@hackinarticles

https://github.com/Ignitetechnologies

https://in.linkedin.com/company/hackingarticles

MITRE Windows ATT&CK Tree

Defense Evasion

- T1112 - Modify Registry
- Binary Padding
- Software Packing
- Steganography
- Compile After Delivery
- Indicator Removal from Tools
- HTML Smuggling
- Dynamic API Resolution
- Stripped Payloads
- Embedded Payloads
- T1027 - Obfuscated Files or Information
- System Firmware
- Component Firmware
- Bootkit
- T1542 - Pre-OS Boot
- Dynamic-link Library Injection
- Portable Executable Injection
- Thread Execution Hijacking
- Asynchronous Procedure Call
- Thread Local Storage
- Extra Window Memory Injection
- Process Hollowing
- Process Doppelgänging
- ListPlanting
- T1055 - Process Injection
- T1620 - Reflective Code Loading
- T1207 - Rogue Domain Controller
- T1014 - Rootkit
- Code Signing
- SIP and Trust Provider Hijacking
- Install Root Certificate
- Mark-of-the-Web Bypass
- Code Signing Policy Modification
- T1553 - Subvert Trust Controls
- Compiled HTML File
- Control Panel
- CMSTP
- InstallUtil
- Mshta
- Msiexec
- Odbcconf
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Verclsid
- Mavinject
- MMC
- T1218 - System Binary Proxy Execution
- PubPrn
- T1216 - System Script Proxy Execution
- T1221 - Template Injection
- Port Knocking
- Socket Filters
- T1205 - Traffic Signaling
- MSBuild
- T1127 - Trusted Developer Utilities Proxy Execution
- Pass the Hash
- Pass the Ticket
- T1550 - Use Alternate Authentication Material
- Default Accounts
- Domain Accounts
- Local Accounts
- T1078 - Valid Accounts
- System Checks
- User Activity Based Checks
- Time Based Evasion
- T1497 - Virtualization/Sandbox Evasion
- T1220 - XSL Script Processing
- Domain Controller Authentication
- Password Filter DLL
- Reversible Encryption
- Multi-Factor Authentication
- Hybrid Identity
- T1556 - Modify Authentication Process
- Invalid Code Signature
- Right-to-Left Override
- Rename System Utilities
- Masquerade Task or Service
- Match Legitimate Name or Location
- Double File Extension
- T1036 - Masquerading
- T1202 - Indirect Command Execution
- Clear Windows Event Logs
- Clear Command History
- File Deletion
- Network Share Connection Removal
- Timestomp
- Clear Network Connection History and Configurations
- Clear Mailbox Data
- Clear Persistence
- T1070 - Indicator Removal
- Disable or Modify Tools
- Disable Windows Event Logging
- Impair Command History Logging
- Disable or Modify System Firewall
- Indicator Blocking
- Safe Mode Boot
- Downgrade Attack
- T1562 - Impair Defenses
- DLL Search Order Hijacking
- DLL Side-Loading
- Executable Installer File Permissions Weakness
- Path Interception by PATH Environment Variable
- Path Interception by Search Order Hijacking
- Path Interception by Unquoted Path
- Services File Permissions Weakness
- Services Registry Permissions Weakness
- COR_PROFILER
- KernelCallbackTable
- T1574 - Hijack Execution Flow
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- NTFS File Attributes
- Hidden File System
- Run Virtual Instance
- VBA Stomping
- Email Hiding Rules
- Process Argument Spoofing
- T1564 - Hide Artifacts
- Windows File and Directory Permissions Modification
- T1222 - File and Directory Permissions Modification
- T1211 - Exploitation for Defense Evasion
- Environmental Keying
- T1480 - Execution Guardrails
- Group Policy Modification
- Domain Trust Modification
- T1484 - Domain Policy Modification
- T1006 - Direct Volume Access
- T1140 - Deobfuscate/Decode Files or Information
- T1622 - Debugger Evasion
- T1197 - BITS Jobs
- Token Impersonation/Theft
- Create Process with Token
- Make and Impersonate Token
- Parent PID Spoofing
- SID-History Injection
- T1134 - Access Token Manipulation
- Bypass User Account Control
- T1548 - Abuse Elevation Control Mechanism

Credential Access

- T1111 - Multi-Factor Authentication Interception
- T1621 - Multi-Factor Authentication Request Generation
- T1040 - Network Sniffing
- LSASS Memory
- Security Account Manager
- NTDS
- LSA Secrets
- Cached Domain Credentials
- DCSync
- T1003 - OS Credential Dumping
- T1649 - Steal or Forge Authentication Certificates
- Golden Ticket
- Silver Ticket
- Kerberoasting
- AS-REP Roasting
- T1558 - Steal or Forge Kerberos Tickets
- T1539 - Steal Web Session Cookie
- Credentials In Files
- Credentials in Registry
- Private Keys
- Group Policy Preferences
- T1552 - Unsecured Credentials
- Domain Controller Authentication
- Password Filter DLL
- Reversible Encryption
- Multi-Factor Authentication
- Hybrid Identity
- T1556 - Modify Authentication Process
- Keylogging
- GUI Input Capture
- Web Portal Capture
- Credential API Hooking
- T1056 - Input Capture
- Web Cookies
- SAML Tokens
- T1606 - Forge Web Credentials
- T1187 - Forced Authentication
- T1212 - Exploitation for Credential Access
- Credentials from Web Browsers
- Windows Credential Manager
- Password Managers
- T1555 - Credentials from Password Stores
- Password Guessing
- Password Cracking
- Password Spraying
- Credential Stuffing
- T1110 - Brute Force
- LLMNR/NBT-NS Poisoning and SMB Relay
- ARP Cache Poisoning
- DHCP Spoofing
- T1557 - Adversary-in-the-Middle

Privilege Escalation

- Change Default File Association
- Screensaver
- Windows Management Instrumentation Event Subscription
- Netsh Helper DLL
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Image File Execution Options Injection
- PowerShell Profile
- Component Object Model Hijacking
- Installer Packages
- T1546 - Event Triggered Execution
- T1068 - Exploitation for Privilege Escalation
- DLL Search Order Hijacking
- DLL Side-Loading
- Executable Installer File Permissions Weakness
- Path Interception by PATH Environment Variable
- Path Interception by Search Order Hijacking
- Path Interception by Unquoted Path
- Services File Permissions Weakness
- Services Registry Permissions Weakness
- COR_PROFILER
- KernelCallbackTable
- T1574 - Hijack Execution Flow
- Dynamic-link Library Injection
- Portable Executable Injection
- Thread Execution Hijacking
- Asynchronous Procedure Call
- Thread Local Storage
- Extra Window Memory Injection
- Process Hollowing
- Process Doppelgänging
- ListPlanting
- T1055 - Process Injection
- At
- Scheduled Task
- T1053 - Scheduled Task/Job
- T1611 - Escape to Host
- Default Accounts
- Domain Accounts
- Local Accounts
- T1078 - Valid Accounts
- Group Policy Modification
- Domain Trust Modification
- T1484 - Domain Policy Modification
- Windows Service
- T1543 - Create or Modify System Process
- Logon Script (Windows)
- Network Logon Script
- T1037 - Boot or Logon Initialization Scripts
- Registry Run Keys / Startup Folder
- Authentication Package
- Time Providers
- Winlogon Helper DLL
- Security Support Provider
- LSASS Driver
- Shortcut Modification
- Port Monitors
- Print Processors
- Active Setup
- T1547 - Boot or Logon Autostart Execution
- Token Impersonation/Theft
- Create Process with Token
- Make and Impersonate Token
- Parent PID Spoofing
- SID-History Injection
- T1134 - Access Token Manipulation
- Bypass User Account Control
- T1548 - Abuse Elevation Control Mechanism

Discovery

- T1057 - Process Discovery
- T1012 - Query Registry
- T1018 - Remote System Discovery
- Security Software Discovery
- T1518 - Software Discovery
- T1082 - System Information Discovery
- System Language Discovery
- T1614 - System Location Discovery
- Internet Connection Discovery
- T1016 - System Network Configuration Discovery
- T1049 - System Network Connections Discovery
- T1033 - System Owner/User Discovery
- T1007 - System Service Discovery
- T1124 - System Time Discovery
- System Checks
- User Activity Based Checks
- Time Based Evasion
- T1497 - Virtualization/Sandbox Evasion
- Local Groups
- Domain Groups
- T1069 - Permission Groups Discovery
- T1120 - Peripheral Device Discovery
- T1201 - Password Policy Discovery
- T1040 - Network Sniffing
- T1135 - Network Share Discovery
- T1046 - Network Service Discovery
- T1615 - Group Policy Discovery
- T1083 - File and Directory Discovery
- T1482 - Domain Trust Discovery
- T1622 - Debugger Evasion
- T1217 - Browser Bookmark Discovery
- T1010 - Application Window Discovery
- Local Account
- Domain Account
- Email Account
- T1087 - Account Discovery

Lateral Movement

- T1091 - Replication Through Removable Media
- T1072 - Software Deployment Tools
- T1080 - Taint Shared Content
- Pass the Hash
- Pass the Ticket
- T1550 - Use Alternate Authentication Material
- Remote Desktop Protocol
- SMB/Windows Admin Shares
- Distributed Component Object Model
- VNC
- Windows Remote Management
- T1021 - Remote Services
- RDP Hijacking
- T1563 - Remote Service Session Hijacking
- T1570 - Lateral Tool Transfer
- T1534 - Internal Spearphishing
- T1210 - Exploitation of Remote Services

Persistence

- T1133 - External Remote Services
- DLL Search Order Hijacking
- DLL Side-Loading
- Executable Installer File Permissions Weakness
- Path Interception by PATH Environment Variable
- Path Interception by Search Order Hijacking
- Path Interception by Unquoted Path
- Services File Permissions Weakness
- Services Registry Permissions Weakness
- COR_PROFILER
- KernelCallbackTable
- T1574 - Hijack Execution Flow
- Domain Controller Authentication
- Password Filter DLL
- Reversible Encryption
- Multi-Factor Authentication
- Hybrid Identity
- T1556 - Modify Authentication Process
- Office Template Macros
- Office Test
- Outlook Forms
- Outlook Home Page
- Outlook Rules
- Add-ins
- T1137 - Office Application Startup
- System Firmware
- Component Firmware
- Bootkit
- T1542 - Pre-OS Boot
- At
- Scheduled Task
- T1053 - Scheduled Task/Job
- SQL Stored Procedures
- Transport Agent
- Web Shell
- IIS Components
- Terminal Services DLL
- T1505 - Server Software Component
- Port Knocking
- Socket Filters
- T1205 - Traffic Signaling
- Default Accounts
- Domain Accounts
- Local Accounts
- T1078 - Valid Accounts
- Change Default File Association
- Screensaver
- Windows Management Instrumentation Event Subscription
- Netsh Helper DLL
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Image File Execution Options Injection
- PowerShell Profile
- Component Object Model Hijacking
- Installer Packages
- T1546 - Event Triggered Execution
- Windows Service
- T1543 - Create or Modify System Process
- Local Account
- Domain Account
- T1136 - Create Account
- T1554 - Compromise Client Software Binary
- T1176 - Browser Extensions
- Logon Script (Windows)
- Network Logon Script
- T1037 - Boot or Logon Initialization Scripts
- Registry Run Keys / Startup Folder
- Authentication Package
- Time Providers
- Winlogon Helper DLL
- Security Support Provider
- LSASS Driver
- Shortcut Modification
- Port Monitors
- Print Processors
- Active Setup
- T1547 - Boot or Logon Autostart Execution
- T1197 - BITS Jobs
- Additional Email Delegate Permissions
- Device Registration
- T1098 - Account Manipulation

Collection

- T1039 - Data from Network Shared Drive
- T1025 - Data from Removable Media
- Local Data Staging
- Remote Data Staging
- T1074 - Data Staged
- Local Email Collection
- Remote Email Collection
- Email Forwarding Rule
- T1114 - Email Collection
- Keylogging
- GUI Input Capture
- Web Portal Capture
- Credential API Hooking
- T1056 - Input Capture
- T1113 - Screen Capture
- T1125 - Video Capture
- T1005 - Data from Local System
- Sharepoint
- T1213 - Data from Information Repositories
- T1115 - Clipboard Data
- T1185 - Browser Session Hijacking
- T1119 - Automated Collection
- T1123 - Audio Capture
- Archive via Utility
- Archive via Library
- Archive via Custom Method
- T1560 - Archive Collected Data
- LLMNR/NBT-NS Poisoning and SMB Relay
- ARP Cache Poisoning
- DHCP Spoofing
- T1557 - Adversary-in-the-Middle

Command and Control

- T1104 - Multi-Stage Channels
- T1095 - Non-Application Layer Protocol
- T1571 - Non-Standard Port
- T1572 - Protocol Tunneling
- Internal Proxy
- External Proxy
- Multi-hop Proxy
- Domain Fronting
- T1090 - Proxy
- T1219 - Remote Access Software
- Port Knocking
- Socket Filters
- T1205 - Traffic Signaling
- Dead Drop Resolver
- Bidirectional Communication
- One-Way Communication
- T1102 - Web Service
- T1105 - Ingress Tool Transfer
- T1008 - Fallback Channels
- Symmetric Cryptography
- Asymmetric Cryptography
- T1573 - Encrypted Channel
- Fast Flux DNS
- Domain Generation Algorithms
- DNS Calculation
- T1568 - Dynamic Resolution
- Junk Data
- Steganography
- Protocol Impersonation
- T1001 - Data Obfuscation
- Standard Encoding
- Non-Standard Encoding
- T1132 - Data Encoding
- T1092 - Communication Through Removable Media
- Web Protocols
- File Transfer Protocols
- Mail Protocols
- DNS
- T1071 - Application Layer Protocol

Execution

- T1129 - Shared Modules
- T1072 - Software Deployment Tools
- Service Execution
- T1569 - System Services
- Malicious Link
- Malicious File
- T1204 - User Execution
- T1047 - Windows Management Instrumentation
- At
- Scheduled Task
- T1053 - Scheduled Task/Job
- T1106 - Native API
- Component Object Model
- Dynamic Data Exchange
- T1559 - Inter-Process Communication
- T1203 - Exploitation for Client Execution
- PowerShell
- Windows Command Shell
- Visual Basic
- Python
- JavaScript
- T1059 - Command and Scripting Interpreter

Exfiltration

- Exfiltration Over Bluetooth
- T1011 - Exfiltration Over Other Network Medium
- Exfiltration over USB
- T1052 - Exfiltration Over Physical Medium
- Exfiltration to Code Repository
- Exfiltration to Cloud Storage
- T1567 - Exfiltration Over Web Service
- T1029 - Scheduled Transfer
- T1041 - Exfiltration Over C2 Channel
- Exfiltration Over Symmetric Encrypted Non-C2 Protocol
- Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
- Exfiltration Over Unencrypted Non-C2 Protocol
- T1048 - Exfiltration Over Alternative Protocol
- T1030 - Data Transfer Size Limits
- T1020 - Automated Exfiltration

Impact

- T1495 - Firmware Corruption
- T1490 - Inhibit System Recovery
- Direct Network Flood
- Reflection Amplification
- T1498 - Network Denial of Service
- T1496 - Resource Hijacking
- T1489 - Service Stop
- T1529 - System Shutdown/Reboot
- OS Exhaustion Flood
- Service Exhaustion Flood
- Application Exhaustion Flood
- Application or System Exploitation
- T1499 - Endpoint Denial of Service
- Disk Content Wipe
- Disk Structure Wipe
- T1561 - Disk Wipe
- Internal Defacement
- External Defacement
- T1491 - Defacement
- Stored Data Manipulation
- Transmitted Data Manipulation
- Runtime Data Manipulation
- T1565 - Data Manipulation
- T1486 - Data Encrypted for Impact
- T1485 - Data Destruction
- T1531 - Account Access Removal

Initial Access

- T1091 - Replication Through Removable Media
- Compromise Software Dependencies and Development Tools
- Compromise Software Supply Chain
- Compromise Hardware Supply Chain
- T1195 - Supply Chain Compromise
- T1199 - Trusted Relationship
- Default Accounts
- Domain Accounts
- Local Accounts
- T1078 - Valid Accounts
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- T1566 - Phishing
- T1200 - Hardware Additions
- T1133 - External Remote Services
- T1190 - Exploit Public-Facing Application
- T1189 - Drive-by Compromise