Endpoint Denial of Service (2)
Discovery (2)	Taint Shared Content (2)	Data from Configuration Repository (2)	Ingress Tool Transfer (2)	Exfiltration Through Web Service (2)	Firmware Corruption (2)
Discovery (2)	Use Alternate Authentication Material (2)	Data from Information Repositories (2)	Multi-Stage Channels (2)	Scheduled Transfer (2)	Inhibit System Recovery (2)
Discovery (2)		Data from Local System (2)	Non-Application Layer Protocol (2)	Transfer Data to Cloud Account (2)	Network Denial of Service (2)
Discovery (2)		Data from Network Shared Drive (2)	Non-Standard Port (2)		Resource Hijacking (2)
Discovery (2)		Data from Removable Media (2)	Protocol Tunneling (2)		Service Stop (2)
Discovery (2)		Data Staged (2)	Proxy (2)		System Shutdown/Reboot (2)
Discovery (2)		Email Collection (2)	Remote Access Software (2)		
Discovery (2)		Input Capture (2)	Traffic Signaling (2)		
Discovery (2)		Screen Capture (2)	Web Service (2)		
Discovery (2)		Video Capture (2)			

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

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)	

Types of Credentials



User-Related

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



Account security

Scan the QR code below using your authenticator application, then enter a valid code below to verify correct setup.

Can't Scan it?

Verification Code

Code

Save your backup codes

Keep these backup codes somewhere safe but accessible.

☐ 7958 9575	☐ 9639 3831
☐ 7630 8446	☐ 3243 6466
☐ 1406 4023	☐ 8634 2741
☐ 7693 9161	☐ 5029 5319
	☐ 4535 6352

backup code once.
generated on: Nov 9, 2017.

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



KEY CROC



HAK5

INTRODUCING



SCREEN CRAB



HAK5

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 $\leftrightarrow$ 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

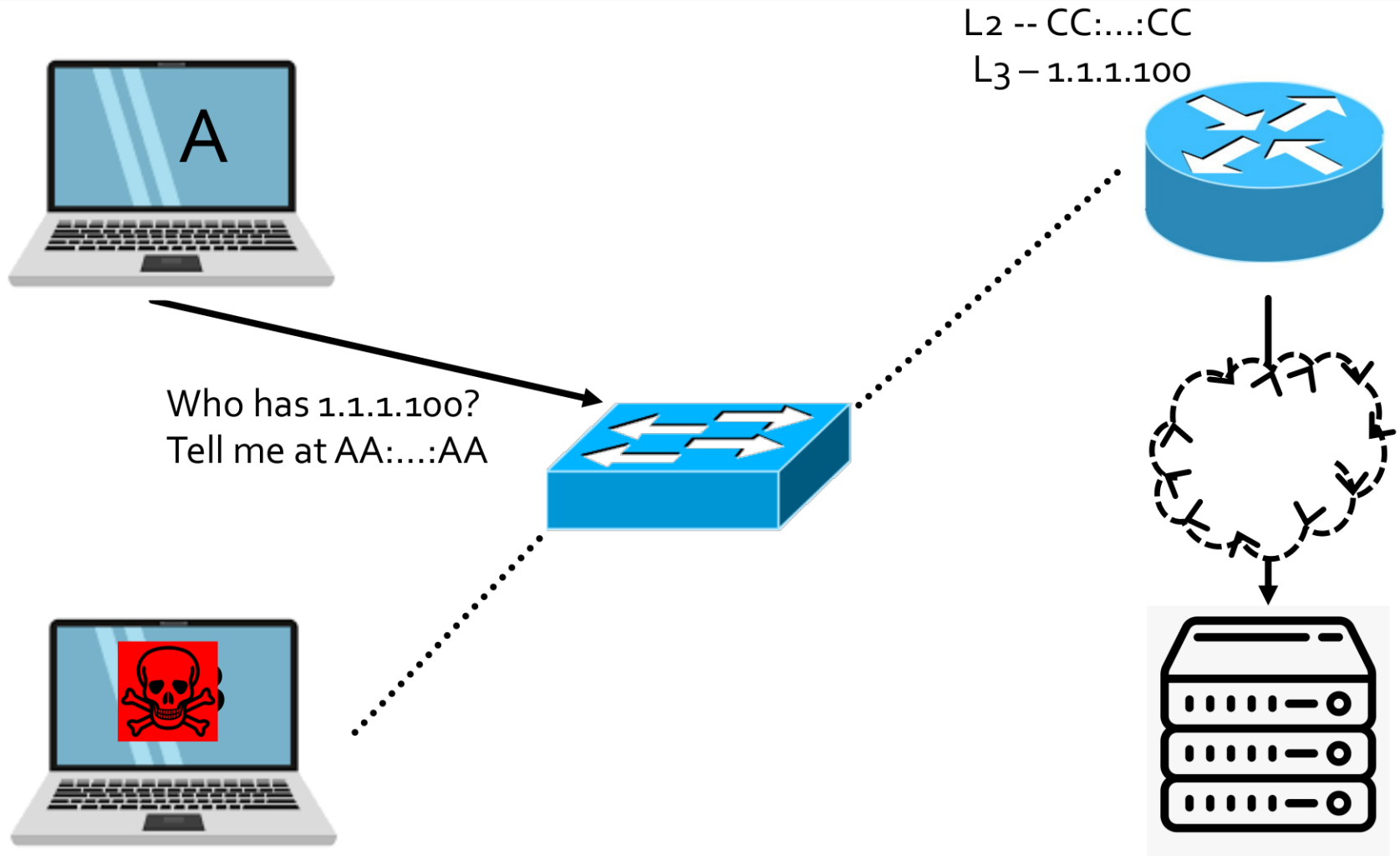
ARP Poisoning/Spoofing



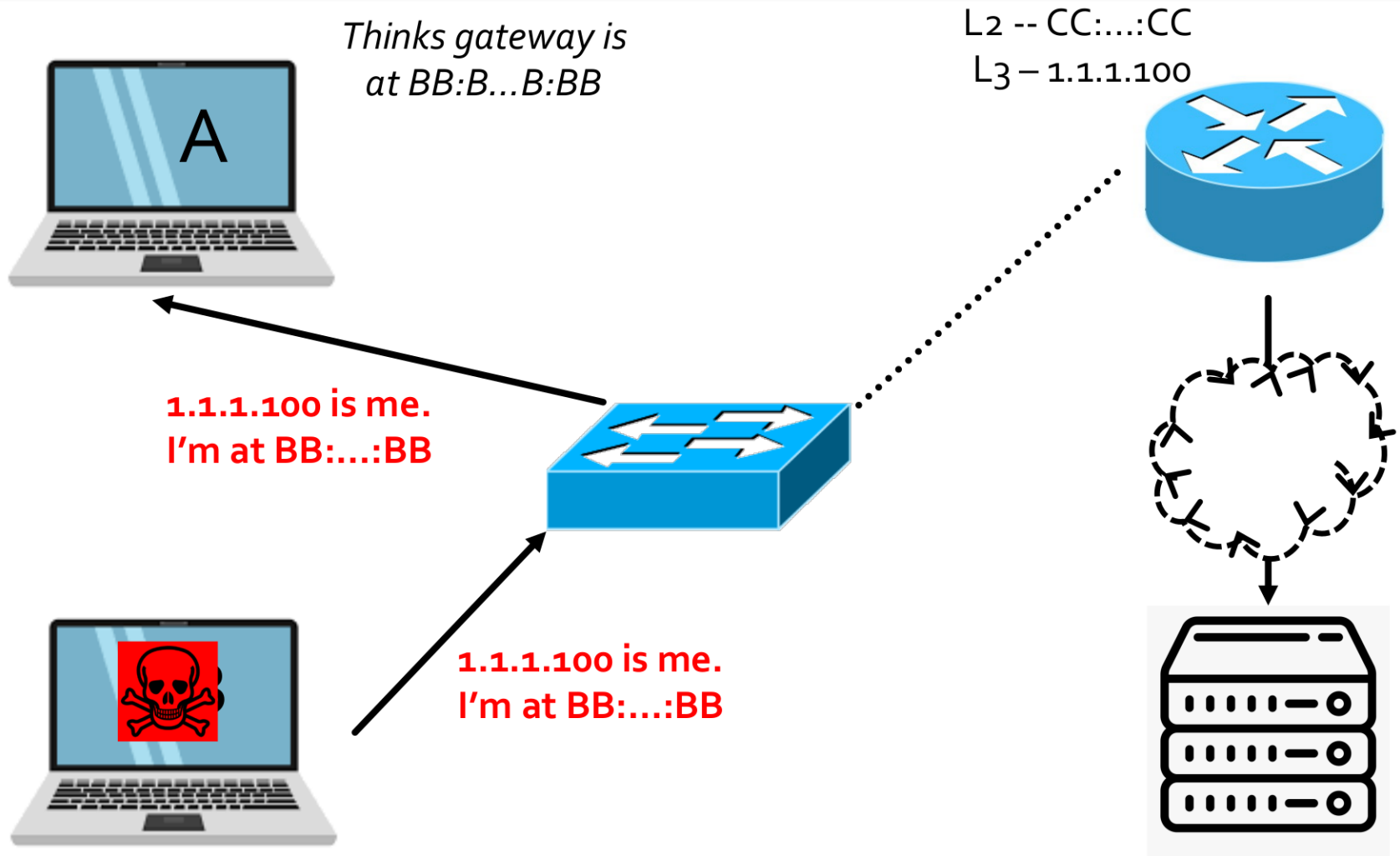
ARP Poisoning/Spoofing Attacks are a set of techniques used to misdirect traffic on the network.

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

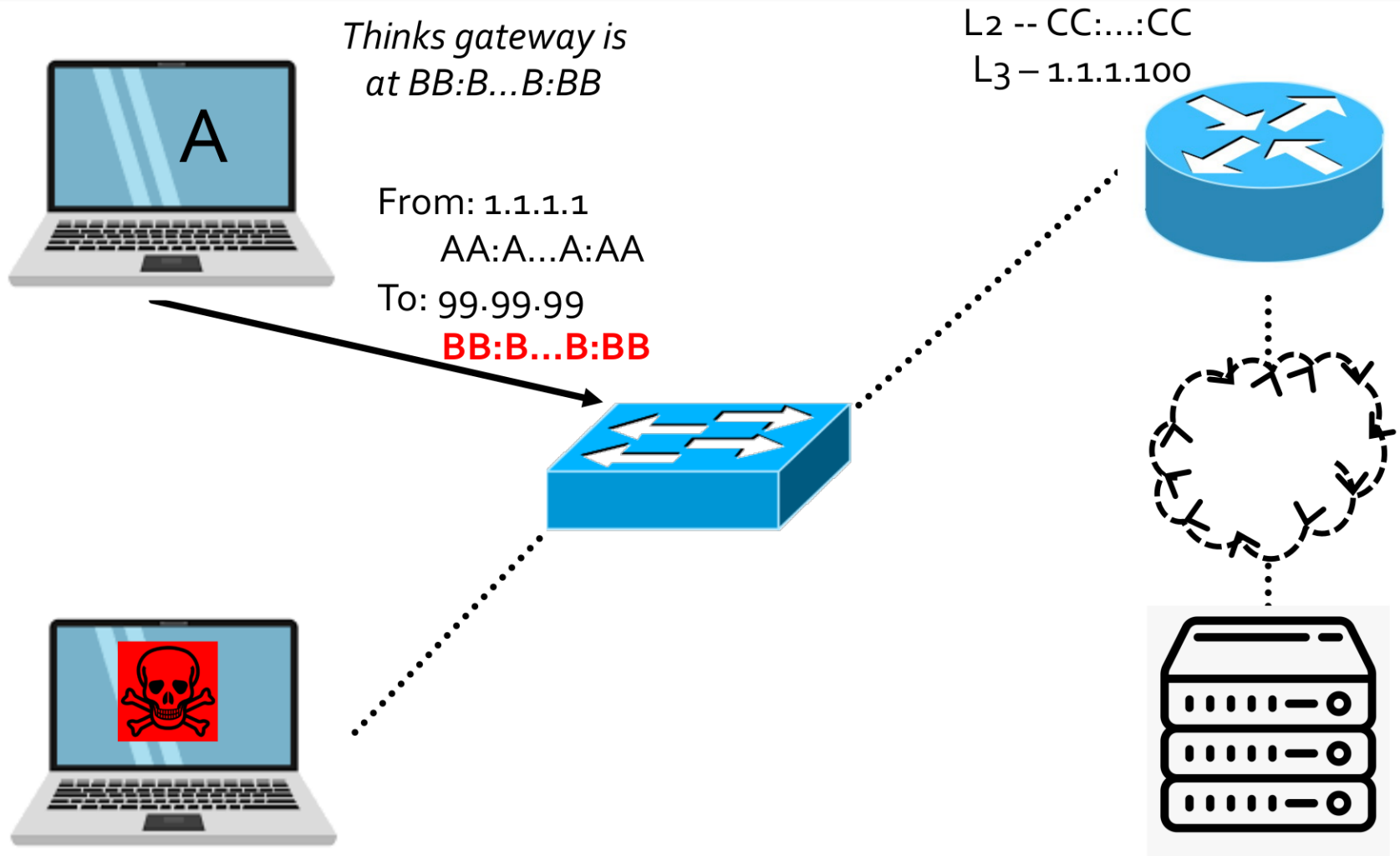
ARP Poisoning/Spoofing



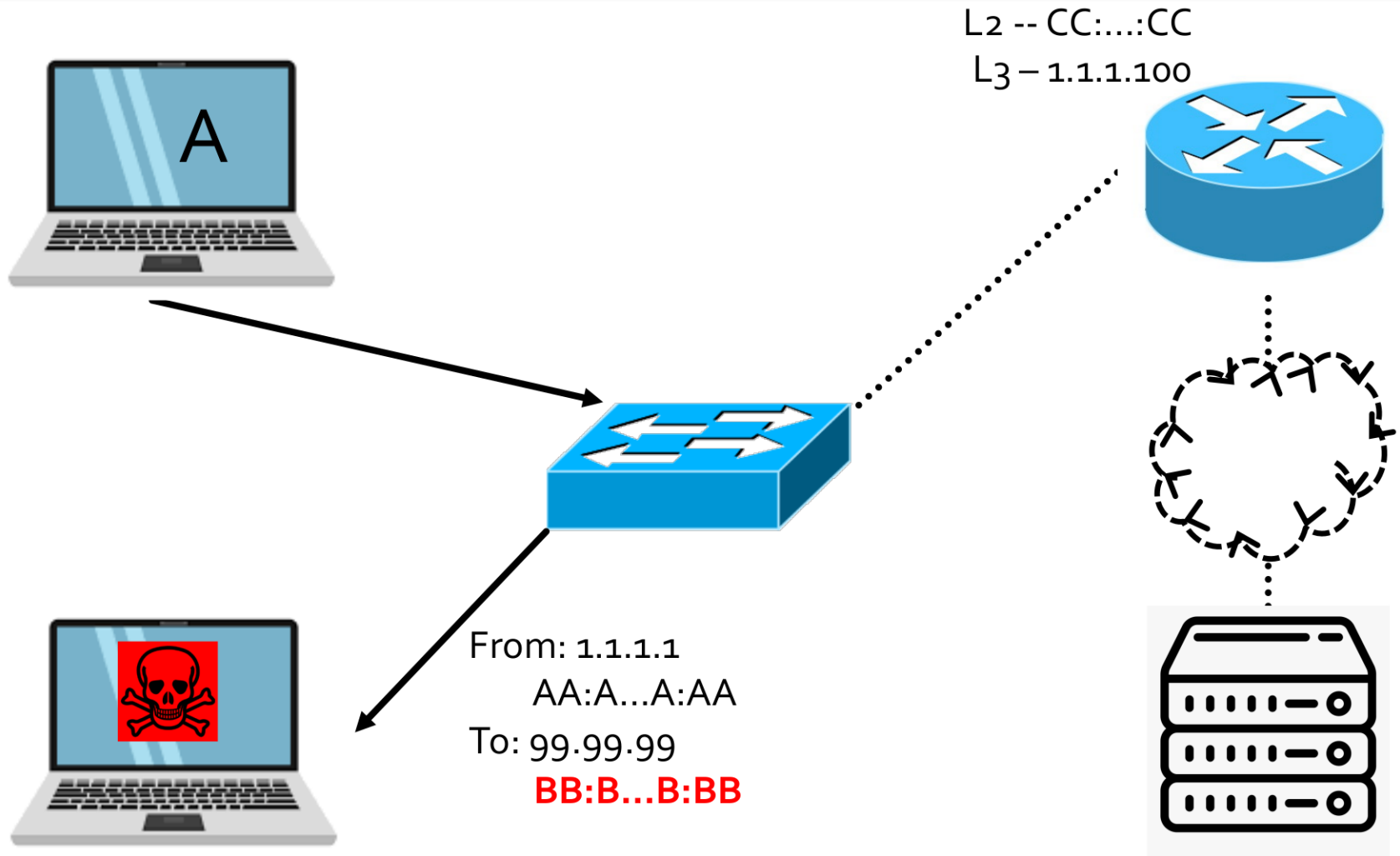
ARP Poisoning/Spoofing



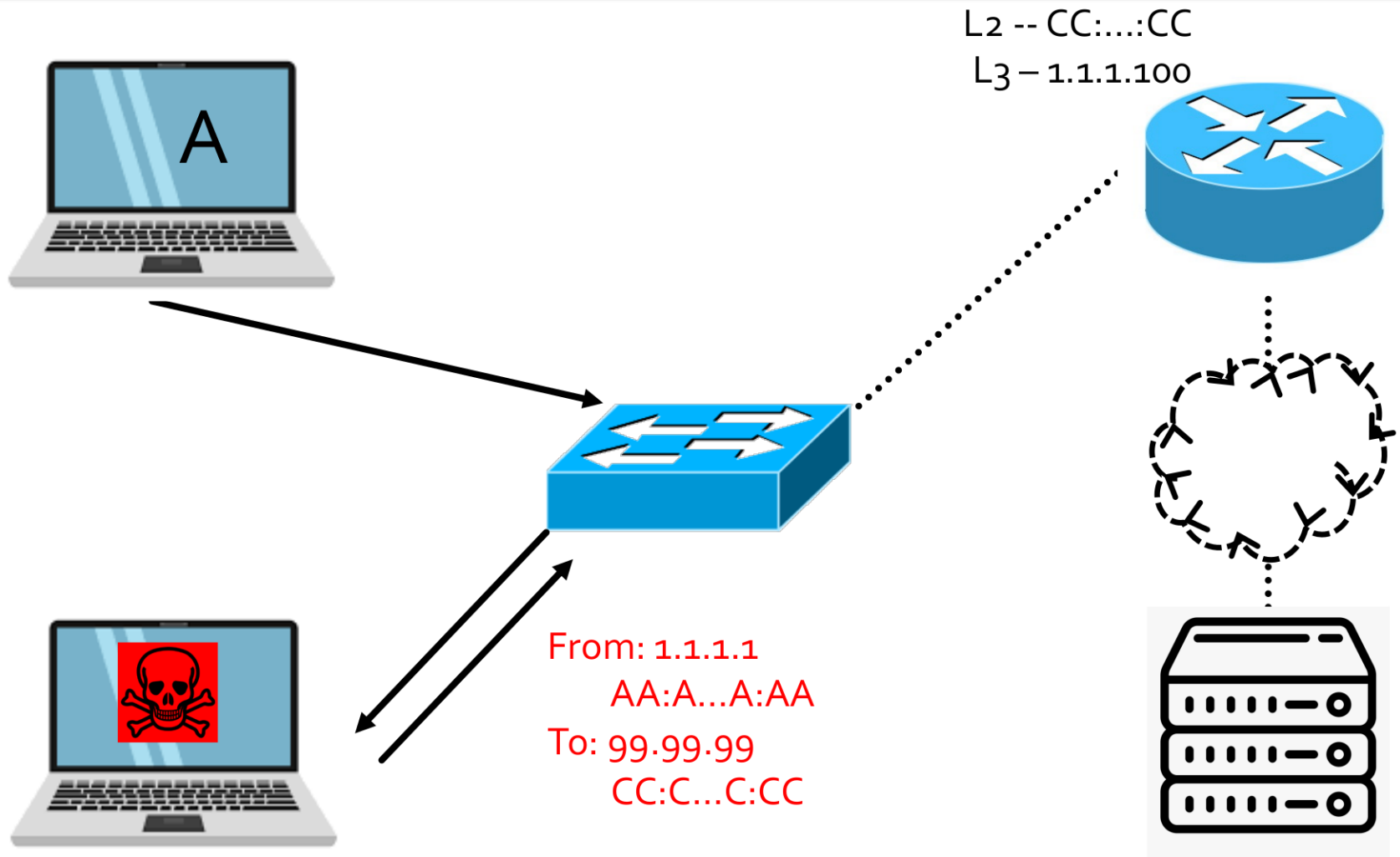
ARP Poisoning/Spoofing



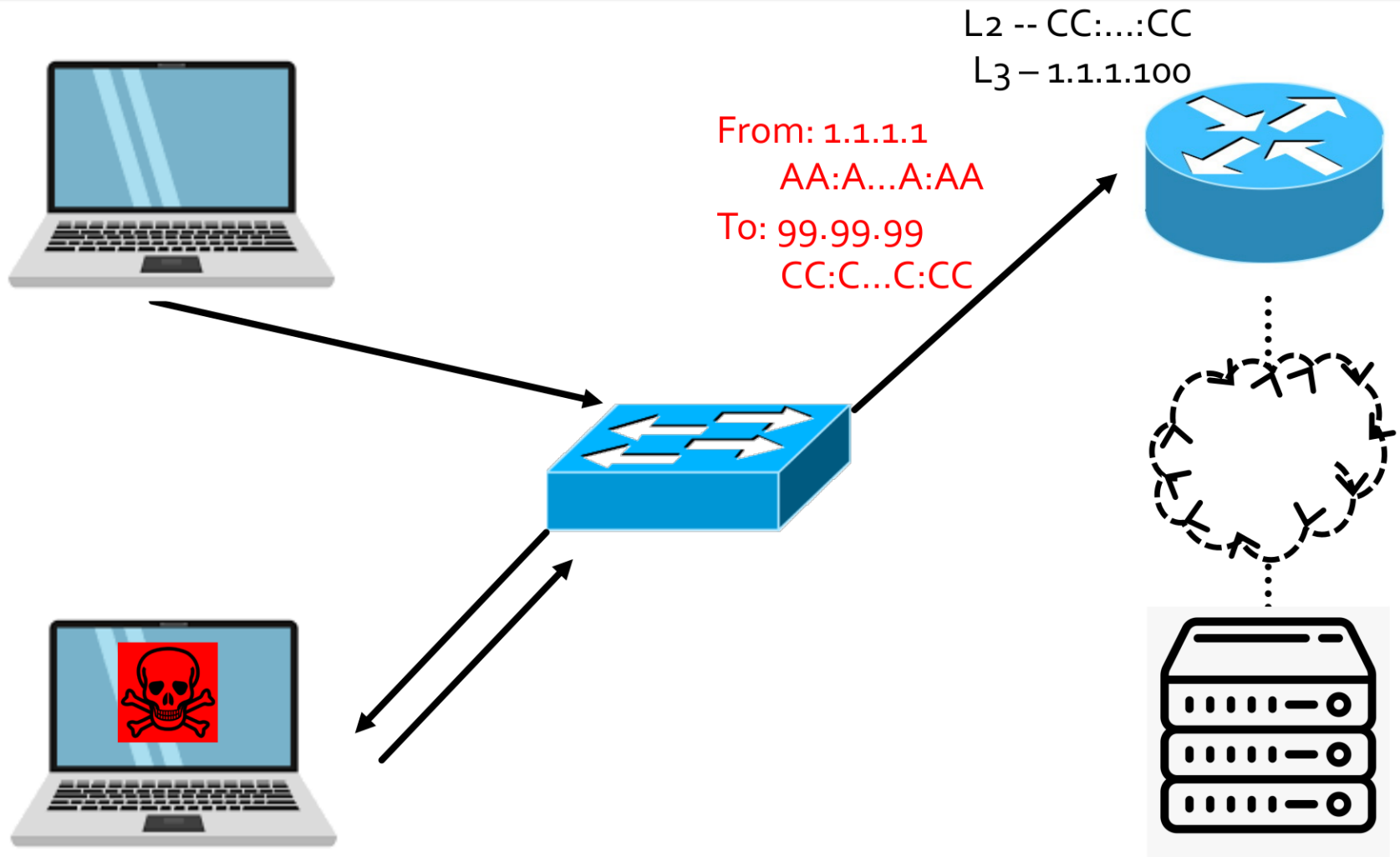
ARP Poisoning/Spoofing



ARP Poisoning/Spoofing



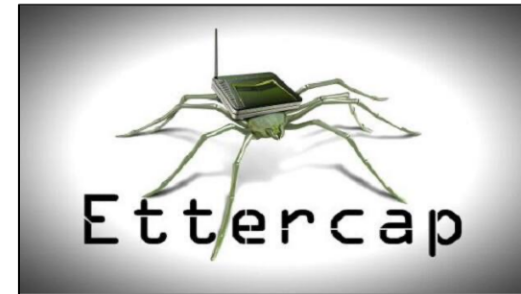
ARP Poisoning/Spoofing



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



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, Linux, macOS, and Android.

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

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques
Active Scanning (2)	Acquire Infrastructure (2)	Drive-by Compromise	Command and Scripting Interface (2)	Account Manipulation (2)	Abuse Elevation of Privileges (2)
Batcher Victim Host Substitution (2)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Job	Access Token Manipulation (2)
Garbage Victim Identity Information (2)	Compromise Infrastructure (2)	External Remote Services	Display Container	Boot or Logon Assistant Execution (2)	Boot or Logon Assistant Execution (2)
Garbage Victim Network Information (2)	Develop Capabilities (2)	Hardware Addition	Exploitation for Client Execution	Boot or Logon Initialization Script (2)	Boot or Logon Initialization Script (2)
Golden Victim Org Information (2)	Establish Accounts (2)	Phishing (2)	Inter-Process Communication (2)	Browser Extension	Client or Mobile Application (2)
Pushing for Information (2)	Optimize Capabilities (2)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)
Search Closed Sources (2)	Supply Chain Compromise (2)	Scheduled Task/Job (2)	Scheduled Task/Job (2)	Create or Modify System Properties (2)	Event Triggered Execution (2)
Search Open Technical Platforms (2)	Trusted Relationship	Valid Accounts (2)	Serverless Execution	Event Triggered Execution (2)	Exploitation for Privilege Escalation
Search Open Webpages (2)	Valid Accounts (2)	Shared Mailbox	Software Deployment Tools	External Remote Services	Hijack Execution Flow (2)
Search Victim-Related Websites	System Services (2)	User Execution (2)	User Execution (2)	Impair Internal Image	Modify Authentication Process (2)
	Windows Management Instrumentation	Windows Management Instrumentation	Windows Management Instrumentation	Modify Authentication Process (2)	Office Application Startup (2)
				Pre-OS Boot (2)	Pre-OS Boot (2)
				Scheduled Task/Job (2)	Scheduled Task/Job (2)
				Service Software Component (2)	Service Software Component (2)
				Traffic Signaling (2)	Traffic Signaling (2)
				Valid Accounts (2)	Valid Accounts (2)

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

Network, Containers.

View on the ATT&CK® Navigator or

Version Permalink

Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (2)	Automated Exfiltration (2)	Account Access Removal
Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Data Transfer Size Limits	Data Transfer Size Limits	Data Destruction
Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Communication Through Removable Media	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (2)
Cloud Service Dashboard	Browser Session Hijacking	Browser Session Hijacking	Data Obfuscation (2)	Exfiltration Over Other Network Medium (2)	Defacement (2)
Cloud Service Discovery	Remote Services (2)	Clipboard Data	Dynamic Resolution (2)	Exfiltration Over Physical Medium (2)	Disk Wipe (2)
Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Web Service (2)	Firmware Corruption
Debugger Evasion	Taint Shared Content	Data from Information Repositories (2)	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Domain Trust Discovery	Use Alternate Authentication Material (2)	Data from Local System	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (2)
File and Directory Discovery	Key Discovery	Data from Network Shared Drive	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
Group Policy Discovery	Service Discovery	Data from Removable Media	Non-Standard Port		Service Stop
Network Service Discovery	Share Discovery	Data Staged (2)	Protocol Tunneling		System Shutdown/Reboot
Network Share Discovery	Sniffing	Email Collection (2)	Proxy (2)		
Network Sniffing	System Discovery	Input Capture (2)	Remote Access Software		
Password Policy Discovery	System Discovery	Screen Capture	Traffic Signaling (2)		
Peripheral Device Discovery	System Discovery	Video Capture	Web Service (2)		
Permission Groups Discovery (3)	System Discovery				
Process Discovery	System Discovery				
Query Registry	System Discovery				
Remote System Discovery	System Discovery				
Software Discovery (1)	System Discovery				
System Information Discovery	System 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
10 techniques

Resource Development
7 techniques

Initial Access
9 techniques

Execution
13 techniques

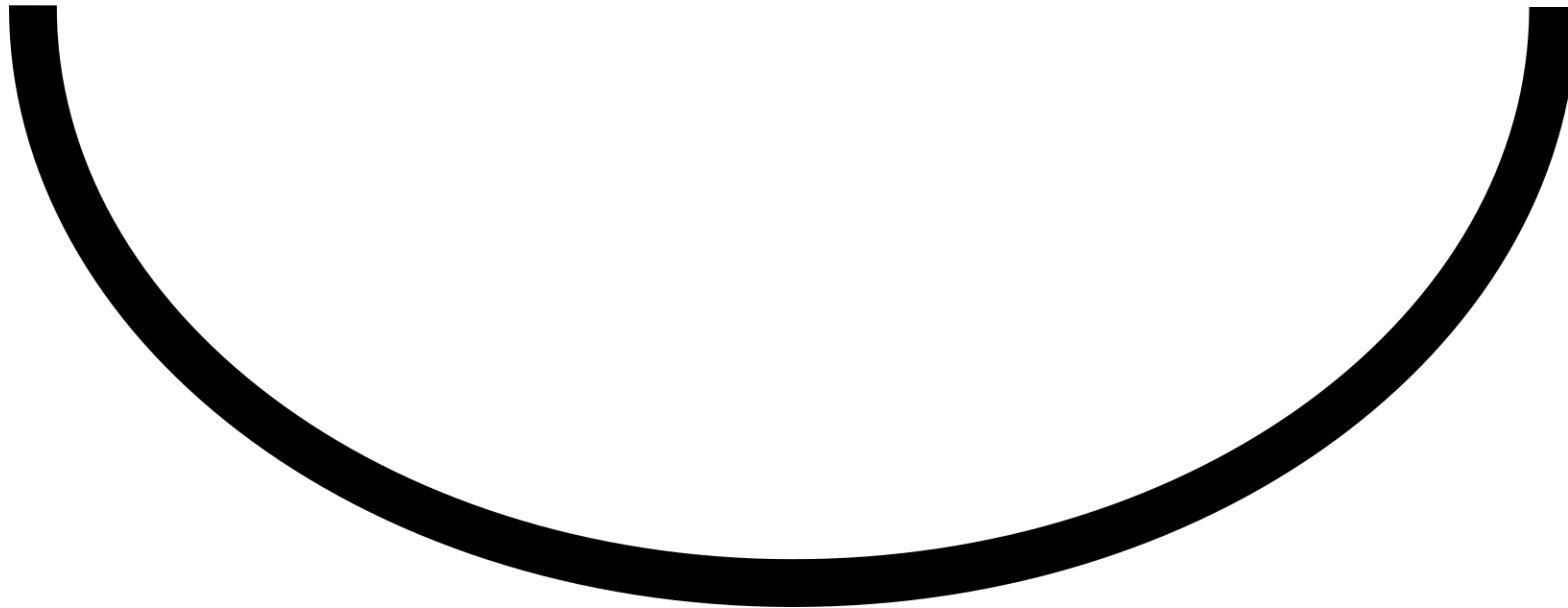
Persistence
19 techniques

Privilege Escalation
13 techniques

Defense Evasion
42 techniques

Credential Access
17 techniques

Discovery
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
10 techniques

Resource Development
7 techniques

Initial Access
9 techniques

Execution
13 techniques

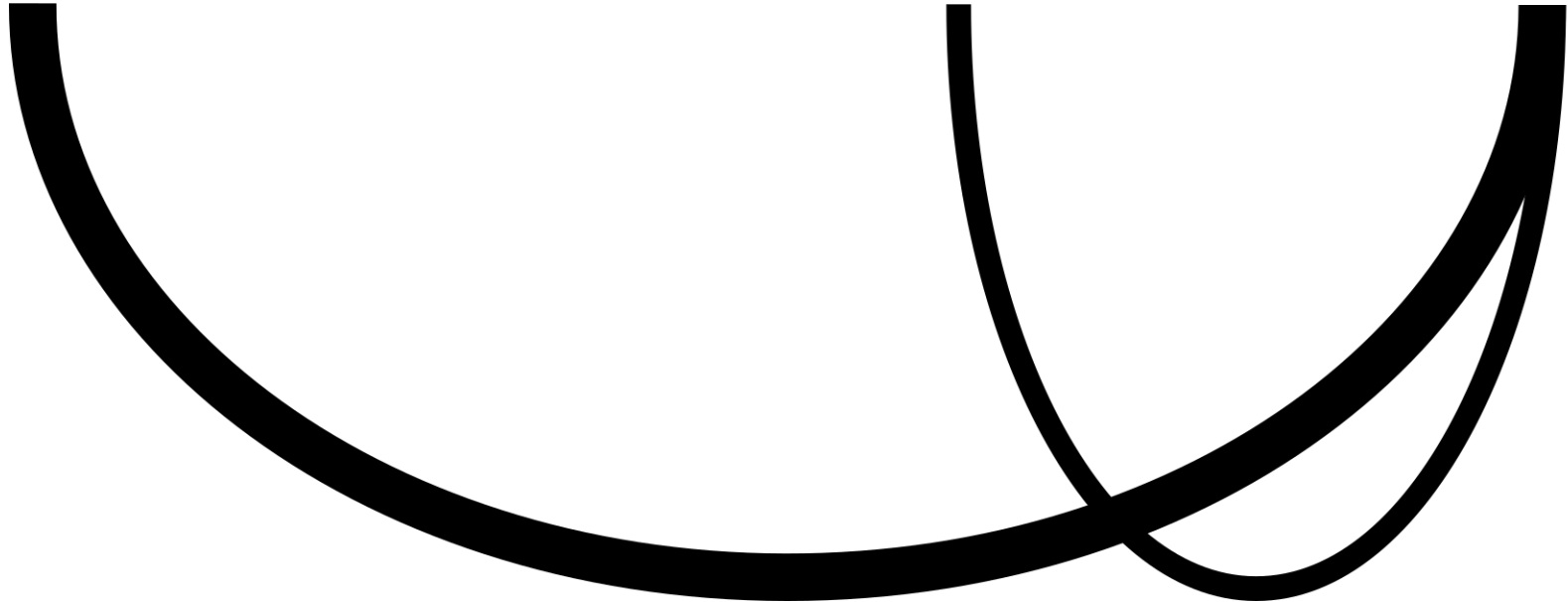
Persistence
19 techniques

Privilege Escalation
13 techniques

Defense Evasion
42 techniques

Credential Access
17 techniques

Discovery
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)



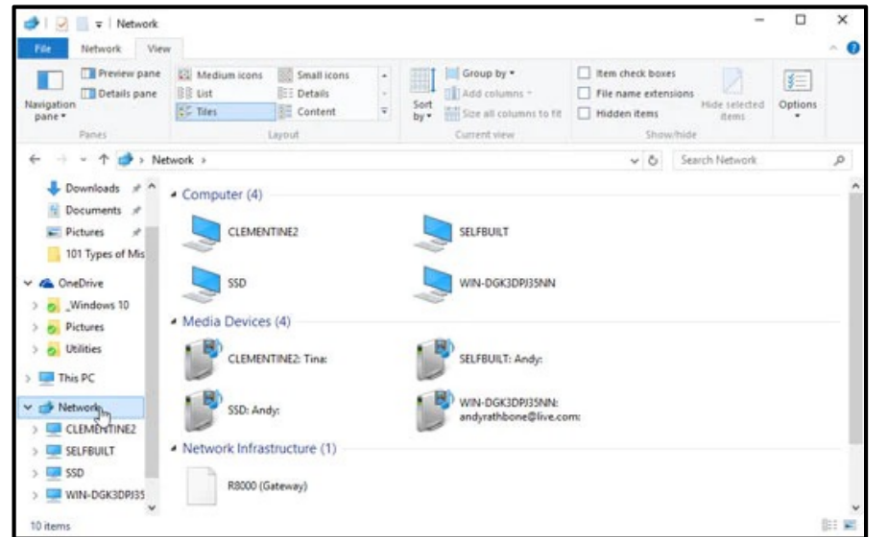
- Gain knowledge of systems/networks useful in orientating the attacker
- Explore current control/capabilities to plan follow-on actions
- Built-in OS tools are often leveraged and sufficient

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



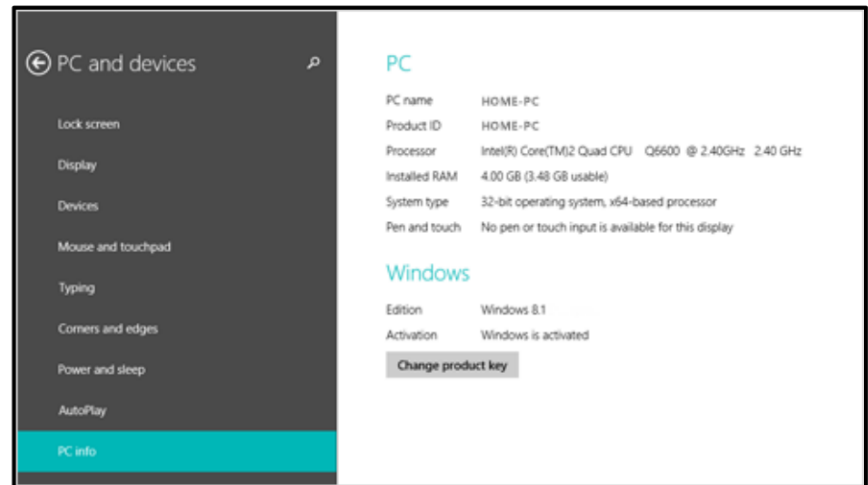
- Enumerate Disks



Windows OS Exploration

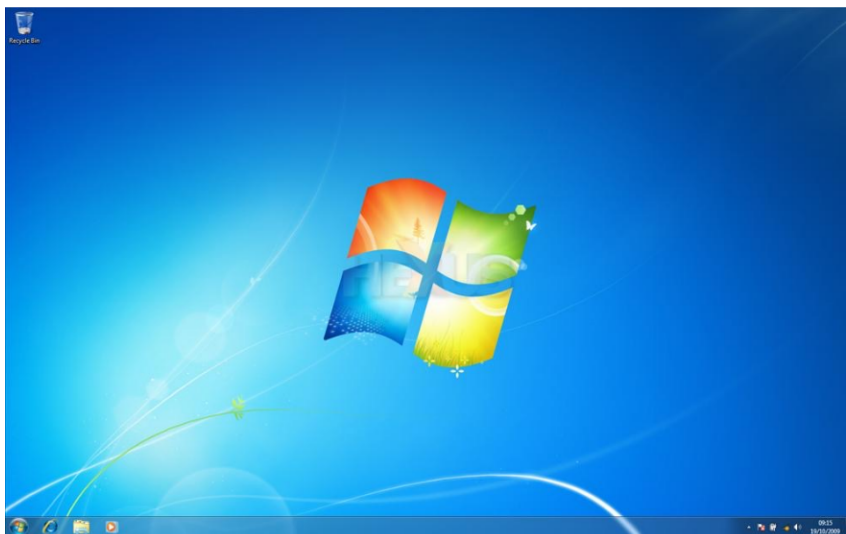


- Enumerate Disks
- Version info



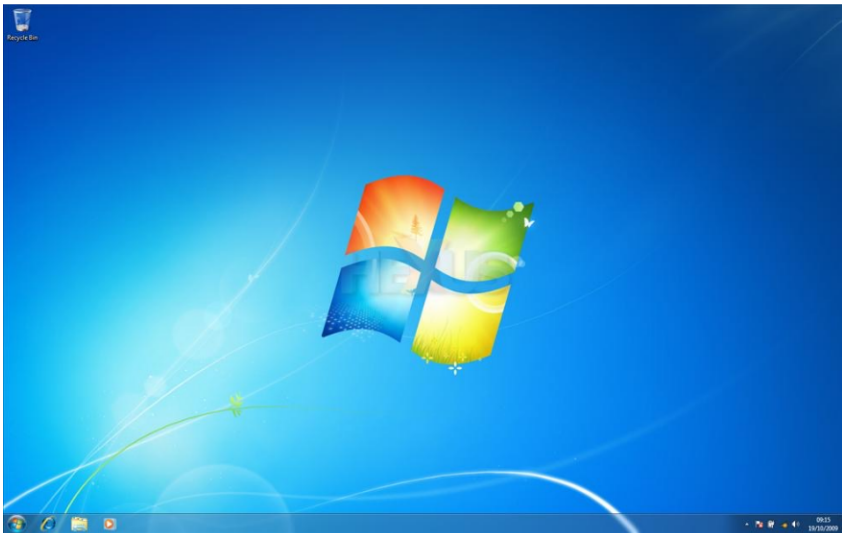


Windows 7





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 confused 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.

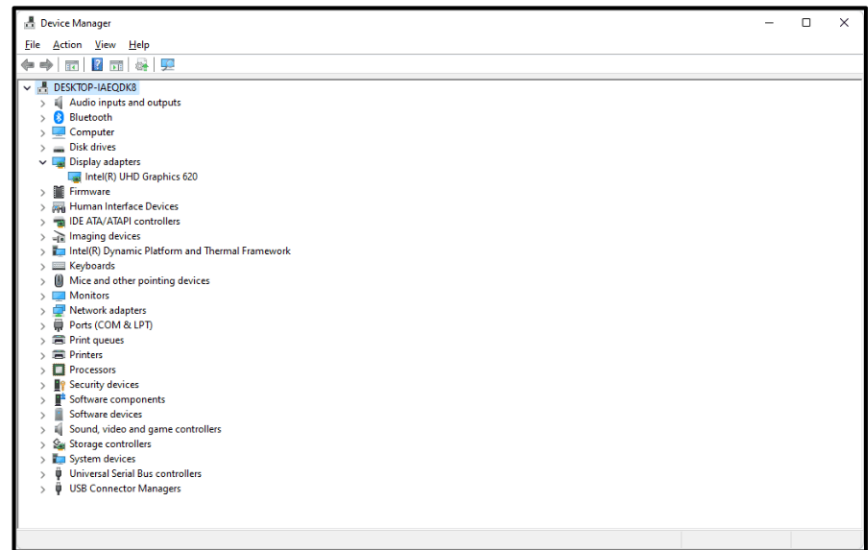
**Nick Peers** 5 min read 

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

Windows OS Exploration



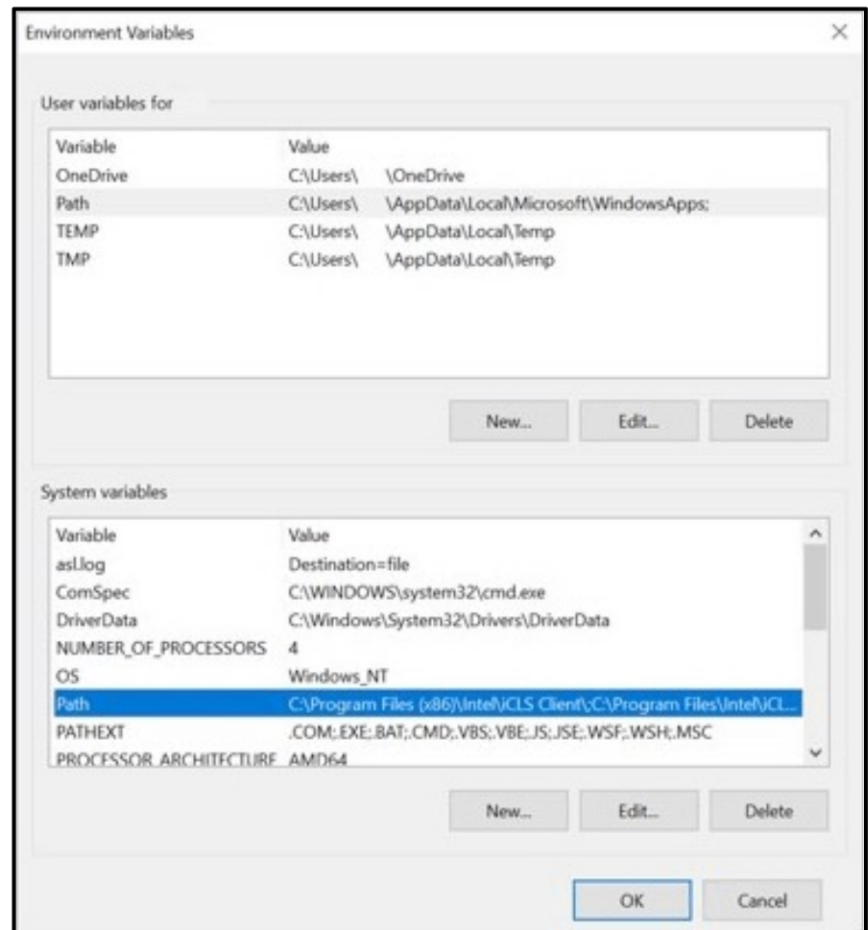
- Enumerate Disks
- Version info
- Device Manager



Windows OS Exploration



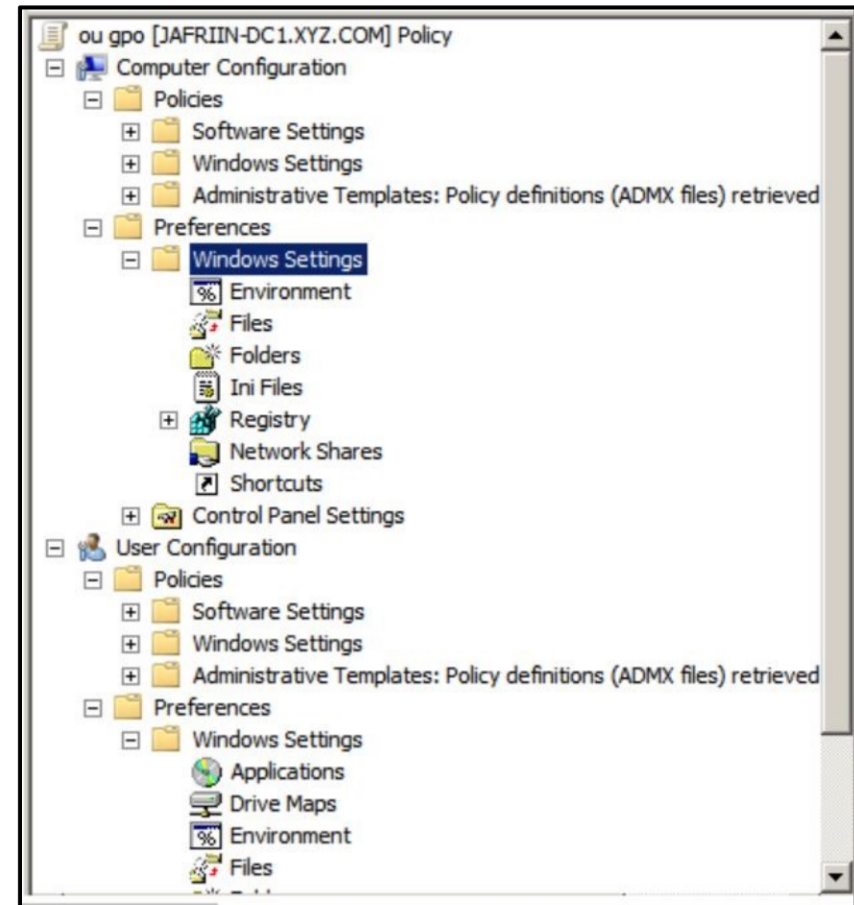
- Enumerate Disks
- Version info
- Device Manager
- Environment



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
 - Info about CPU
 - Info about RAM
 - Show all hardware
 - Enumerate disks & block devices
 - Default user settings
- `uname -a`
 - `cat /proc/cpuinfo`
 - `cat /proc/meminfo`
 - `lshw`
 - `lsblk -f`
 - `/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

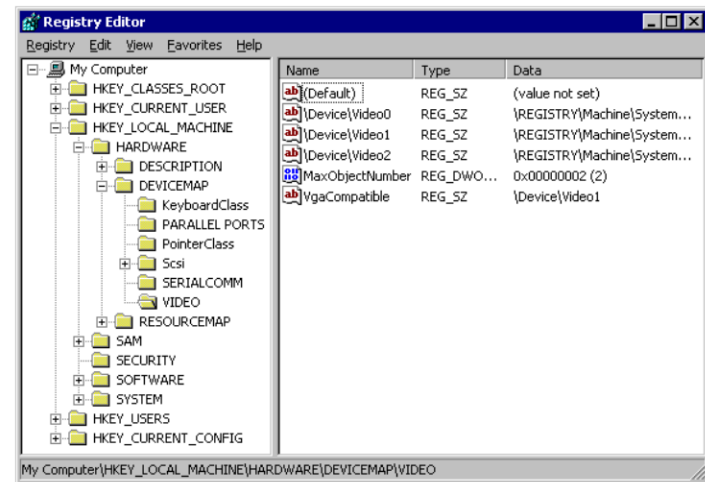


“[A] central hierarchal database used to store information that is necessary to configure the system for one or more users, applications, and hardware devices.”

Pre-Windows 2000

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

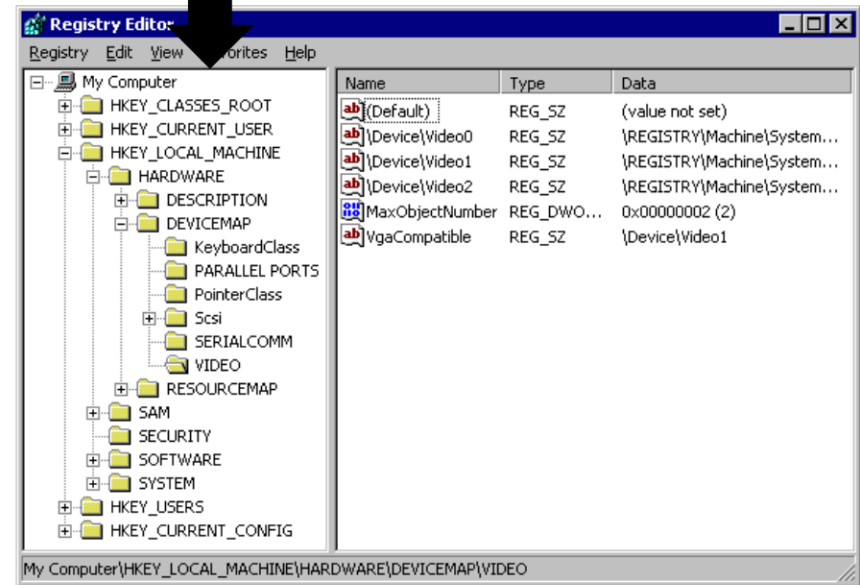
Post-Windows 2000



Windows Registry



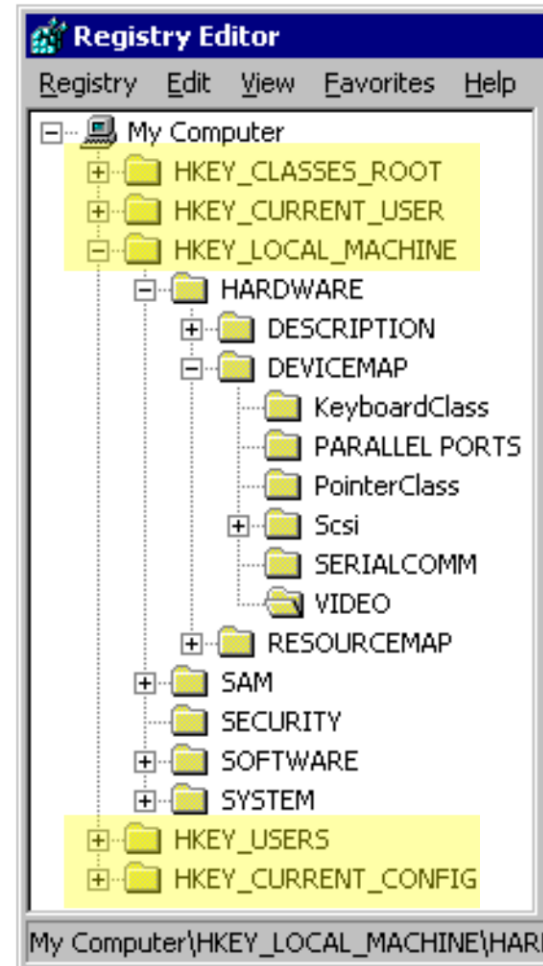
- Registry keys
 - Hold multiple “values” analogous to FS directories



Windows Registry



- “Hives”
 - Logical grouping of registry key collections



Hive Organization

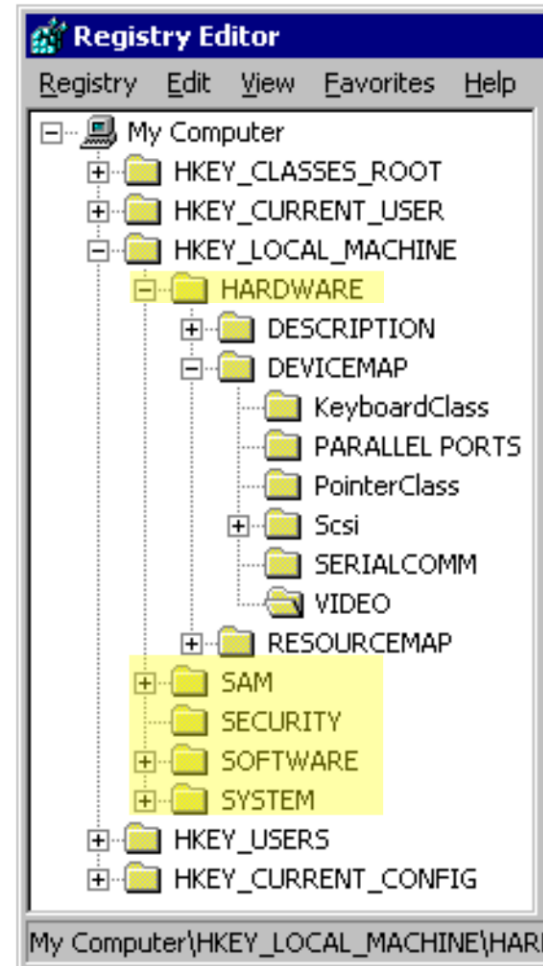


- HKEY_CLASSES_ROOT (HKCR)
 - Information related to file name extensions and Object Linking and Embedding (OLE) mappings
- HKEY_CURRENT_USER (HKCU)
 - Settings for the currently logged on user
- HKEY_USERS (HKU)
 - Information of different user settings consolidated from HKCU hive
- HKEY_LOCAL_MACHINE (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



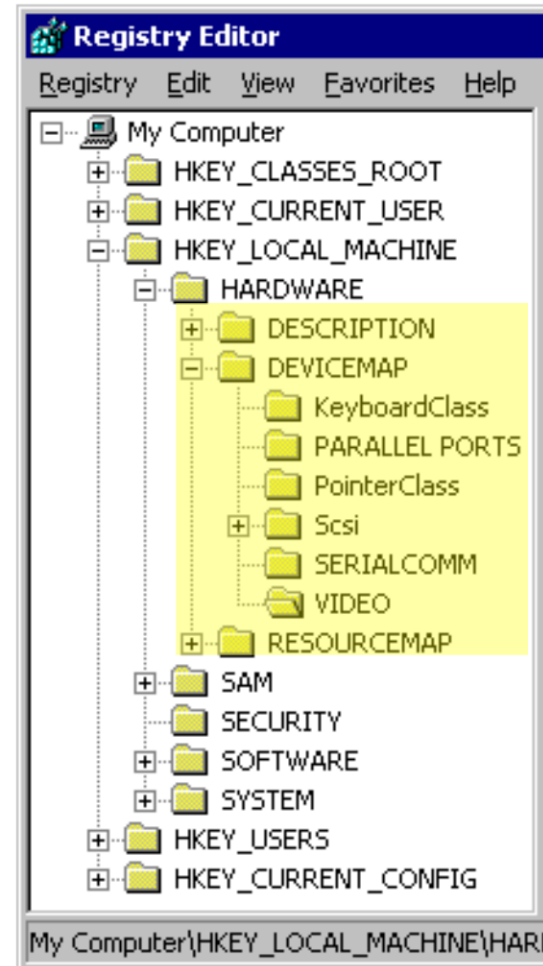
- “Hives”
 - Logical grouping of registry key collections
- “Keys”



Windows Registry



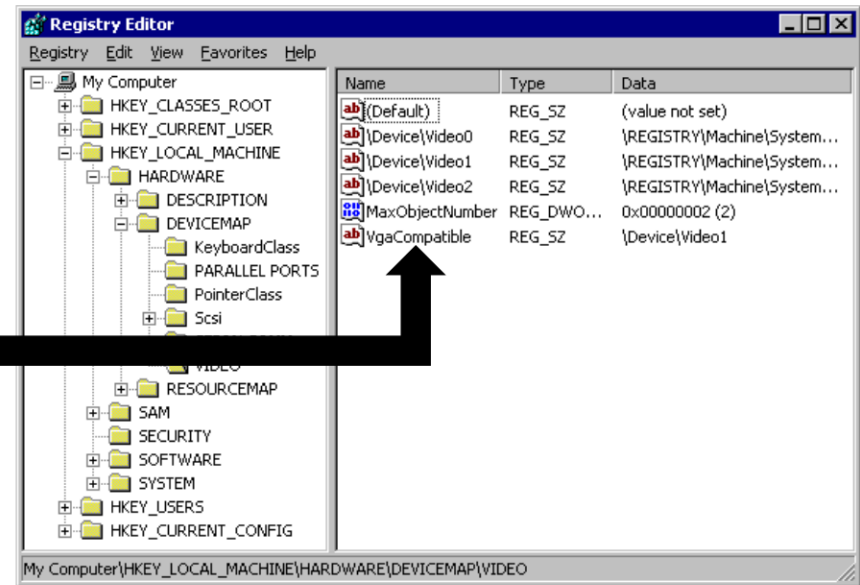
- “Hives”
 - Logical grouping of registry key collections
- “Keys”
- “Subkeys”
 - Registry keys logically nested under other registry keys



Windows Registry



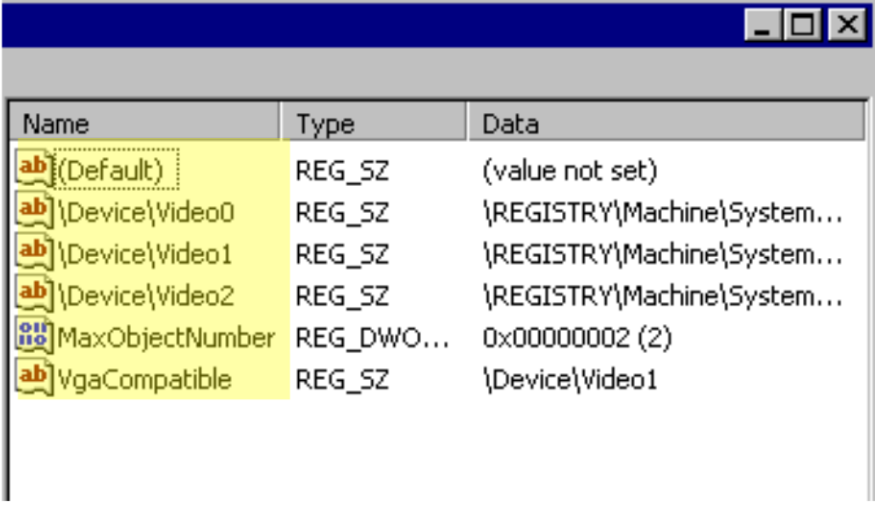
- Registry keys
 - Hold multiple “values” analogous to FS directories
- Registry values
 - Hold a single, typed configuration analogous to FS files



Windows Registry



- “Key Name”
 - Lowest referenceable tree node



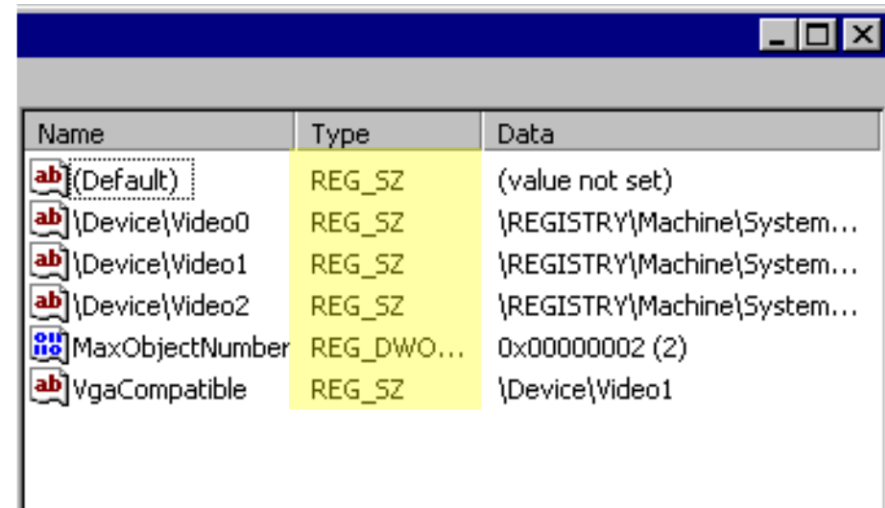
A screenshot of the Windows Registry Editor window. The window has a blue title bar with standard minimize, maximize, and close buttons. Below the title bar is a menu bar. The main area displays a list of registry values in a table format. The first row, '(Default)', is highlighted with a yellow background. Each row includes a small icon to the left of the name, the name itself, the data type, and the data value.

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



A screenshot of the Windows Registry Editor window. The window has a blue title bar and a menu bar. Below the menu bar is a tree view on the left and a list of registry values on the right. The list has three columns: Name, Type, and Data. The values are as follows:

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 level of tree node

- “Key Type”

- Indicates how data is interpreted

... / Desktop Technologies / System Services / Windows System Information /

Registry value types

Article • 02/08/2023 • 7 contributors [Feedback](#)

In this article

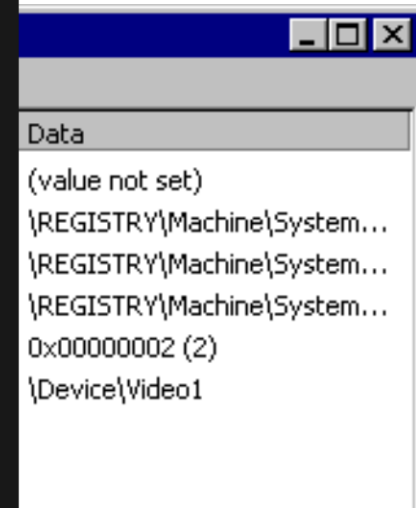
- String values
- Byte formats

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](#)

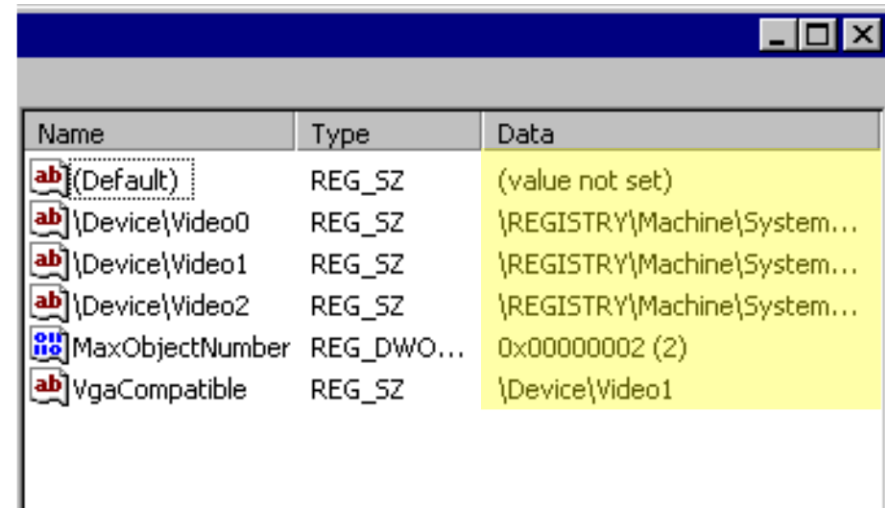
Value	Type
<code>REG_BINARY</code>	Binary data in any form.
<code>REG_DWORD</code>	A 32-bit number.
<code>REG_DWORD_LITTLE_ENDIAN</code>	A 32-bit number in little-endian format . Windows is designed to run on little-endian computer architectures. Therefore, this value is defined as <code>REG_DWORD</code>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



Windows Registry



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



A screenshot of the Windows Registry Editor window. The window has a blue title bar and a standard Windows XP-style interface. The main area displays a list of registry values in a table format. The table has three columns: 'Name', 'Type', and 'Data'. The first row is highlighted in yellow. The 'Name' column shows icons for each value: a folder icon for '(Default)', a folder icon for '\Device\Video0', a folder icon for '\Device\Video1', a folder icon for '\Device\Video2', a folder icon for 'MaxObjectNumber', and a folder icon for 'VgaCompatible'. The 'Type' column shows the registry value type: 'REG_SZ' for the first four, 'REG_DWO...' for 'MaxObjectNumber', and 'REG_SZ' for 'VgaCompatible'. The 'Data' column shows the value: '(value not set)' for '(Default)', '\REGISTRY\Machine\System...' for the video keys, '0x00000002 (2)' for 'MaxObjectNumber', and '\Device\Video1' for 'VgaCompatible'.

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



- Browsers are excellent source of info

- User
inter
- Inter
em
- Inter
only



charts,

Browser Artifacts



Browser Usage	History	Cookies	Cache	Session Restore	Flash & Super Cookies	Google Analytics Cookies
	Description: Records websites visited by date and time. Details stored for each local user account. Records number of times visited (frequency). Also tracks scores of local system files. Location: Internet Explorer -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Firefox -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Chrome -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5	Description: Cookies give insight into what websites have been visited and what activities may have taken place there. Location: Internet Explorer -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Firefox -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Chrome -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5	Description: The cache is where web page components can be stored locally to speed up subsequent visits Location: Internet Explorer -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Firefox -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Chrome -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5	Description: Automatic Crash Recovery features built into the browser Location: Internet Explorer -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Firefox -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Chrome -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5	Description: Local Stored Objects (LSOs), or Flash Cookies, have become ubiquitous on most systems due to the extremely high penetration of Flash applications across the Internet. They tend to be much more persistent because they do not expire, and there is no built-in mechanism within the browser to remove them. In fact, many sites have begun using LSOs for their tracking mechanisms because they rarely get cleared like traditional cookies. Location: Internet Explorer -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Firefox -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Chrome -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5	Description: Google Analytics (GA) has developed an extremely sophisticated methodology for tracking site visits, user activity and paid search. Since GA is largely free, it has a commanding share of the market, estimated at over 80% of sites using traffic analysis and over 50% of all sites. Location: Internet Explorer -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Firefox -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5 Chrome -C:\WINDOWS\LOCAL SETTINGS\History\History.IE5

- 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
- .tables
- Print table schema
- PRAGMA
table_info(XXXX)
- Extracting info from
table directly
- *Standard SQL*

Extracting Browser Info

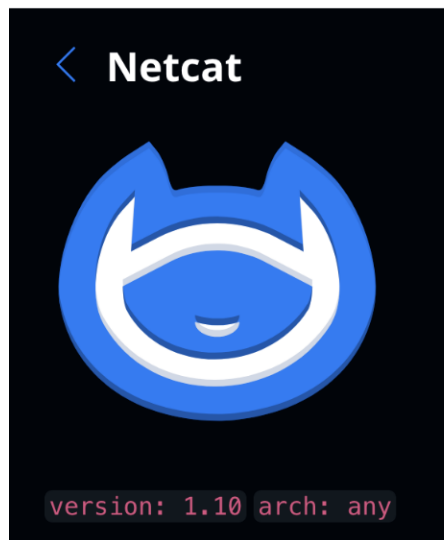


- Listing all tables
 - Print table schema
 - Extracting info from table directly
 - Dumping table data to *usable* format
- `.tables`
 - PRAGMA
table_info(XXXX)
 - ***Standard SQL***
 - sqlite3> .mode json
sqlite3> .once
out.json
sqlite3> SELECT *
from XXXX;

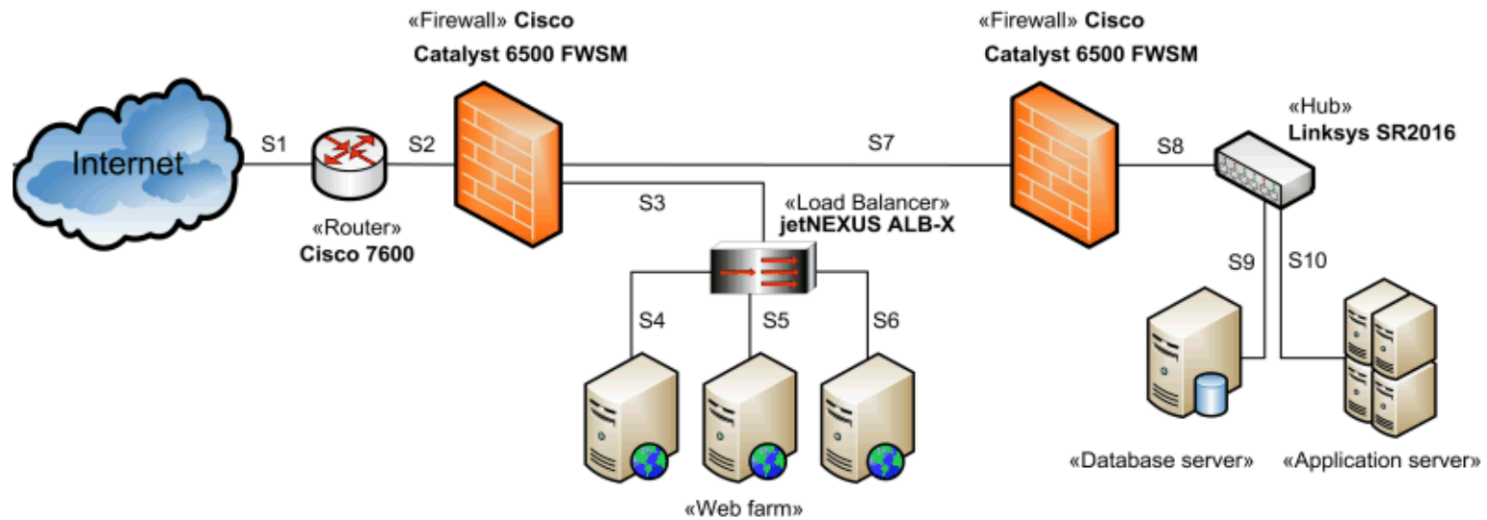
Internal Network Scanning



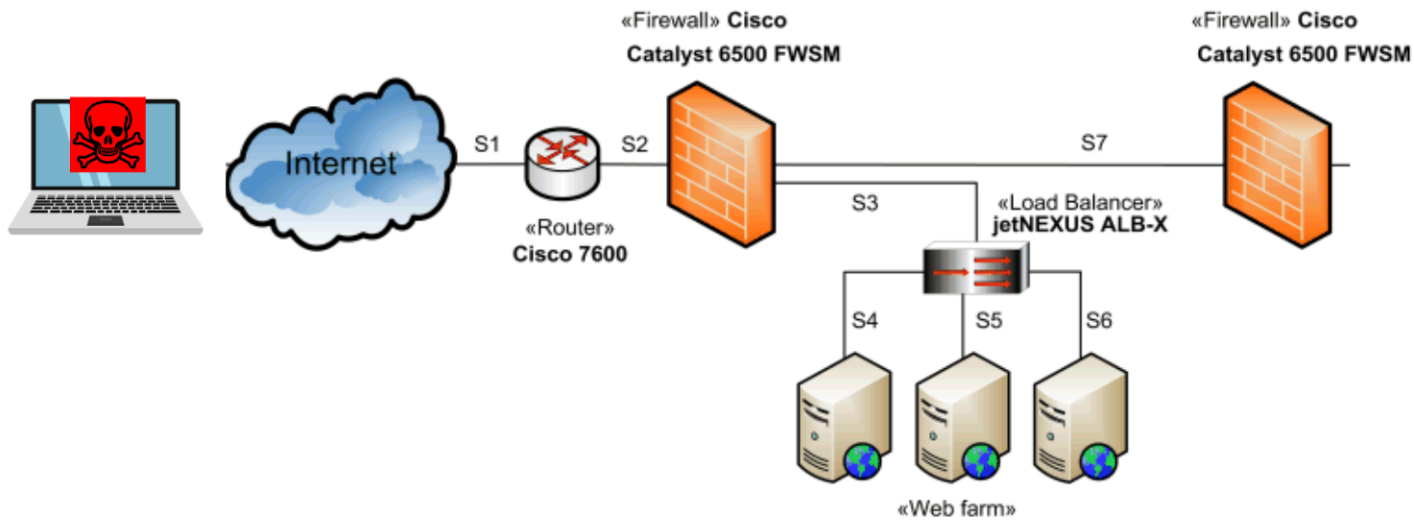
- All the same TTPs from reconnaissance but with a **different perspective.**



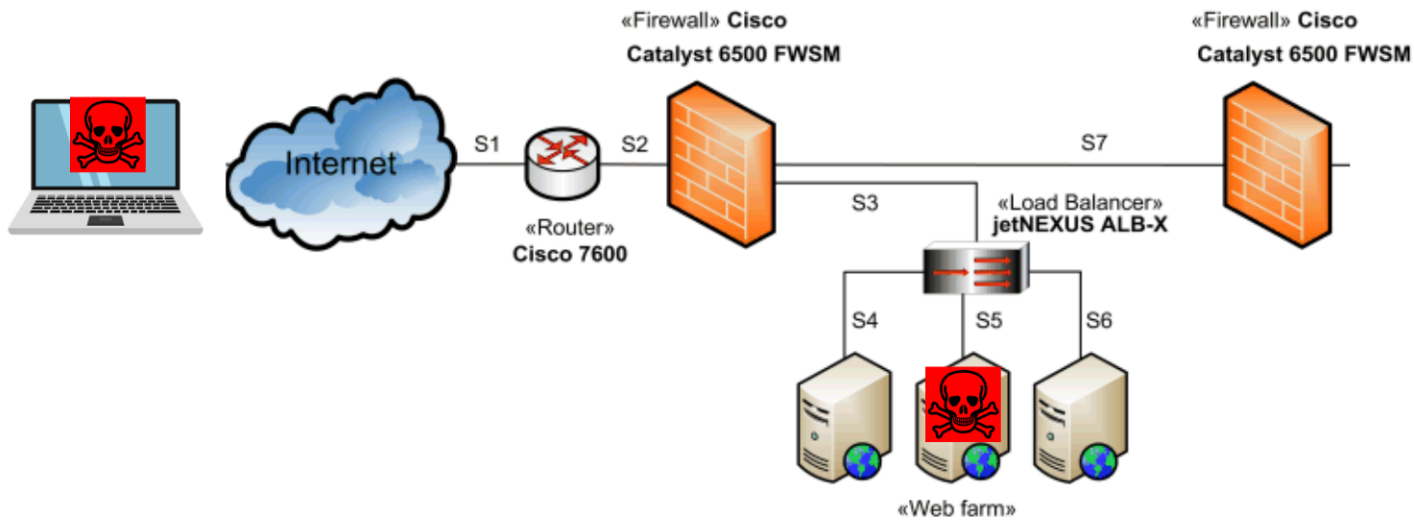
Scanning Perspective



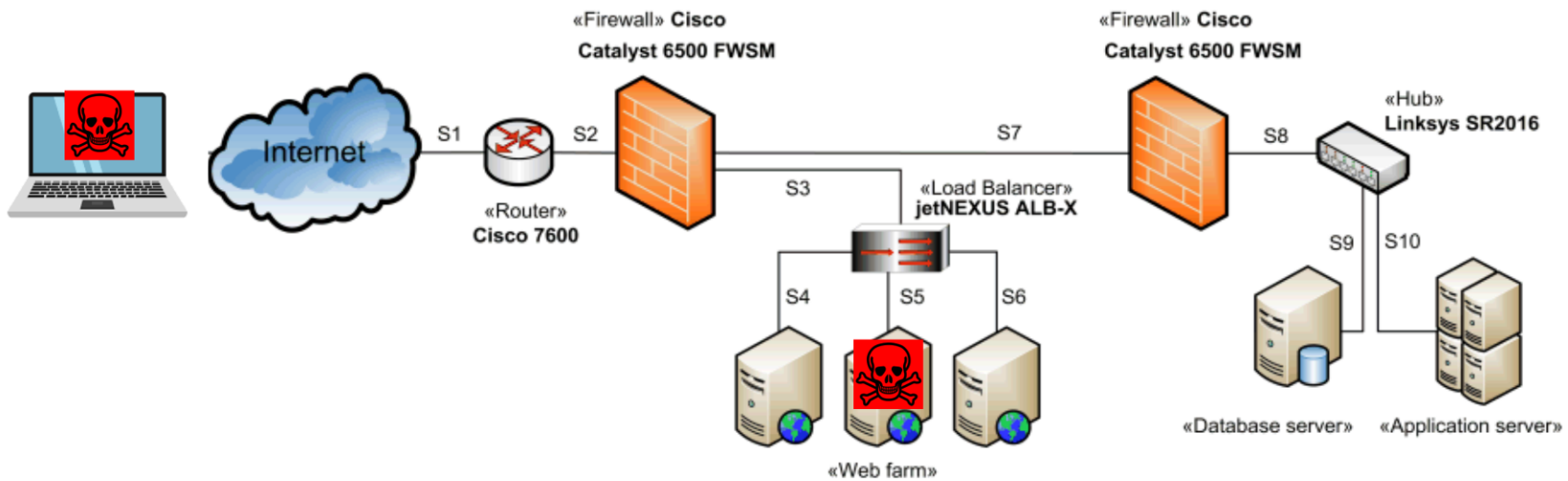
Scanning Perspective



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

