Reconnaissance Vulnerability	Gather Victim Organization Information
Reconnaissance Vulnerability	Phishing for Information
Reconnaissance Vulnerability	Search Closed Sources
Reconnaissance Vulnerability	Search Open Technical Databases

Reconnaissance Vulnerability	Active Scanning
Reconnaissance Vulnerability	Gather Victim Host Information
Reconnaissance Vulnerability	Gather Victim Identity Information
Reconnaissance Vulnerability	Gather Victim Network Information

Reconnaissance Vulnerability

Reconnaissance Vulnerability

Search Open Websites/Domains

Search Victim-Owned Websites

Initial Access Vulnerability

Hardware Additions

Initial Access Vulnerability

Phishing

Initial Access Vulnerability

Replication Through Removable Media

Initial Access Vulnerability

Supply Chain Compromise

Initial Access Vulnerability

Content Injection

Initial Access Vulnerability

Drive-by Compromise

Initial Access Vulnerability

Exploit Public-Facing Application

Initial Access Vulnerability

External Remote Services

Initial Access Vulnerability

Container Administration Command

Initial Access Vulnerability

Exploitation for Client Execution

Execution Vulnerability

Inter-Process Communication

Execution Vulnerability

Native API

Execution Vulnerability

Trusted Relationship

Execution Vulnerability

Valid Accounts

Execution Vulnerability

Cloud Administration Command

Execution Vulnerability

Command and Scripting Interpreter

Execution Vulnerability

System Services

Execution Vulnerability

User Execution

Execution Vulnerability

Windows Management Instrumentation

Execution Vulnerability

Account Manipulation

Execution Vulnerability

Schedule Task/Job

Execution Vulnerability

Serverless Execution

Execution Vulnerability

Shared Modules

Persistence Vulnerability

Software Deployment Tools

Persistence Vulnerability

Client Software Binary

Persistence Vulnerability

Create Account

Persistence Vulnerability

Create/Modify System Process

Persistence Vulnerability

Event Triggered Execution

Persistence Vulnerability

BITS Jobs

Persistence Vulnerability

Boot or Logon Autostart Execution

Persistence Vulnerability

Boot or Logon Initialization Scripts

Persistence Vulnerability

Browser Extensions

Persistence Vulnerability

Office Application Startup

Persistence Vulnerability

Power Settings

Persistence Vulnerability

Pre-OS Boot

Persistence Vulnerability

Scheduled Task/Job

Persistence Vulnerability	External Remote Services
Persistence Vulnerability	Hijack Execution Flow
Persistence Vulnerability	Implant Internal Image
Persistence Vulnerability	Modify Authentication Process

Persistence Vulnerability

Access Token Manipulation

Persistence Vulnerability

Account Manipulation

Persistence Vulnerability

Boot or Logon Autostart Execution

Privilege Escalation Vulnerability

Boot or Logon Initialization Scripts

Privilege Escalation Vulnerability

Server Software Component

Privilege Escalation Vulnerability

Traffic Signaling

Privilege Escalation Vulnerability

Valid Accounts

Privilege Escalation Vulnerability

Elevation Control Mechanism

Privilege Escalation Vulnerability

Exploitation for Privilege Escalation

Privilege Escalation Vulnerability

Hijack Execution Flow

Privilege Escalation Vulnerability

Process Injection

Privilege Escalation Vulnerability

Scheduled Task/Job

Privilege Escalation Vulnerability

Create/Modify System Process

Privilege Escalation Vulnerability

Domain Policy Modification

Privilege Escalation Vulnerability

Escape to Host

Privilege Escalation Vulnerability

Event Triggered Execution

Privilege Escalation Vulnerability

Build Image on Host

Defense Evasion Vulnerability

Debugger Evasion

Defense Evasion Vulnerability

Deobfuscate/Decode Files or information

Defense Evasion Vulnerability

Deploy Container

Defense Evasion Vulnerability

Valid Accounts

Defense Evasion Vulnerability

Abuse Elevation Control Mechanism

Defense Evasion Vulnerability

Access Token Manipulation

Defense Evasion Vulnerability

BITS Jobs

Defense Evasion Vulnerability

File and Directory Permissions Modification

Defense Evasion Vulnerability

Hide Artifacts

Defense Evasion Vulnerability

Hijack Execution Flow

Defense Evasion Vulnerability

Impair Defenses

Defense Evasion Vulnerability

Direct Volume Access

Defense Evasion Vulnerability

Domain Policy Modification

Defense Evasion Vulnerability

Execution Guardrails

Defense Evasion Vulnerability

Exploitation for Defense Evasion

Defense Evasion Vulnerability

Modify Authentication Process

Defense Evasion Vulnerability

Modify Cloud Compute Infrastructure

Defense Evasion Vulnerability

Modify Registry

Defense Evasion Vulnerability

Modify System Image

Defense Evasion Vulnerability

Impersonation

Defense Evasion Vulnerability

Indicator Removal

Defense Evasion Vulnerability

Indirect Command Execution

Defense Evasion Vulnerability

Masquerading

Defense Evasion Vulnerability

Process Injection

Defense Evasion Vulnerability

Reflective Code Loading

Defense Evasion Vulnerability

Rogue Domain Controller

Defense Evasion Vulnerability

Rootkit

Defense Evasion Vulnerability

Network Boundary Bridging

Defense Evasion Vulnerability

Obfuscated Files/Information

Defense Evasion Vulnerability

Plist File Modification

Defense Evasion Vulnerability

Pre-OS Boot

Defense Evasion Vulnerability

Traffic Signaling

Defense Evasion Vulnerability

Trusted Developer Utilities Proxy Execution

Defense Evasion Vulnerability

Unused/Unsupported Cloud Regions

Defense Evasion Vulnerability

Use Alternate Authentication Material

Defense Evasion Vulnerability

Subvert Trust Controls

Defense Evasion Vulnerability

System Binary Proxy Execution

Defense Evasion Vulnerability

System Script Proxy Execution

Defense Evasion Vulnerability

Template Injection

Defense Evasion Vulnerability

Adversary-in-the-Middle

Defense Evasion Vulnerability

Brute Force

Defense Evasion Vulnerability

Credentials from Password Stores

Defense Evasion Vulnerability

Exploitation for Credentials Access

Credential Access Vulnerability

Valid Accounts

Credential Access Vulnerability

Virtualization/Sandbox Evasion

Credential Access Vulnerability

Weaken Encryption

Credential Access Vulnerability

XSL Script Processing

Credential Access Vulnerability

Multi-Factor Authentication Interception

Credential Access Vulnerability

Multi-Factor Authentication Request Generation

Credential Access Vulnerability

Network Sniffing

Credential Access Vulnerability

OS Credentials Dumping

Credential Access Vulnerability

Forced Authentication

Credential Access Vulnerability

Forge Web Credentials

Credential Access Vulnerability

Input Capture

Credential Access Vulnerability

Modify Authentication Process

Credential Access Vulnerability

Unsecured Credentials

Credential Access Vulnerability

Account Discovery

Credential Access Vulnerability

Application Window Discovery

Credential Access Vulnerability

Browser Information Discovery

Credential Access Vulnerability

Steal Application Access Token

Discovery Vulnerability

Steal/Forge Authentication Certificates

Discovery Vulnerability

Steal/Forge Kerberos Tickets

Discovery Vulnerability

Steal Web Session Cookie

Discovery Vulnerability

Container and Resource Discovery

Discovery Vulnerability

Debugger Evasion

Discovery Vulnerability

Device Driver Discovery

Discovery Vulnerability

Domain Trust Discovery

Discovery Vulnerability

Cloud Infrastructure Discovery

Discovery Vulnerability

Cloud Service Dashboard

Discovery Vulnerability

Cloud Service Discovery

Discovery Vulnerability

Cloud Storage Object Discovery

Discovery
Vulnerability

Network
Share
Discovery

Discovery
Vulnerability

Network
Sniffing

Discovery
Vulnerability

Password
Policy
Discovery

Discovery
Vulnerability

Peripheral
Device
Discovery

Discovery Vulnerability

File and Directory Discovery

Discovery Vulnerability

Group Policy Discovery

Discovery Vulnerability

Log Enumeration

Discovery Vulnerability

Network Service Discovery

Discovery
Vulnerability

Software
Discovery

Discovery
Vulnerability

System
Information
Discovery

Discovery
Vulnerability

System
Location
Discovery

Discovery
Vulnerability

System
Network
Configurations
Discovery

Discovery
Vulnerability

Permission
Groups
Discovery

Discovery
Vulnerability

Process
Discovery

Discovery
Vulnerability

Query
Registry

Discovery
Vulnerability

Remote
System
Discovery

Discovery Vulnerability

Virtualization/Sandbox Evasion

Discovery Vulnerability

Exploitation of Remote Services

Discovery Vulnerability

Internal Spearphishing

Discovery Vulnerability

Lateral Tool Transfer

Discovery Vulnerability

System Network Connections Discovery

Lateral Movement Vulnerability

System Owner/User Discovery

Lateral Movement Vulnerability

System Service Discovery

Lateral Movement Vulnerability

System Time Discovery

Lateral Movement Vulnerability

Taint Shared Content

Lateral Movement Vulnerability

Use Alternate Authentication Material

Lateral Movement Vulnerability

Adversary-in-the-middle

Lateral Movement Vulnerability

Archive Collected Data

Lateral Movement Vulnerability

Remote Service Session Hijacking

Lateral Movement Vulnerability

Remote Services

Collection Vulnerability

Replication Through Removable Media

Collection Vulnerability

Software Deployment Tools

Collection Vulnerability

Data from Cloud Storage

Collection Vulnerability

Data from Configuration Repository

Collection Vulnerability

Data from Information Repositories

Collection Vulnerability

Data from Local System

Collection Vulnerability

Audio Capture

Collection Vulnerability

Automated Collection

Collection Vulnerability

Browser Session Hijacking

Collection Vulnerability

Clipboard Data

Collection Vulnerability

Input Capture

Collection Vulnerability

Screen Capture

Collection Vulnerability

Video Capture

Collection Vulnerability

Application Layer Protocol

Collection Vulnerability

Data from Network Shared Drive

Collection Vulnerability

Data from Removable Media

Collection Vulnerability

Data Staged

Command and Control Vulnerability

Email Collection

Command and Control Vulnerability

Dynamic Resolution

Command and Control Vulnerability

Encrypted Channel

Command and Control Vulnerability

Fallback Channels

Command and Control Vulnerability

Ingress Tool Transfer

Command and Control Vulnerability

Communication Through Removable Media

Command and Control Vulnerability

Content Injection

Command and Control Vulnerability

Data Encoding

Command and Control Vulnerability

Data Obfuscation

Command and Control Vulnerability	Proxy
Command and Control Vulnerability	Remote Access Service
Command and Control Vulnerability	Traffic Signaling
Command and Control Vulnerability	Web Service

Command and Control Vulnerability

Multi-Stage Channels

Command and Control Vulnerability

Non-Application Layer Protocol

Command and Control Vulnerability

Non-Standard Port

Command and Control Vulnerability

Protocol Tunneling

Exfiltration Vulnerability

Exfiltration Over Other Network Medium

Exfiltration Vulnerability

Exfiltration Over Physical Medium

Exfiltration Vulnerability

Exfiltration Over Web Service

Exfiltration Vulnerability

Scheduled Transfer

Exfiltration Vulnerability

Automated Exfiltration

Exfiltration Vulnerability

Data Transfer Size Limits

Exfiltration Vulnerability

Exfiltration Over Alternative Protocol

Exfiltration Vulnerability

Exfiltration Over Channel

Exfiltration Vulnerability

Data Manipulation

Impact Vulnerability

Defacement

Impact Vulnerability

Disk Wipe

Impact Vulnerability

Endpoint Denial of Service

Impact Vulnerability

Transfer Data to Cloud Account

Impact Vulnerability

Account Access Removal

Impact Vulnerability

Data Destruction

Impact Vulnerability

Data Encrypted for Impact

Impact Vulnerability

Resource Hijacking

Impact Vulnerability

Service Stop

Impact Vulnerability

System Shutdown/Reboot

Impact Vulnerability

Impact Vulnerability

Financial Theft

Impact Vulnerability

Firmware Corruption

Impact Vulnerability

Inhibit System Recovery

Network Denial of Service