Common Hacker Tools that Complement Mimikatz

blog.netwrix.com/2023/08/14/mimikatz-and-hacker-tools

Joe Dibley

Mimikatz is a popular post-exploitation tool that hackers use for lateral movement and privilege escalation. While Mimikatz is quite powerful, it does have some important limitations:

- It requires local admin rights on the compromised machine.
- Organizations can block Mimikatz from executing by enabling PowerShell protections.
- Using Mimikatz effectively requires a specialized skills and considerable time.

As a result, other toolkits have been created to complement Mimikatz. This article explains how three of them — Empire, DeathStar and CrackMapExec — make attacks easier for adversaries.

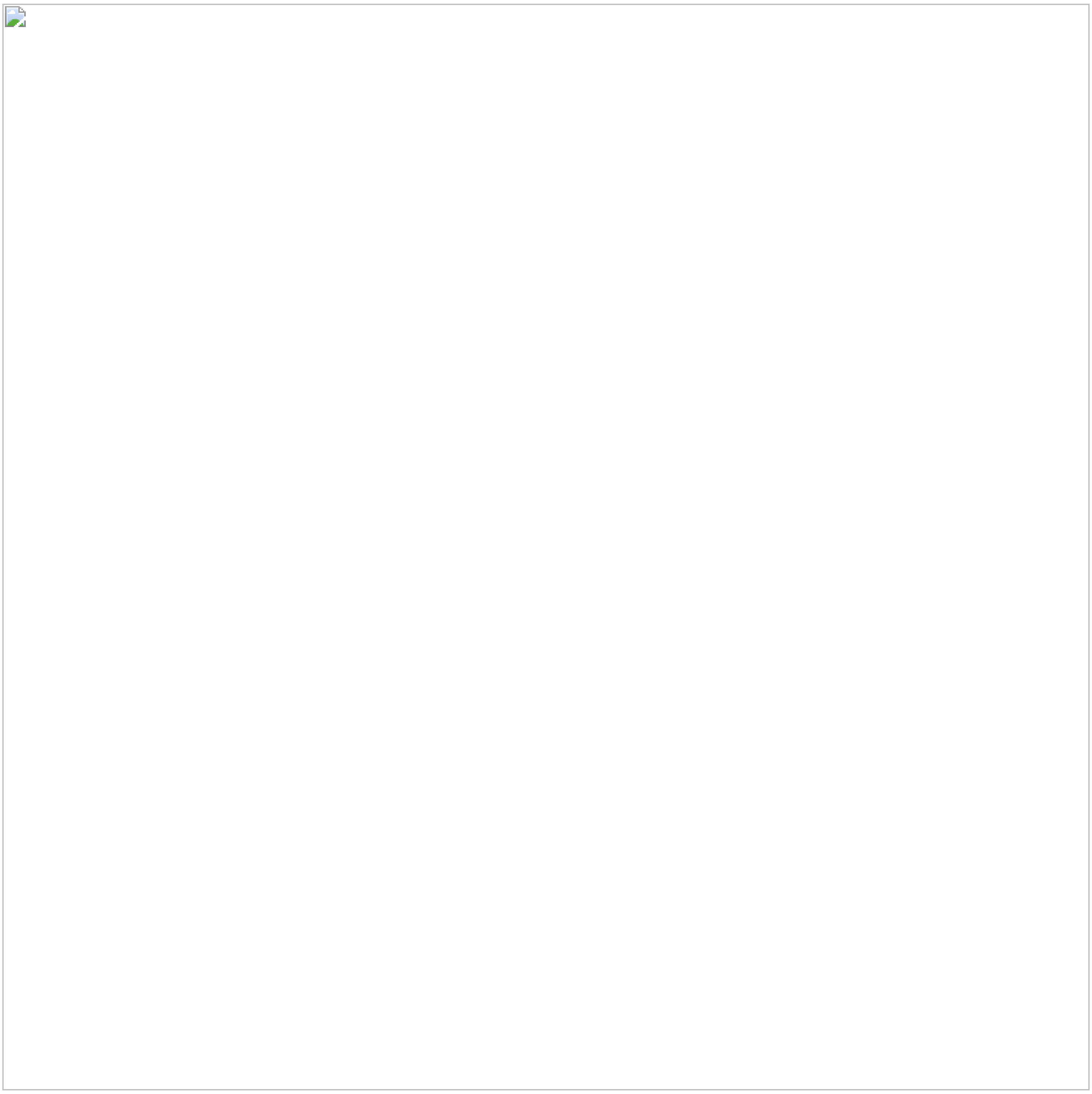
Learn how to tackle AD attacks:
Credential & Data Theft Attack Catalog

Empire

Privilege Escalation

By denying local admin rights to standard users, organizations can help prevent attackers from stealing credentials using Mimikatz. To get around this, adversaries can turn to Empire, which includes several modules for escalating privileges:

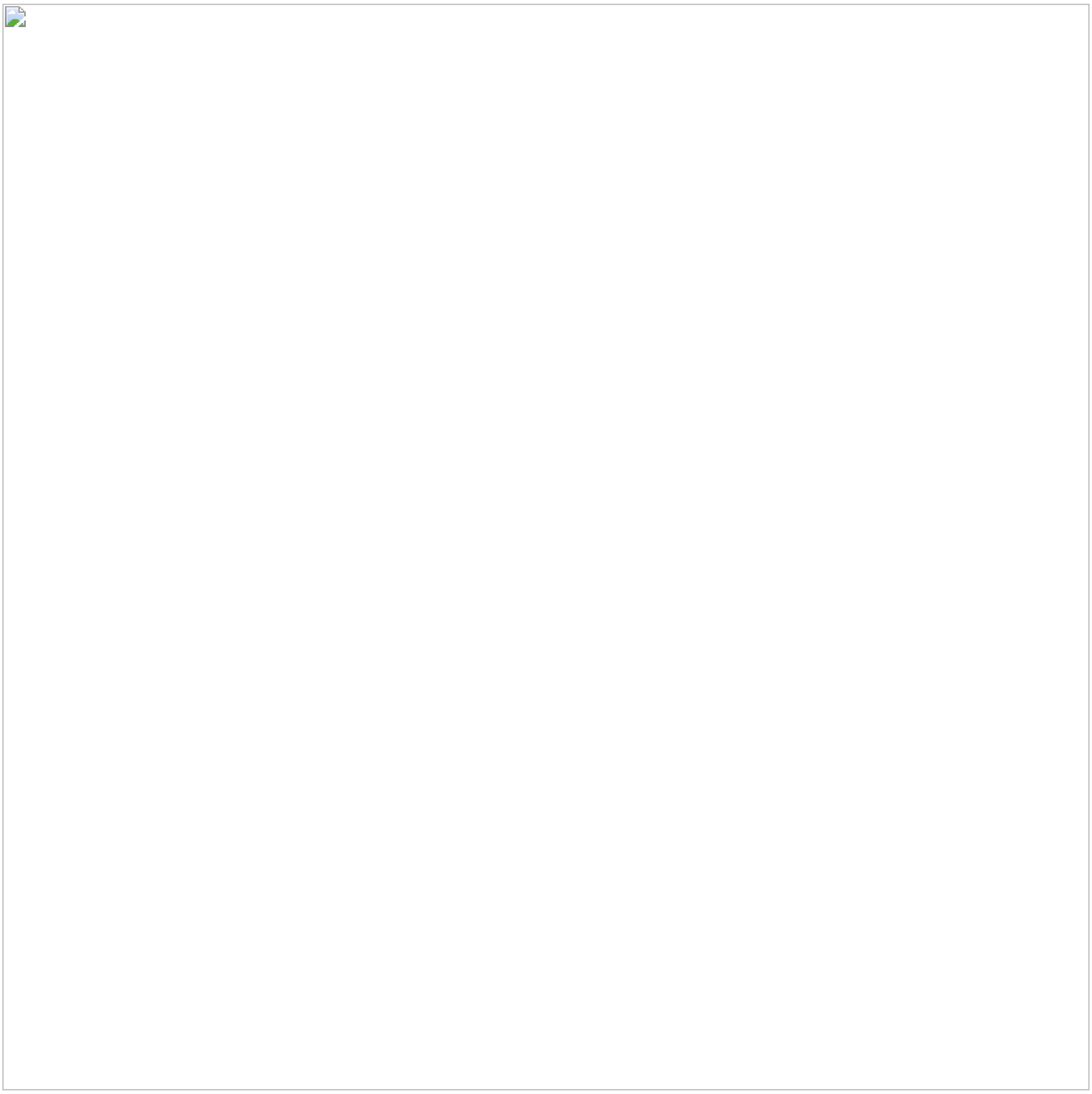
- The **BypassUAC** module helps hackers bypass User Account Control (UAC) on Windows systems.
- The **GPP** module takes advantage of a vulnerability in Group Policy Preferences to decrypt passwords stored in a Group Policy object (GPO).
- The **PowerUp** module scans a system for common privilege escalation vectors such as misconfigured permissions, vulnerable services and unpatched software. The screenshot below shows this module in action:



In this case, Empire found a DLL hijacking vulnerability, which an adversary could exploit using the following command: **powerup/write dllhijacker**.

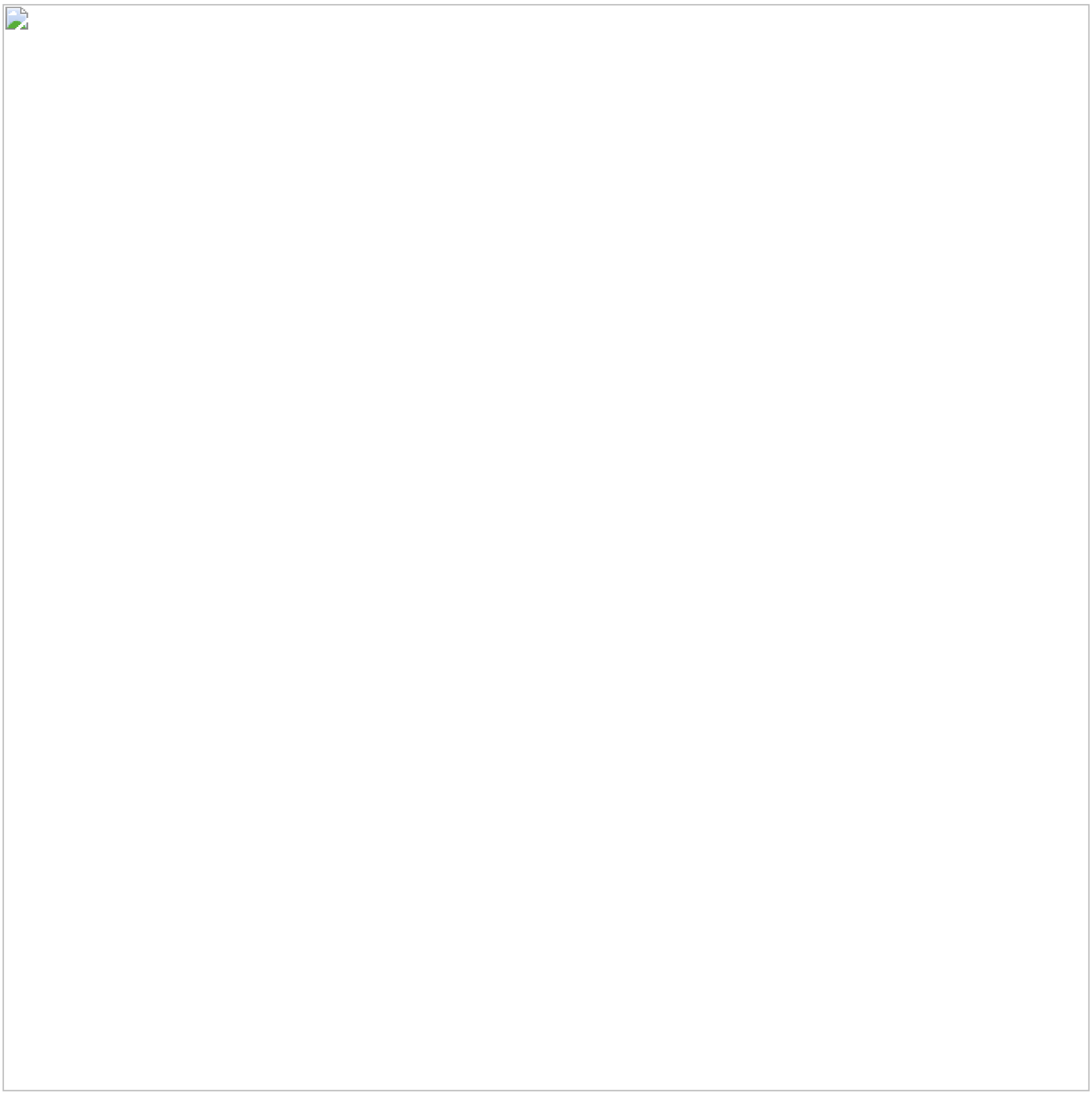
Agent Management

Empire also provides an easy-to-use interface that allows an attacker to monitor and interact with agents deployed in a targeted network, as shown in the screenshot below. This command and control feature is made possible using HTTP with a configurable port.



Credential Theft

Empire uses multiple approaches to help Mimikatz steal credentials: It will dump all passwords and password hashes from memory, and even present them in a table for easy viewing:

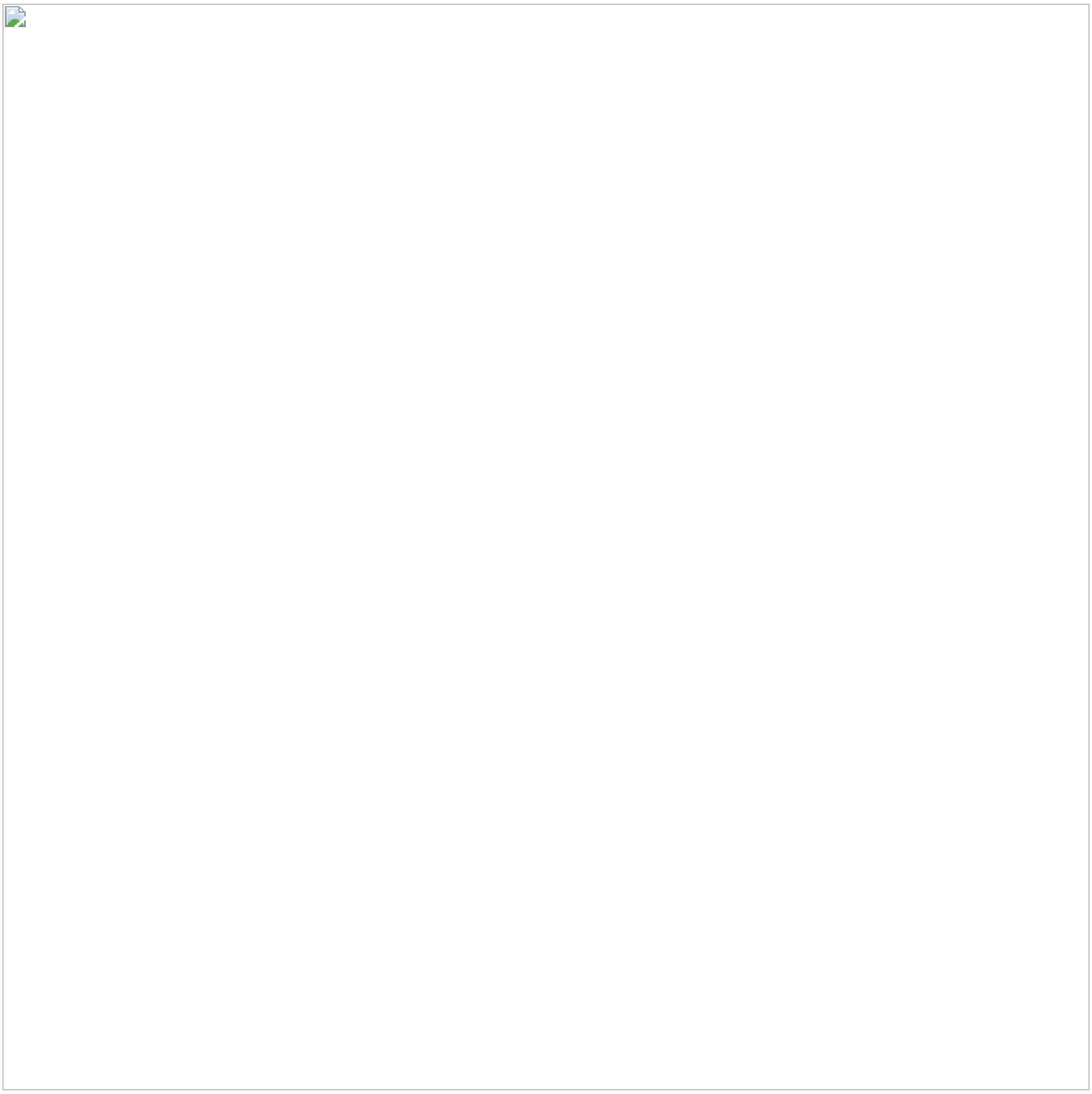


Empire also works with DCSync to steal credentials from Active Directory domains by impersonating a domain controller and making replication requests for password data.

DeathStar

DeathStar is an Empire module that merits its own discussion. It provides a powerful automation engine that empowers adversaries to execute scripts and other Empire modules on a large scale.

DeathStar operates similarly to another post-exploitation tool called BloodHound. While both tools are used by security professionals and penetration testers for legitimate tasks, they are also misused by hackers for malevolent purposes like network reconnaissance, vulnerability scanning, privilege escalation and lateral movement. The screenshot below shows the DeathStar module in action:

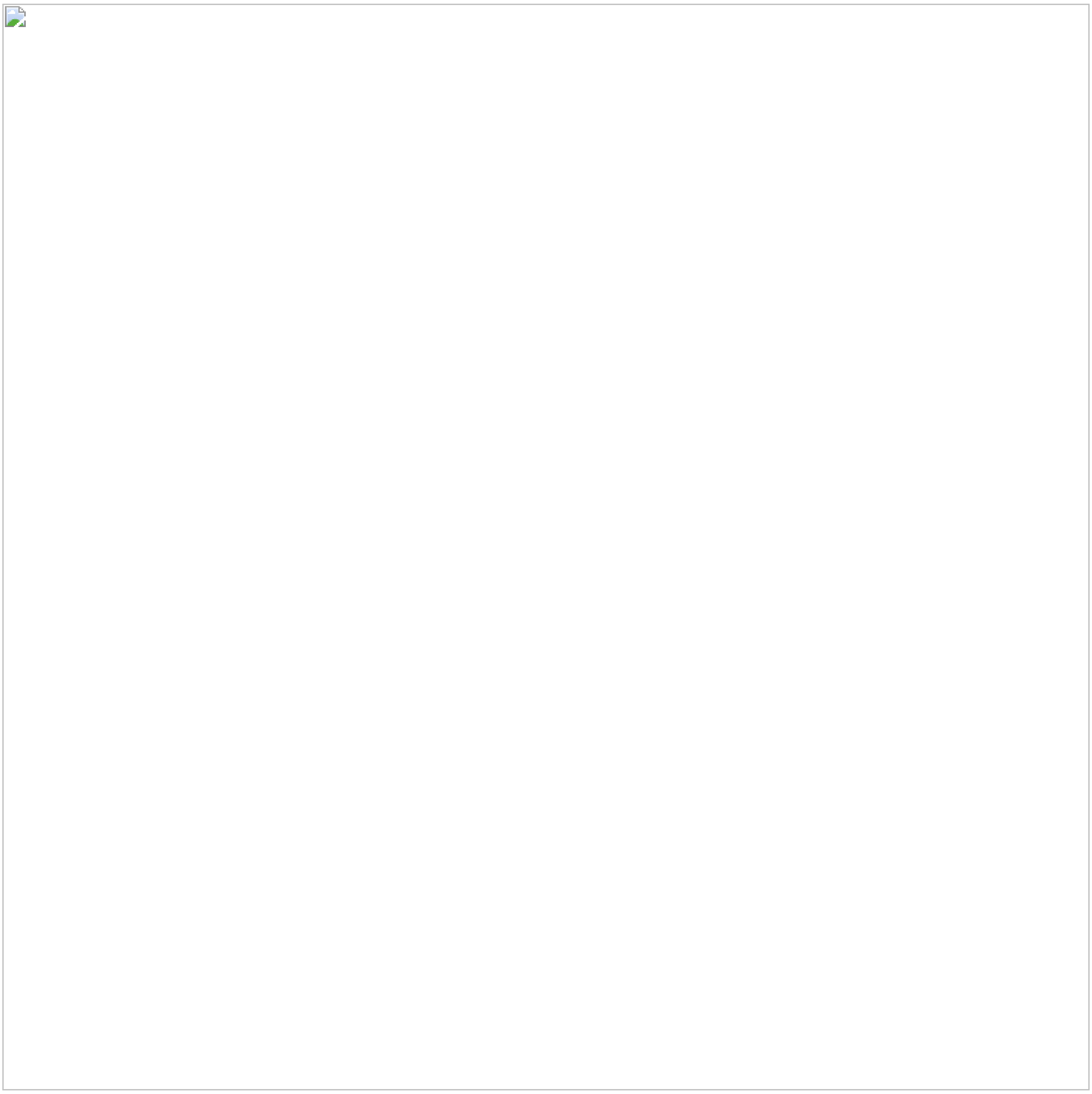


CrackMapExec

CrackMapExe (CME) is another post-exploitation tool that is a powerful enabler when integrated with Empire and DeathStar.

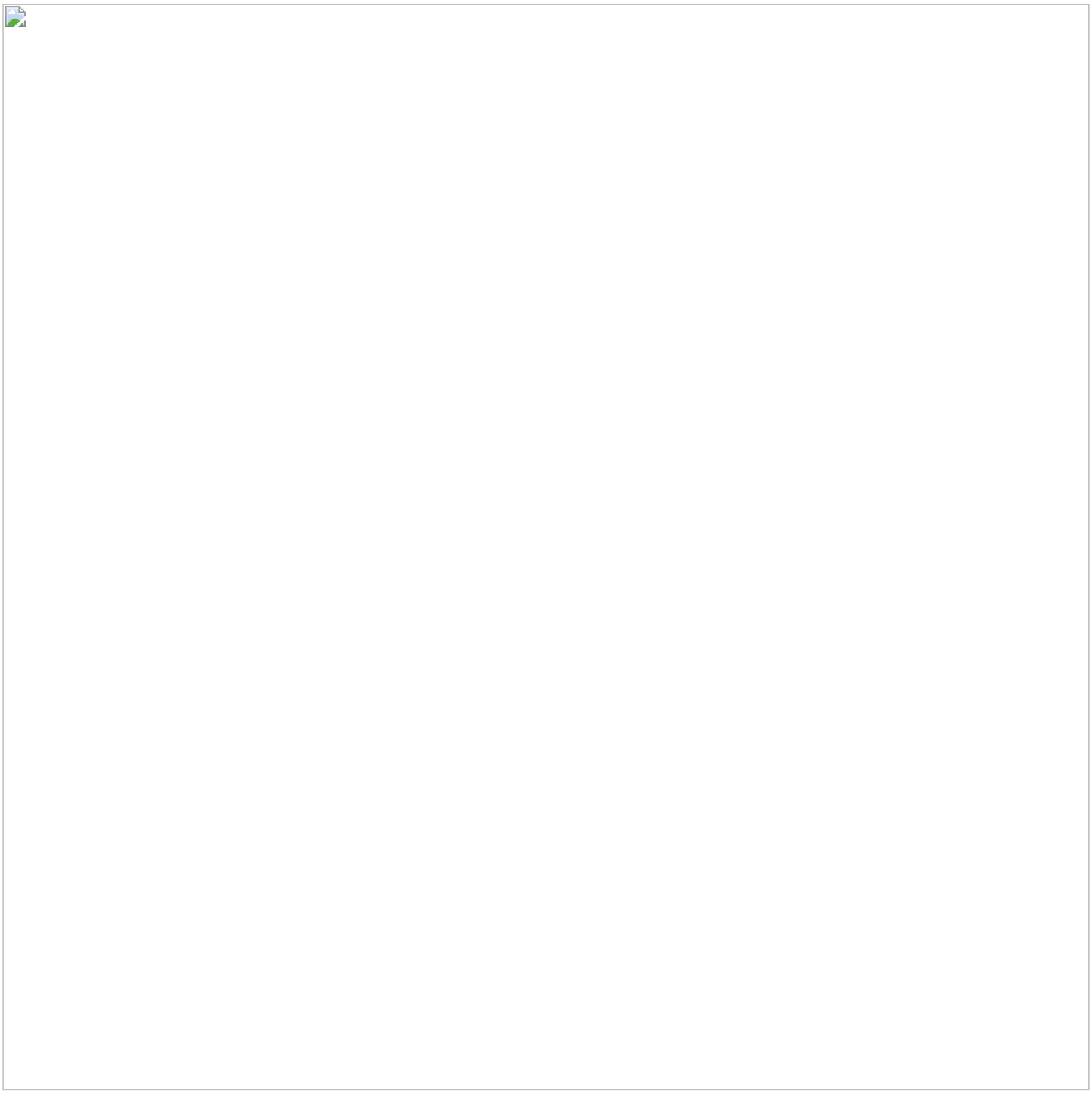
Domain Reconnaissance

CrackMapExec simplifies the reconnaissance process for attackers who have gained a foothold in an AD domain. CME can quickly enumerate the domain’s password policy and provide insights into details such as complexity requirements and lockout settings, as shown below.



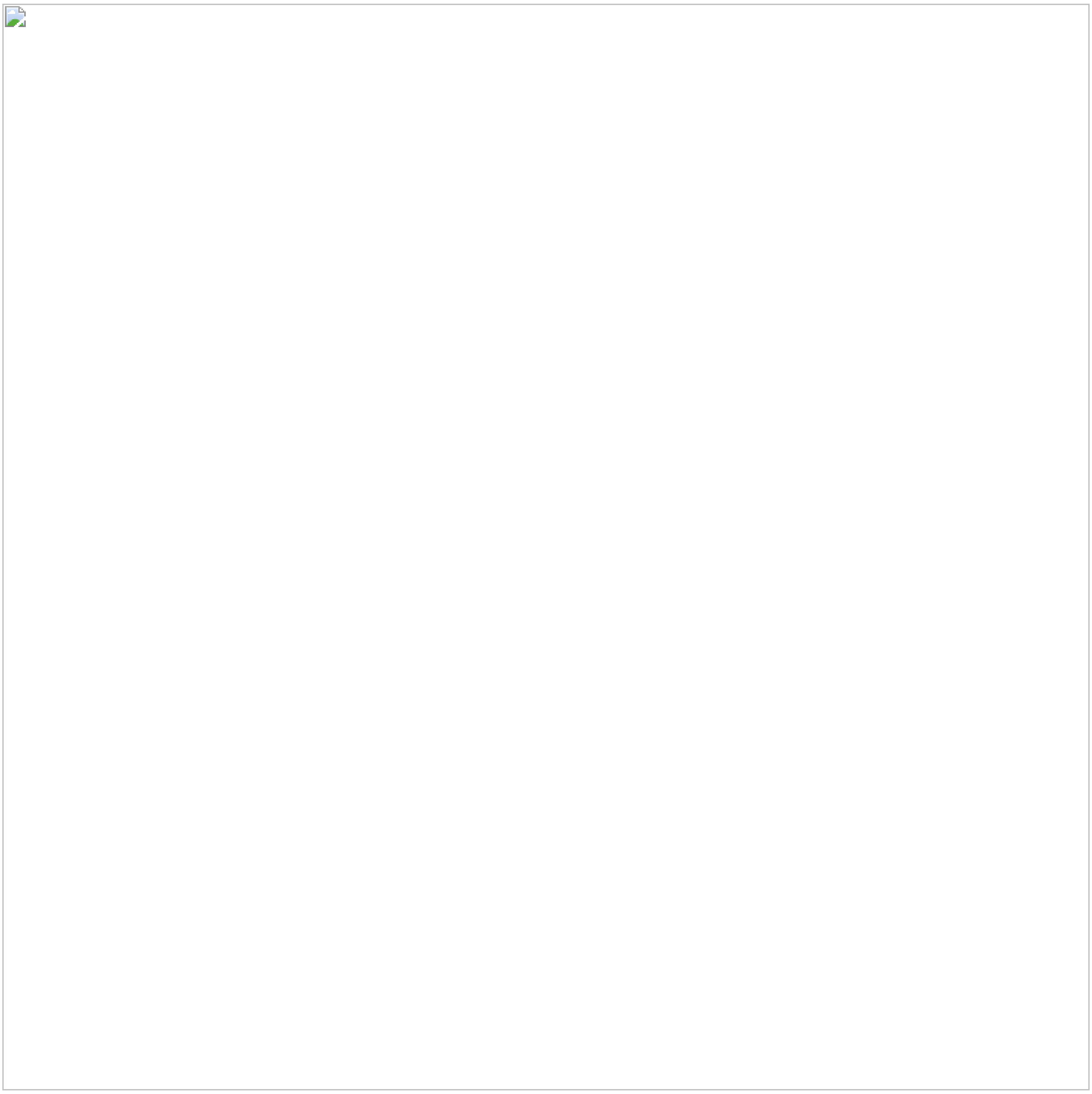
Enumerating AD Objects

CME will also enumerate all objects, including users and groups, in a brute-force fashion by guessing every resource identifier (RID), as shown below. (A RID is the ending set of digits in a security identifier [SID].)



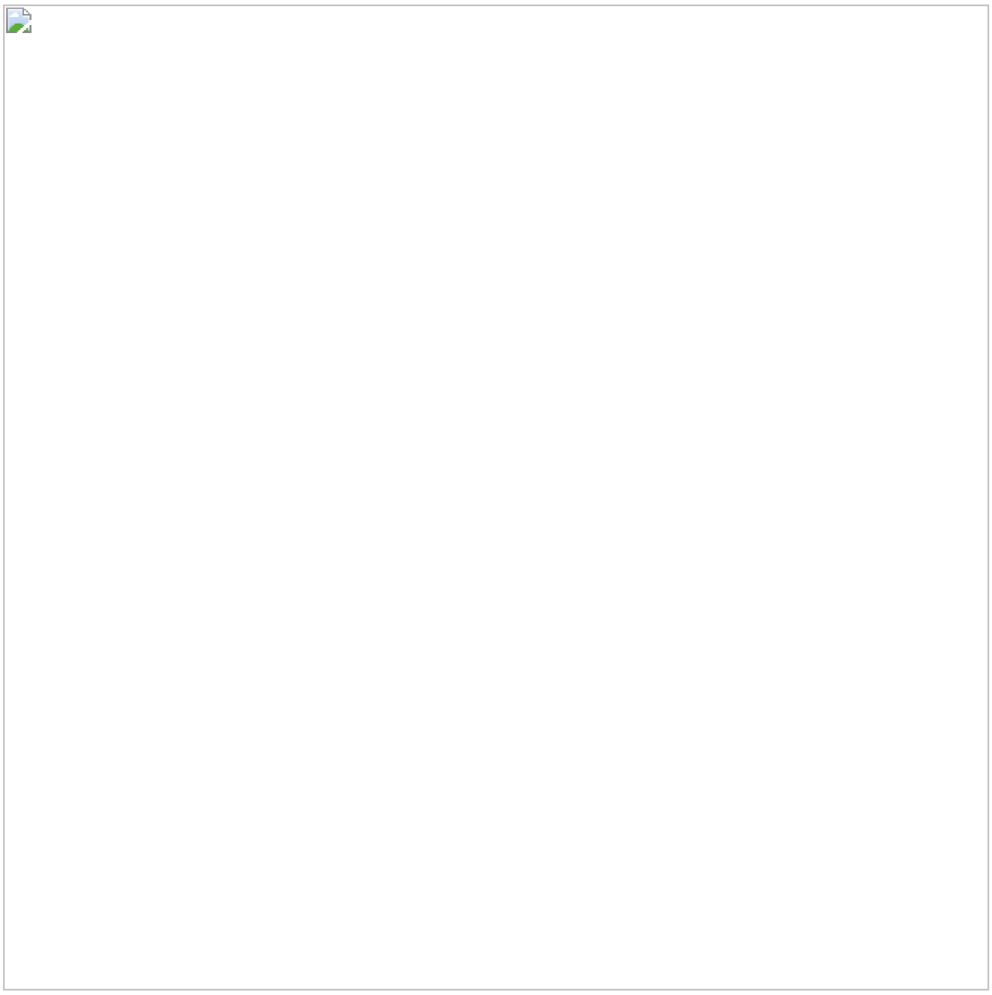
Discovering Anti-Virus Tools

CrackMapExec’s **enum_avproducts** module can discover what anti-virus software an organization is using. The output below shows where Windows Defender running.



Understanding an Account’s Rights

The lateral movement capabilities of CrackMapExec are very valuable. For instance, an adversary can discover all hosts in a specified IP range and whether a particular account has rights on those hosts, as shown here:



How Netwrix Can Help

By integrating tools like Empire, CrackMapExec and DeathStar with Mimikatz, threat actors who have gained a foothold in your Windows environment gain the ability to move laterally and escalate their privileges. While there are some basic PowerShell protections that can be enabled to detect and mitigate these types of attacks, those protections can be easily bypassed by experienced hackers.

One proven way to protect your organization from these malicious toolsets and other attacks is the Netwrix Active Directory Security Solution. It helps secure your Active Directory from end to end by empowering you to:

- Proactively identify and mitigate security gaps
- Promptly detect and respond to threats
- Recover quickly from security incidents to minimize downtime and other business impacts

With the Netwrix Active Directory Security Solution, you can be assured that all your AD identities and the underlying AD infrastructure that supports them are clean, properly configured, continually monitored, and tightly controlled, thus making the job of your IT teams easier and your organization more secure.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.