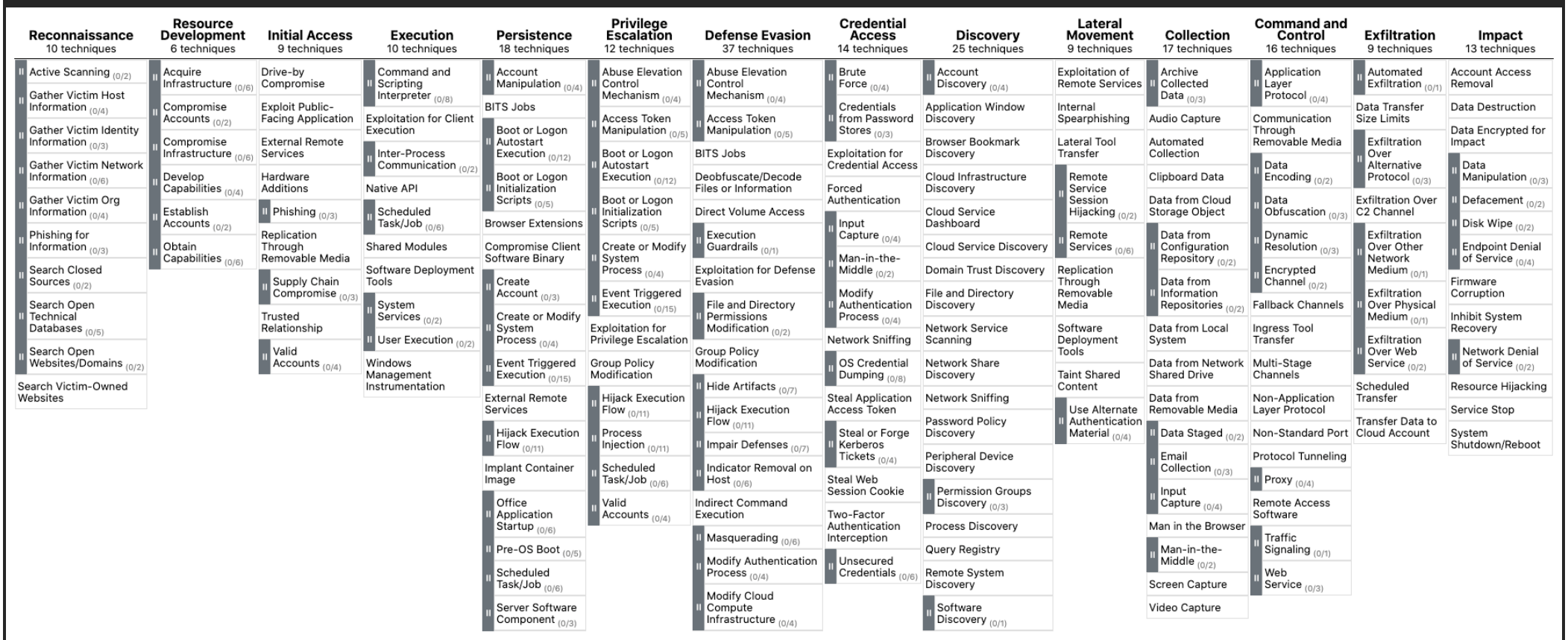
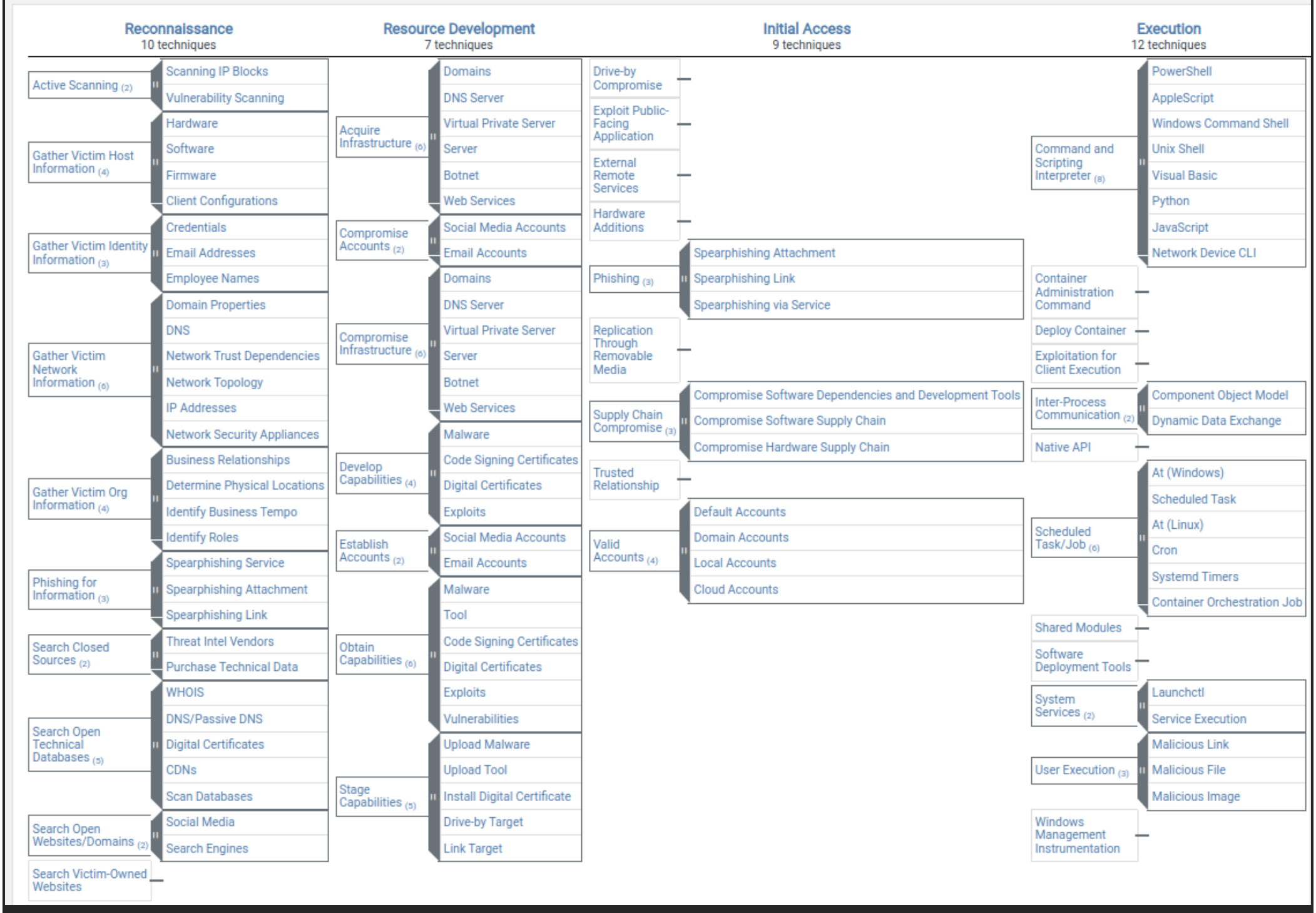
Chapter 2: Labs

Activity 2.1: Explore the ATT&CK Framework

https://attack.mitre.org/



Recon | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation



Add Office 365 Global Administrator Role
SSH Authorized Keys

BITS Jobs

Boot or Logon Autostart Execution (15)
- Registry Run Keys / Startup Folder
- Authentication Package
- Time Providers
- Winlogon Helper DLL
- Security Support Provider
- Kernel Modules and Extensions
- Re-opened Applications
- LSASS Driver
- Shortcut Modification
- Port Monitors
- Plist Modification
- Print Processors
- XDG Autostart Entries
- Active Setup
- Login Items

Boot or Logon Initialization Scripts (5)
- Logon Script (Windows)
- Logon Script (Mac)
- Network Logon Script
- RC Scripts
- Startup Items

Browser Extensions

Compromise Client Software Binary

Create Account (3)
- Local Account
- Domain Account
- Cloud Account

Create or Modify System Process (4)
- Launch Agent
- Systemd Service
- Windows Service
- Launch Daemon

Event Triggered Execution (15)
- Change Default File Association
- Screensaver
- Windows Management Instrumentation Event Subscription
- Unix Shell Configuration Modification
- Trap
- LC_LOAD_DYLIB Addition
- Netsh Helper DLL
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Image File Execution Options Injection
- PowerShell Profile
- Emond
- Component Object Model Hijacking

External Remote Services

Hijack Execution Flow (11)
- Services File Permissions Weakness
- Executable Installer File Permissions Weakness
- Services Registry Permissions Weakness
- Path Interception by Unquoted Path
- Path Interception by PATH Environment Variable
- Path Interception by Search Order Hijacking
- DLL Search Order Hijacking
- DLL Side-Loading
- Dynamic Linker Hijacking
- Dylib Hijacking
- COR_PROFILER

Implant Internal

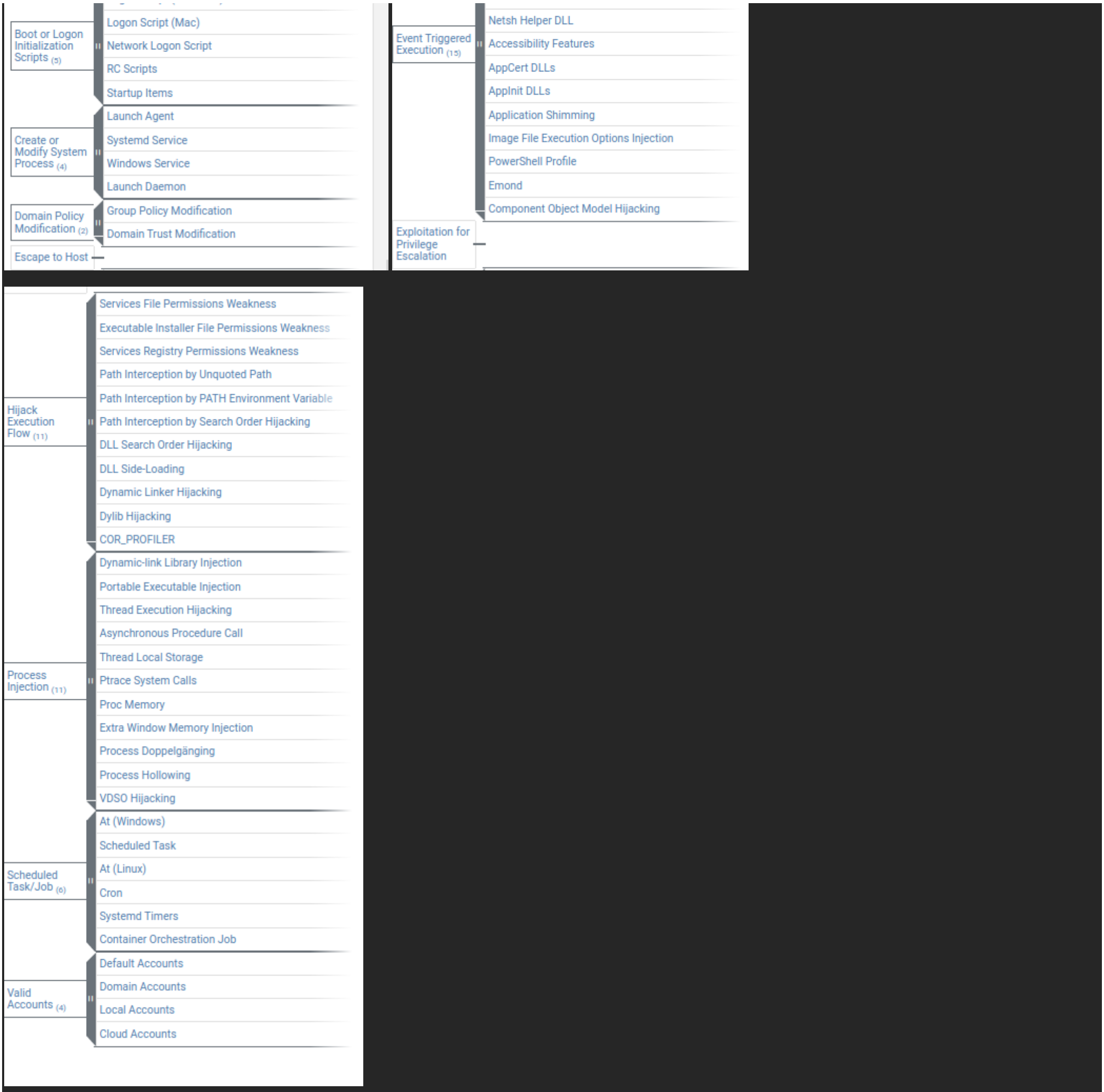
Privilege Escalation
13 techniques

Abuse Elevation Control Mechanism (4)
- Setuid and Setgid
- Bypass User Account Control
- Sudo and Sudo Caching
- Elevated Execution with Prompt

Access Token Manipulation (5)
- Token Impersonation/Theft
- Create Process with Token
- Make and Impersonate Token
- Parent PID Spoofing
- SID-History Injection

Boot or Logon Autostart Execution (15)
- Registry Run Keys / Startup Folder
- Authentication Package
- Time Providers
- Winlogon Helper DLL
- Security Support Provider
- Kernel Modules and Extensions
- Re-opened Applications
- LSASS Driver
- Shortcut Modification
- Port Monitors
- Plist Modification
- Print Processors
- XDG Autostart Entries
- Active Setup
- Login Items
- Logon Script (Windows)

Change Default File Association
Screensaver
Windows Management Instrumentation Event Subs
Unix Shell Configuration Modification
Trap
LC_LOAD_DYLIB Addition



https://edition.cnn.com/2021/06/11/cars/vw-audi-hack-customer-information/index.html

1.

What was stolen?

hit by a data breach that exposed the contact information and, in some cases, personal details, like driver license numbers, of customers in the United States and Canada.

Who is affected?

More than 3 million customers or shoppers had at least basic contact information stolen from an outside company that worked with the automakers, according VW. That data included phone numbers, email addresses, postal mailing addresses and, in some cases, vehicle identification numbers.

What is the company doing to "make it better?"

The company is offering free credit protection to those who had very sensitive information taken.

How was the data stolen?

The data, which was stolen from an outside vendor that VW and Audi and some of their dealers use, had been gathered between 2014 and 2019. The information had been collected and saved for marketing purposes, according to VW(VLKPF), and had been left in an unsecured file. VW did not name the vendor.

Part 1: Build a threat profile/Part 2: Analysis

1. List what you know about the compromise or exploit, including details about the threat actor, what occurred, what tools were used, and as many other details as you can find.

2. Review your list against the headings for the appropriate ATT&CK matrix. Do you have items that match the headings?
3. If you still lack data, you should continue your search or find another example to work through!

Insider Threat (unintentional): VW did not protect the data securely, and exposed the file to a 3rd party. The file was unsecured.
ATT&CK: Enterprise/Trusted Relationship
Mitigation: Properly manage accounts and permissions used by parties in trusted relationships to minimize potential abuse by the party and if the party is compromised by an adversary.
OR
ATT&CK: Collection/Archived Collected Data
Mitigation: Systems scans to identify unauthorized archival utilities

Activity 2.2: Set Up a STIX/TAXII Feed

user: anomali
default password: anomolistaxx
changed pw: biddion4212

Anomali's STAXX community version provides an easy way to consume STIX feeds. In this exercise, you will download and install the STAXX client, and then review the data from one of the included feeds.

1. Visit www.anomali.com/community/staxx and download the STAXX Community edition software. STAXX is a 1 GB download and requires an email to get the download link.
2. Install the STAXX client. You will need a virtualization environment like VirtualBox or VMWare to open the OVA file. Follow the Anomali setup and installation guide at update.anomali.com/staxx/docs/Anomali_STAXX_Installation_&_Administration_Guide.pdf.
3. This guide will help you get Anomali set up. When you connect to the web interface, you will need to accept the insecure connection on most major browsers.
4. When asked, use the Anomali Limo service to gather data for your first feeds.
5. Once you are in and Anomali has ingested its feeds, explore the dashboards. What is the most common indicator type? Does it match what you would expect?
6. Advanced: Identify a STIX feed that isn't part of the STAXX default feed list and add it to STAXX.