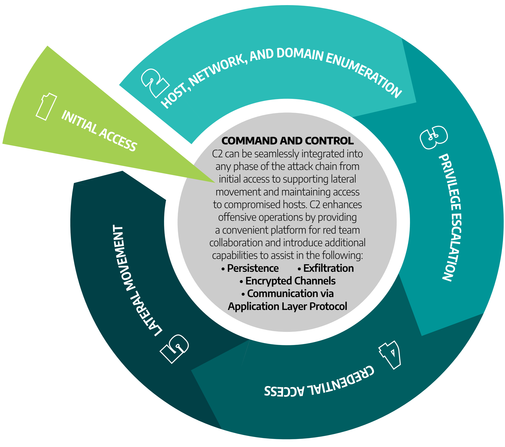
DRAGOS
SAFEGUARDING CIVILIZATION

Anatomy of a Penetration Test



PIVOT, ENUMERATE, REPEAT.

To reach our target system in the OT environment, it may require multiple hops traversing between network zones, pivoting through workstations and servers. For each new system encountered, the process is repeatable, requiring host and domain/network enumeration, harvesting credentials, and reassessing our path forward.

1

INITIAL ACCESS begins with an assumed breach approach working collaboratively with the client. A non-collaborative approach (Black Box) may require client-side or server-side exploitation to achieve initial access.

- Phishing
- Collaborative, Assumed Breach: Access to Valid Accounts
- Exploit Public-Facing Application (Server-Side Attack)

2

HOST, NETWORK, AND DOMAIN ENUMERATION Once we have obtained initial access to the corporate network, host and network enumeration is conducted to provide situational awareness of the environment. The goal is to identify potential paths that may lead to local and domain privilege escalation. Additionally, domain and network enumeration are crucial in determining the most efficient paths forward to achieve our objectives.

For example, domain or enterprise administrator may not always be the initial target when enumerating the environment, sometimes what is more important is to accurately identify the key groups and personnel that may have the adequate accesses to the operational environment (OT). To evade detection from endpoint security solutions, we leverage techniques such as PowerShell reflection to download and execute our tools from memory, preventing dropping any tools on the hard drive.

Examples of Host Enumeration

- File + Directory Discovery
- Application Window Discovery
- Account Discovery
- Seatbelt
- PowerSploit (includes PowerUp)

Examples of Network and Domain Enumeration

- Network Service Scanning
- Group Policy Discovery
- Bloodhound
- Domain Trusts

3

PRIVILEGE ESCALATION The goal is to elevate our privileges on the host we have compromised (Local Privilege Escalation) or obtain an elevated presence on the domain (Domain/Network Privilege Escalation) by identifying and compromising vulnerable services, applications, and domain configurations

EXPLOITATION FOR PRIVILEGE ESCALATION

- Steal or Forge Kerbros Tickets
- Print Nightmare
- Hive Nightmare

4

CREDENTIAL ACCESS Once we have elevated our privileges to an administrator (Local or Domain) or NT Authority System level access, the goal is to collect credentials from the local system. Credential harvesting may include obtaining the SAM database, dumping the LSASS process or searching through the file system for cached credentials (browser, application) or saved passwords in folders

- OS Credential Dumping
- Unsecured Credentials
- Credentials from Password Stores

5

LATERAL MOVEMENT Once we have obtained additional local and domain credentials, we can leverage native services to masquerade as valid users throughout the environment. To reduce the potential of detection, we prioritize utilizing native services and masquerading to perform lateral movement before resorting to remote service exploitation techniques.

For example, if the environment is not utilizing a local administrator password solution, we can reuse the local administrator password we obtained to pivot to additional workstations or servers

REMOTE SERVICES (COMMON SERVICES LEVERAGED)

- Remote Desktop Protocol (RDP)
- Windows Management Instrumentation
- Windows Remote Management
- Virtual Network Computing
- Secure Shell
- Server Message Block

EXPLOITATION OF REMOTE SERVICES (COMMON EXPLOITS LEVERAGED)

- EternalBlue (MS17-010)
- Zerologon (CVE-2020-1472)
- BlueKeep (CVE-2019-0708)

DRAGOS