

Candor Protect Product Capabilities

April 2022



Candor Penetration Testing Types

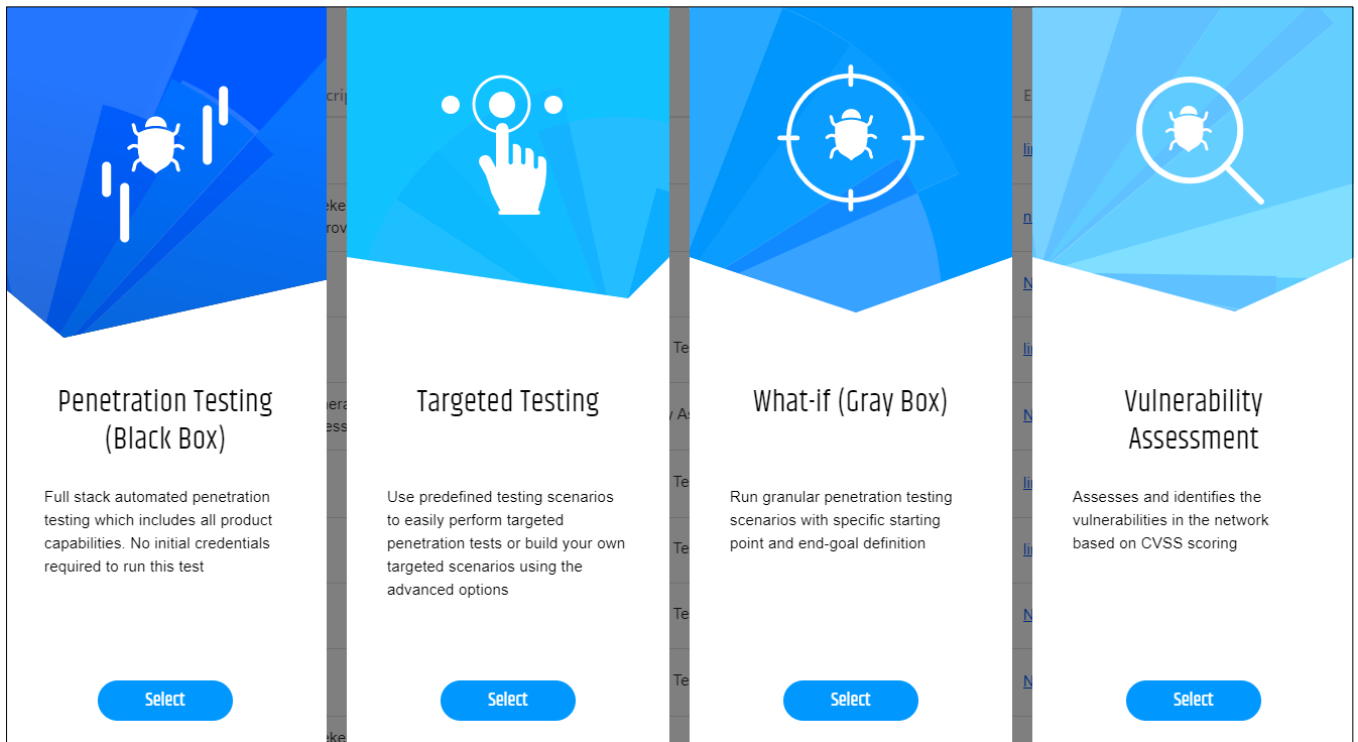
Penetration Testing (Black Box) – Full stack automated penetration testing which includes all product capabilities. No initial credentials required to run this test.





Targeted Testing – Use predefined testing scenarios to easily perform targeted penetration tests or build your own targeted scenarios using the advanced options:

AD Password Strength Assessment – The Active Directory Password Strength Assessment targeted Testing Scenario is used to evaluate the actual password strength of your entire user directory. This Testing Scenario uses a privileged user account to dump the entire password database and perform an offline password cracking test using Candor's advanced built-in cracking engine(s). This will help you flag accounts with passwords that adhere to your policy, but can still be easily cracked by hackers.

What-if (Gray Box) – Run granular penetration testing scenarios with specific starting point and end-goal definition.

Vulnerability Assessment – Assesses and identifies the vulnerabilities in the network based on CVSS¹ scoring.



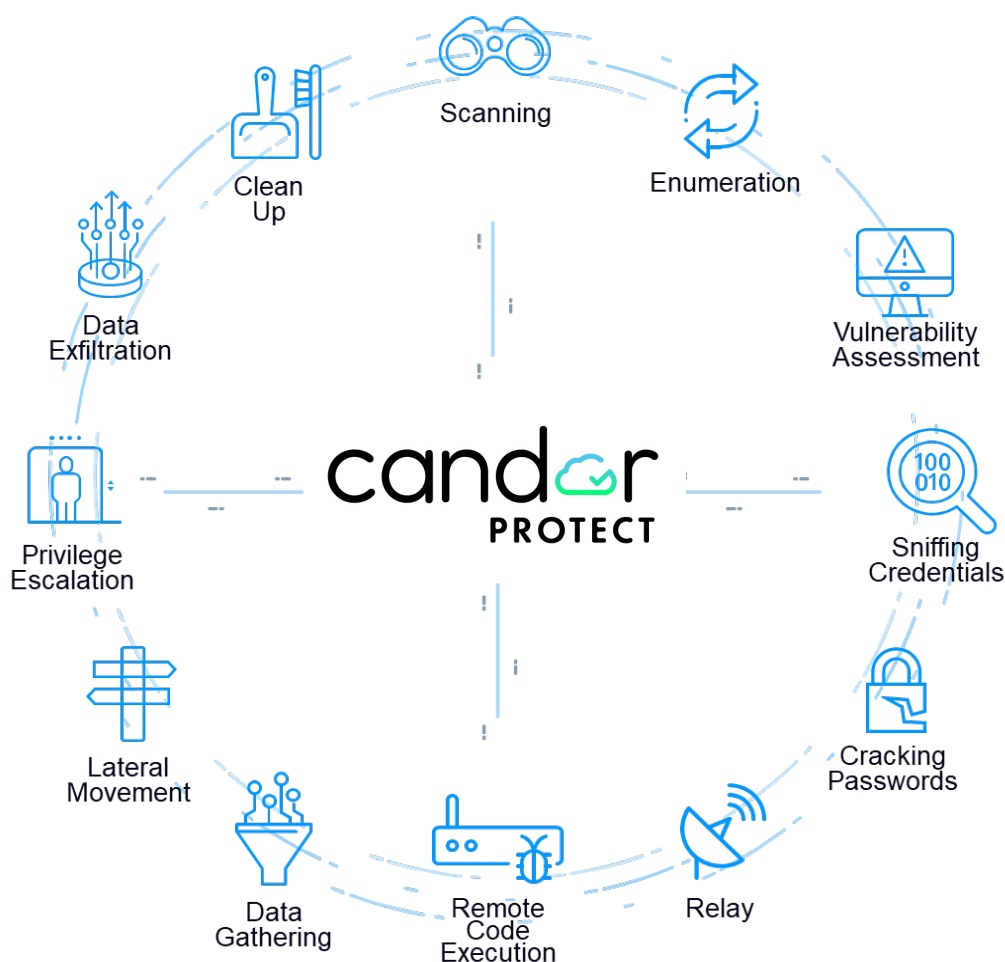
Penetration Testing (Black Box)	Targeted Testing	What-if (Gray Box)	Vulnerability Assessment
			
Penetration Testing (Black Box)	Targeted Testing	What-if (Gray Box)	Vulnerability Assessment
Full stack automated penetration testing which includes all product capabilities. No initial credentials required to run this test	Use predefined testing scenarios to easily perform targeted penetration tests or build your own targeted scenarios using the advanced options	Run granular penetration testing scenarios with specific starting point and end-goal definition	Assesses and identifies the vulnerabilities in the network based on CVSS scoring
Select	Select	Select	Select

¹ <https://www.first.org/cvss/>

Attack Phases

Within each penetration test, Candor executes multiple dynamic attack phases against the target network segment(s). The test starts with Reconnaissance (Scanning, Enumeration, Vulnerability scan), mapping the attack surface. Based on the findings Candor will start to dynamically exploit the network with a focus on the identified vulnerabilities. Each attack step is analyzed and the results can be used to continue the test across the network and expand the attack surface. Candor will sniff credentials, try to crack passwords, and use valid credentials with privileged access. It will continue Discovery across the network to target the test. It will start Lateral Movement, run Exploitation and Post-Exploitations actions, try to bypass EDR/ NGAV solutions to validate their effectiveness. The image below demonstrates the testing stages and dynamic nature of the test adjusting and progressing the test based on the target network attack surface. In the final stage, a full clean-up and sanitation of the target network – safety is key.

The following pages will detail each attack phase by specifying examples of offensive tactics and techniques and their relations to the MITRE ATT&CK2 framework for the Enterprise.

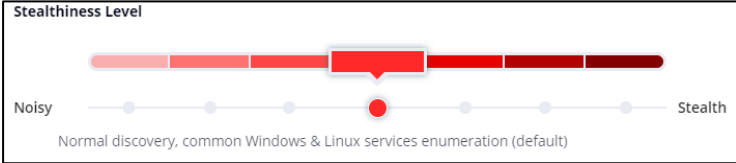


² <https://attack.mitre.org/>

Attack Phases Overview

Attack Phase	Description
<u>Scanning</u>	Probing a given network by identifying active IP addresses, ports and topology details and discovery of all related hosts, servers and devices
<u>Enumeration</u>	Extract machine data, user data, hostnames, network resources/shares, file system and other services by creating an active connection to a given system
<u>Vulnerability Assessment</u>	Scanning the active hosts for known vulnerabilities
<u>Sniffing Credentials</u>	Interception of network traffic and host related data to extract users' credentials with focus on privileged users including AD domain accounts, local accounts
<u>Passwords Cracking</u>	Use multiple measures to recover plaintext passwords of users, hosts and servers by cracking passwords hashes from data stored in, or transported from, a system using a combination of brute-force and dictionary techniques
<u>Relay</u>	Intercept communications between two parties and relaying the data to another (third party) device including MITM network-based techniques
<u>Remote Code Execution (RCE)</u>	Utilize multiple methods for remote code execution on a given system by using defense evasion capabilities to bypass AV/EDR detection mechanisms and open a C&C channel to control the attack on the targeted device
<u>Data Gathering</u>	Gather additional data from the endpoint including security products, network access details, domain/ local credentials, browser credentials/history, Security Account Manager (SAM) file and access to cloud/on-premise critical services and apps
<u>Lateral Movement</u>	Manage a dedicated extraction procedure of authentication material to be able to pivot laterally to new endpoints across the network
<u>Privilege Escalation</u>	Remote and local capabilities to escalate from non-privileged user to being able to execute code with high permissions
<u>Data Exfiltration</u>	Data transfer from a targeted endpoint triggered by takeover of a device
<u>Cleanup</u>	Cleanup of attack created residues

1. Scanning

Description	
<p>Probing a given network by identifying active IP addresses, ports and topology details and discovery of all related hosts, servers and devices</p>	
Measures Examples	MITRE ATT&CK Related TTPs
<ul style="list-style-type: none"> ▪ Discover live hosts using variants of the ARP protocol to achieve maximal stealthiness ▪ Leverage L3 protocols to cross boundaries to new network segments by using variant of ICMP specifications, SCTP and multicast protocols ▪ Discover active devices based on common applications and their response analysis ▪ Harness broadcast and multicast protocols to trigger response from neighbor endpoints ▪ Candor allows controlling the “Stealthiness” level settings of each testing scenario in order to define the noisiness and aggression of the penetration test  <p>The diagram shows a horizontal slider labeled 'Stealthiness Level'. The left end is labeled 'Noisy' and the right end is labeled 'Stealth'. A red bar above the slider indicates the range of possible settings. A red dot on the slider is positioned at approximately the 40% mark from the left, with a white arrow pointing to it. Below the slider, the text reads: 'Normal discovery, common Windows & Linux services enumeration (default)'.</p>	<p>Active Scanning (T1595), Gather Victim Network Information (T1590), Network Sniffing (T1040), Account Discovery (T1087), Domain Trust Discovery (T1482), Network Service Scanning (T1046), Network Share Discovery (T1135), Password Policy Discovery (T1201), Permission Groups Discovery (T1069), Remote System Discovery (T1018), System Information Discovery (T1082), System Network Configuration Discovery (T1016), System Network Connections Discovery (T1049)</p>

2. Enumeration

Description	
<p>Extract machine data, user data, hostnames, network resources/shares, file system and other services by creating an active connection to a given system</p>	
Measures Examples	MITRE ATT&CK Related TTPs
<ul style="list-style-type: none"> ▪ Web server response analysis to discover underlying technology as – WordPress, Joomla, ASP ▪ Create heat map for prioritization according to common operating systems discovered in this phase ▪ Compare between anonymous enumeration to authenticated enumeration to understand underlying misconfiguration ▪ Mark and identify peripheral devices ▪ Discover specific roles of network servers as DHCP, DNS, Web, Domain controller, Database, Terminal services servers 	<p>Gather Victim Host Information (T1592), Gather Victim Identity Information (T1589), External Remote Services (T1133), Valid Accounts (T1078), Credentials from Password Stores:(T1555), OS Credential Dumping (T1003), Account Discovery (T1087), Cloud Infrastructure Discovery (T1580), Cloud Service Discovery (T1526), Domain Trust Discovery (T1482), File and Directory Discovery (T1083), Permission Groups Discovery (T1069), Process Discovery (T1057), System Information Discovery (T1082), System Owner/User Discovery (T1033), System Service Discovery (T1007), Data from Local System (T1005)</p>

3. Vulnerability Assessment

Description	
Scanning the active hosts for known vulnerabilities	
Measures Examples	MITRE ATT&CK Related TTPs
<ul style="list-style-type: none"> ▪ Discover static vulnerabilities based on network traffic fingerprinting ▪ Discover dynamic vulnerabilities by chaining several attack scenarios combined with the human factor interaction ▪ Use various remote code execution channels to conduct authenticated vulnerability discoveries 	<p>Active Scanning: Vulnerability Scanning (T1595.002), Exploit Public-Facing Application (T1190), Exploitation of Remote Services (T1210)</p>

4. Sniffing Credentials

Description	
Interception of network traffic and host related data to discover users' credentials with focus on privileged users including AD domain accounts, local accounts	
Measures Examples	MITRE ATT&CK Related TTPs
<ul style="list-style-type: none"> ▪ Passively capture network traffic to discover credentials. ▪ For more proactive scenarios, use Candor hosted servers for common network protocols to create forced authentication scenarios over SMB, RDP, HTTP, LDAP, MSSQL and more. 	Brute Force: Credential Stuffing (T1110.004), Credentials from Password Stores (T1555), Forced Authentication (T1187), Network Sniffing (T1040), Input Capture (T1056), Password Policy Discovery (T1201)

5. Passwords Cracking

Description	
<p>Use multiple measures to recover plaintext passwords of users, hosts and servers by cracking passwords hashes from data stored in, or transported from, a system using a combination of brute-force and dictionary techniques</p>	
Measures Examples	MITRE ATT&CK Related TTPs
<ul style="list-style-type: none"> ▪ Use of default manufacturer password on peripheral devices ▪ Validate existence of weak passwords ▪ Check robustness of more complex passwords and test if they adhere to the corporate's policy ▪ Use hardware based cracking capabilities to detect flaws in the Kerberos ecosystem ▪ Test privileged accounts password strength on unmanaged endpoints ▪ Harness specialized GPU computing power for high performance cracking techniques 	<p>Brute Force: Password Guessing (T1110.001), Brute Force: Password Cracking (T1110.002), Brute Force: Password Spraying (T1110.003), Brute Force: Credential Stuffing (T1110.004), Valid Accounts: Default Accounts (T1078.001), Valid Accounts: Domain Accounts (T1078.002), Valid Accounts: Local Accounts (T1078.003), Password Policy Discovery (T1201)</p>

6. Relay

Description	
Intercept communications between two parties and relaying the data to another (third party) device including MITM network-based techniques	
Measures Examples	MITRE ATT&CK Related TTPs
<ul style="list-style-type: none"> ▪ Abuse common Windows authentication protocols to relay credentials over SMB/RDP/LDAP/RPC/HTTP ▪ Conduct ARP poisoning to intercept cleartext credentials over common protocols ▪ Abuse DHCP protocol to conduct MITM attacks for intercepting cleartext credentials over common protocols and perform Relay attacks 	<p>Valid Accounts (T1078), Brute Force: Credential Stuffing (T1110.004), Forced Authentication (T1187), Man-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001), Man-in-the-Middle: ARP Cache Poisoning (T1557.002), Modify Authentication Process: Password Filter DLL (T1556.002), Domain Trust Discovery (T1482), Use Alternate Authentication Material (T1550)</p>

7. Remote Code Execution (RCE)

Description	
<p>Utilize multiple methods for remote code execution on a given system by using defense evasion capabilities to bypass AVs/EDRs detection mechanisms and open C&C channel to control the attack on the targeted device</p>	
Measures Examples	MITRE ATT&CK Related TTPs
<ul style="list-style-type: none"> ▪ Open remote execution channels through known management protocols - SMB/WMI/WINRM/SSH/ RDP ▪ Utilize exploitation to run code in an unauthenticated manner ▪ Deploy various payload types – SH/EXE/DLL/PS1/HTA ▪ Test your EDR and AV detection capabilities by generating payloads with a vary degree of forensic evasiveness ▪ Test reactiveness of the endpoints protections to stagefull and/or stageless payloads 	<p>Command and Scripting Interpreter (T1059), Exploitation for Client Execution (T1203), Inter-Process Communication (T1559), Native API (T1106), Scheduled Task/Job (T1053), System Services (T1569), Windows Management Instrumentation (T1047), BITS Jobs (T1197), Create Account (T1136.), Create or Modify System Process (T1543), Hijack Execution Flow (T1574), Valid Accounts (T1078), Access Token Manipulation (T1134), De-obfuscate/Decode Files or Information (T1140), Direct Volume Access (T1006), Exploitation for Defense Evasion (T1211), Group Policy Modification (T1484), Hide Artifacts (T1564), Indirect Command Execution (T1202), Masquerading (T1036), Modify Authentication Process (T1556), Modify Registry (T1112), Network Boundary Bridging (T1599), Obfuscated Files or Information (T1027), Process Injection (T1055), Rogue Domain Controller (T1207), Signed Binary Proxy Execution (T1218), Trusted Developer Utilities Proxy Execution (T1127), Use Alternate Authentication Material (T1550), Valid Accounts (T1078), XSL Script Processing (T1220), Credentials from Password Stores (T1555), Exploitation for Credential Access (T1212), Application Layer Protocol (T1071), Data Encoding (T1132), Data Obfuscation (T1001), Dynamic Resolution (T1568), Encrypted Channel (T1573), Fallback Channels (T1008), Ingress Tool Transfer (T1105), Multi-Stage Channels (T1104), Non-Application Layer Protocol (T1095), Non-Standard Port (T1571), Protocol Tunneling (T1572), Proxy (T1090)</p>

8. Data Gathering

Description	
<p>Gather additional data from the endpoint including security products, network access details, domain/ local credentials, browser credentials/history, Security Account Manager (SAM) file and access to cloud/on-premise critical services and apps</p>	
Measures Examples	MITRE ATT&CK Related TTPs
<ul style="list-style-type: none"> ▪ Search for critical assets by keywords and predefined customer's data ▪ Harvest passwords in scripts and files by exfiltrating the data to Candor/off-line processing ▪ Extract passwords stored in web browsers ▪ Perform screen captures from the host ▪ Extract data and secret material from databases files ▪ Take advantage of weak crypto management systems in administrative applications 	<p>Gather Victim Host Information (T1592), Valid Accounts (T1078), Exploitation for Credential Access (T1212), Credentials from Password Stores (T1555), OS Credential Dumping (T1003), Unsecured Credentials (T1552), Input Capture (T1056), File and Directory Discovery (T1083), Process Discovery (T1057), Query Registry (T1012), Software Discovery (T1518), System Owner/User Discovery (T1033), System Service Discovery (T1007), Automated Collection (T1119), Clipboard Data (T1115), Data from Information Repositories (T1213), Data from Local System (T1005), Data from Network Shared Drive (T1039), Data from Removeable Media (T1025), Man-in-the-Middle (T1557), Screen Capture (T1113), Email Collection (T1114), Data Staged (T1074)</p>

9. Lateral Movement

Description	
<p>Manage a dedicated extraction procedure of authentication material to be able to pivot laterally to new endpoints across the network</p>	
Measures Examples	MITRE ATT&CK Related TTPs
<p>Leverage credentials acquired using multiples techniques in order to perform remote code execution on additional hosts:</p> <ul style="list-style-type: none"> ▪ Extract web credentials from browser databases and validate and use them on discovered webapps ▪ Dump Windows credentials from LSASS/SAM/NTDS/VAULTS and try to execute code on other endpoints to test password reuse ▪ Extract SSH Keys from endpoints and try to move laterally to other SSH servers on the network ▪ Test segmentation by altering C&C protocols between payloads and Candor ▪ Upload command and control tools to compromised endpoints 	<p>Modify Authentication Process (T1556), OS Credential Dumping (T1003), Unsecured Credentials (T1552), Domain Trust Discovery (T1482), Remote System Discovery (T1018), Exploitation of Remote Services (T1210), Lateral Tool Transfer (T1570), Remote Services (T021), Software Development Tools (T1072), Taint Shared Content (T1080), Use Alternate Authentication Material (T1550), Internal Spearphishing (T1534)</p>

10. Privilege Escalation

Description	
Remote and local capabilities to escalate from non-privileged user to being able to execute code with high permissions	
Measures Examples	MITRE ATT&CK Related TTPs
<ul style="list-style-type: none"> ▪ Discovery of privileged accounts including AD domain accounts and local accounts ▪ Use remote exploitation to escalate privileges on Windows and Linux hosts ▪ Abuse network misconfigurations to get a hold on privileged authentication material – GPP passwords/credentials in openly accessible databases ▪ Take over system/root account with low privileged user by exploiting local privilege escalation vulnerabilities 	<p>Abuse Elevation Control Mechanism (T1548), Access Token Manipulation: Token Impersonation/Theft (T1134.001), Access Token Manipulation: Make and Impersonate Token (T1134.003), Exploitation for Privilege Escalation (T1068), Group Policy Modification (T1484), Process Injection: Dynamic-link Library Injection (1055.001), Process Injection: Thread Execution Hijacking (1055.003), Process Injection: Asynchronous Procedure Call (1055.004), Process Injection: Proc Memory (1055.009), Scheduled Task/Job (T1053), Valid Accounts (T1078)</p>

11. Data Exfiltration

Description	
Data transfer from a targeted endpoint triggered by takeover of a device	
Measures Examples	MITRE ATT&CK Related TTPs
<ul style="list-style-type: none"> ▪ Engage remote file systems including FTP, CIFS, HTTP based and SSH ▪ Search in files and scripts for business-sensitive data ▪ Extract source code, Personally Identifiable Information (PII), SSN, etc. ▪ Automatically parse and analyze vast variety of file formats – MSOffice, PDF, Scripts, Databases, etc. 	Automated Exfiltration (T1020), Network Share Discovery (T1135), File and Directory Discovery (T1083), Credentials from Password Stores (T1555), Automated Exfiltration (T1020), Exfiltration Over C2 Channel (T1041), Exfiltration Over Alternative Protocol (T1048)

12. Cleanup

Description	
Cleanup of attack created residues	
Measures Examples	MITRE ATT&CK Related TTPs
<ul style="list-style-type: none"> ▪ Registry values cleanup of deployed scheduled tasks ▪ Clean deployed file-based payloads ▪ Delete created users from privilege escalation phases ▪ Focus on cleanup of all residues from hosts including providing a full audit trail and deletion status of all residues 	Indicator Removal on Host (T1070)

Candor Capabilities Based on MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration
Exploit Public-Facing Application	Command and Scripting Interpreter	Create Account	Abuse Elevation Control Mechanism	Access Token Manipulation	Brute Force	Account Discovery	Exploitation of Remote Services	Automated Collection	Application Layer Protocol	Automated Exfiltration
External Remote Services	Exploitation for Client Execution	Scheduled Task/Job	Access Token Manipulation	BITS Jobs	Credentials from Password Stores	Cloud Infrastructure Discovery	Lateral Tool Transfer	Clipboard Data	Data Encoding	Exfiltration Over C2 Channel
Trusted Relationship	Inter-Process Communication	BITS Jobs	Exploitation for Privilege Escalation	De-obfuscate/Decode Files or Information	Exploitation for Credential Access	Cloud Service Discovery	Remote Services	Data from Information Repositories	Data Obfuscation	Exfiltration Over Alternative Protocol
Valid Accounts	Native API	Valid Accounts	Group Policy Modification	Direct Volume Access	Forced Authentication	Domain Trust Discovery	Software Deployment Tools	Data from Local System	Dynamic Resolution	
	Scheduled Task/Job	Create or Modify System Process	Process Injection	Exploitation for Defense Evasion	Man-in-the-Middle	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive	Encrypted Channel	
	Software Deployment Tools	Hijack Execution Flow	Scheduled Task/Job	Group Policy Modification	Modify Authentication Process	Network Service Scanning	Use Alternate Authentication Material	Data from Removeable Media	Fallback Channels	
	System Services		Valid Accounts	Hide Artifacts	Network Sniffing	Network Share Discovery	Internal Spear phishing	Man-in-the-Middle	Ingress Tool Transfer	
	Windows Management Instrumentation			Indicator Removal on Host	OS Credential Dumping	Network Sniffing		Screen Capture	Multi-Stage Channels	
				Indirect Command Execution	Unsecured Credentials	Password Policy Discovery		Email Collection	Non-Application Layer Protocol	
				Masquerading	Input Capture	Permission Groups Discovery		Data Staged	Non-Standard Port	
				Modify Authentication Process		Process Discovery			Protocol Tunneling	
				Modify Registry		Query Registry			Proxy	
				Network Boundary Bridging		Remote System Discovery				
				Obfuscated Files or Information		Software Discovery				
				Process Injection		System Information Discovery				
				Rogue Domain Controller		System Network Configuration Discovery				
				Signed Binary Proxy Execution		System Network Connections Discovery				
				Trusted Developer Utilities Proxy Execution		System Owner/User Discovery				
				Use Alternate Authentication Material		System Service Discovery				
				Valid Accounts						
				XSL Script Processing						