Impacket, Software S0357 | MITRE ATT&CK®

Archived: 2026-04-05 12:55:48 UTC

Domain	ID		Name	Use
Enterprise	T1557	.001	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay	Impacket modules like ntlmrelayx and smbrelayx can be used in conjunction with Network Sniffing and LLMNR/NBT-NS Poisoning and SMB Relay to gather NetNTLM credentials for Brute Force or relay attacks that can gain code execution.[1]
Enterprise	T1570		Lateral Tool Transfer	Impacket has used its `wmiexec` command, leveraging Windows Management Instrumentation, to remotely stage and execute payloads in victim networks.[2]
Enterprise	T1040		Network Sniffing	Impacket can be used to sniff network traffic via an interface or raw socket.[1]
Enterprise	T1003	.001	OS Credential Dumping: LSASS Memory	SecretsDump and Mimikatz modules within Impacket can perform credential dumping to obtain account and password information.[1]
		.002	OS Credential Dumping: Security Account Manager	SecretsDump and Mimikatz modules within Impacket can perform credential dumping to obtain account and password information.[1]
		.003	OS Credential Dumping: NTDS	SecretsDump and Mimikatz modules within Impacket can perform credential dumping to obtain account and password information from NTDS.dit.[1]
		.004	OS Credential Dumping: LSA Secrets	SecretsDump and Mimikatz modules within Impacket can perform credential dumping to

Domain	ID		Name	Use
				obtain account and password information.[1]
Enterprise	T1558	.003	Steal or Forge Kerberos Tickets: Kerberoasting	Impacket modules like GetUserSPNs can be used to get Service Principal Names (SPNs) for user accounts. The output is formatted to be compatible with cracking tools like John the Ripper and Hashcat.[1]
		.005	Steal or Forge Kerberos Tickets: Ccache Files	Impacket tools – such as `getST.py` or `ticketer.py` – can be used to steal or forge Kerberos tickets using ccache files given a password, hash, aesKey, or TGT.[3][4]
Enterprise	T1569	.002	System Services: Service Execution	Impacket contains various modules emulating other service execution tools such as PsExec.[1]
Enterprise	T1047		Windows Management Instrumentation	Impacket's `wmiexec` module can be used to execute commands through WMI.[1][2]

Source: https://attack.mitre.org/software/S0357