

Assignment 4.1: Post-Exploitation and Nmap Scanning

Joshua A. Wortz

University of San Diego

CSOL-570

Prof. Melanie Thomas

09/29/2025

Introduction

Open-source tools used by attackers are often the same tools defenders rely on for network visibility, troubleshooting, and validating security controls. This dual-use nature creates both risk and opportunity. Attackers employ tools such as Nmap, PowerView, SharpHound, BloodHound, and Mimikatz to enumerate services, harvest credentials, and plan lateral movement. At the same time, defenders use them to identify exposures, validate detections, and prioritize remediation (Diogenes & Ozkaya, 2022, Chs. 8–9). The TryHackMe labs *Post-Exploitation Basics* and *Nmap* demonstrate how these tools function in practice, highlighting their effectiveness for both Red and Blue Teams. This paper reflects on each lab, analyzing their usefulness, how their outputs can support a more active defense posture, and the defensive and monitoring strategies that can mitigate malicious use.

Lab 4.1 - Post-Exploitation Basics

Usefulness and Effectiveness

From a Red Team perspective, the post-exploitation toolkit presented in the lab is efficient. PowerView and SharpHound offer a straightforward, script-based approach to enumerating Active Directory environments, collecting information on user sessions, group memberships, and administrative rights, and identifying potential lateral movement paths. Once this data is ingested into BloodHound, attackers can visualize shortest paths to high-value targets such as domain administrators (Diogenes & Ozkaya, 2022, Ch. 8). Mimikatz, though requiring elevated privileges, is particularly powerful in extracting plaintext credentials, NTLM hashes, and Kerberos ticket-granting tickets (TGTs) from LSASS memory. When attackers gain access to the *krbtgt* account, they can generate golden tickets that provide persistent domain-wide

access (Diogenes & Ozkaya, 2022, Ch. 9). These tools are freely available and easy to deploy on compromised systems, making them attractive to adversaries. However, they also generate detectable activity, such as unusual PowerShell usage or LSASS memory access, which well-instrumented environments can identify (Microsoft, 2014, pp. 31–33).

From a Blue Team standpoint, these same tools are invaluable for defensive validation. Running SharpHound or BloodHound in a controlled setting enables defenders to view the same attack graphs that an adversary would, allowing them to identify excessive privileges, unconstrained delegation, and overexposed accounts. Similarly, testing with Mimikatz in a lab environment can validate whether LSA protection and Credential Guard are appropriately configured to prevent credential dumping. The practical realism of these tools also makes them excellent training resources in purple-team exercises, ensuring detection and response teams are familiar with the artifacts and telemetry attackers produce.

Informing Active Defense

The outputs of these post-exploitation tools are directly actionable for defenders. SharpHound and PowerView generate data about group memberships, local administrator rights, and session information, which can be compared with organizational policies to identify privilege creep or shadow administrative access. BloodHound’s visual attack paths highlight the shortest and most dangerous escalation routes, giving defenders a prioritized roadmap for remediation. Mimikatz outputs, including hashes and Kerberos tickets, indicate which credentials are at risk; their presence in an environment should prompt immediate containment steps such as rotating service account and *krbtgt* keys (Microsoft, 2014, pp. 29–31). Together, these deliverables transform

offensive reconnaissance into defensive intelligence, enabling organizations to pre-empt the lateral movement paths an attacker would likely follow.

Defensive and Monitoring Controls

To counter the malicious use of these tools, Blue Teams must deploy a layered set of host, identity, and network defenses. At the host level, enabling Credential Guard and LSA protection makes it significantly harder for attackers to extract credentials from LSASS memory (Microsoft, 2014, pp. 31–33). Endpoint detection rules should monitor for suspicious PowerShell usage, unusual process access to LSASS, and binaries that match Mimikatz behavior. Within Active Directory, organizations can restrict privileged account use to hardened administrative workstations, enforce unique local administrator passwords with solutions such as LAPS, and apply Authentication Policy Silos or the Protected Users group to limit Kerberos ticket exposure (Microsoft, 2014, pp. 42–47). Finally, centralized logging and SIEM correlation rules should combine Kerberos events, process creation logs, and network telemetry to detect credential theft and lateral movement attempts. By using the same visibility tools attackers rely on, defenders can continuously validate that these controls are adequate.

Lab 4.2 - Nmap

Usefulness and Effectiveness

Nmap is one of the most widely used tools for network reconnaissance, and it is equally valuable for both attackers and defenders. For Red Teams, its power lies in comprehensive service discovery. By scanning for open ports, fingerprinting services and operating systems, and using the Nmap Scripting Engine (NSE) for vulnerability checks, attackers can quickly identify exploitable services and misconfigurations. The tool is freely available, easy to deploy from

almost any system, and customizable through timing options and scan types, enabling adversaries to balance stealth against speed. Even when attackers attempt to be discreet, Nmap's scanning behavior often produces distinct signatures detectable by intrusion detection systems (IDS) and firewalls (Diogenes & Ozkaya, 2022, Ch. 8; CIS, 2021, pp. 8–11).

For Blue Teams, Nmap is indispensable for maintaining accurate network inventories. Regular, authorized scans identify shadow services, validate firewall rules, and confirm patching status. Defensive teams can replicate common attacker scan types in lab environments to ensure their IDS, IPS, and SIEM tools are tuned to detect reconnaissance patterns. As with post-exploitation tools, its value to defenders lies in using it proactively before adversaries do.

Informing Active Defense

Nmap outputs provide a wealth of defensive intelligence. Lists of open ports and service versions allow defenders to prioritize patching and close unnecessary exposures. For example, suppose Nmap identifies Remote Desktop Protocol (RDP) listening on multiple endpoints. In that case, defenders can implement CIS recommendations to place RDP behind Remote Desktop Gateways or VPNs and enforce multi-factor authentication (CIS, 2021, pp. 8–11). Saving scan outputs over time creates baselines that can be compared against subsequent scans to detect anomalies, such as unexpected new services that could indicate compromise or unauthorized software. When integrated into a broader vulnerability management process, Nmap outputs enable defenders to act on the same reconnaissance data that attackers would leverage.

Defensive and Monitoring Controls

Mitigating malicious use of Nmap requires a combination of network, host, and monitoring controls. Network segmentation and ingress filtering reduce the exposure of management ports,

while requiring RDG or VPN access for remote management significantly limits the attack surface (CIS, 2021, pp. 8–11). Host-based firewalls should restrict management services to known administrative ranges, and system administrators should turn off unnecessary services or ports. IDS and IPS sensors must be configured to detect common scanning signatures, such as sequential SYN packets or bursts of connection attempts across multiple ports. Finally, SIEM correlation rules should link scan-like activity with follow-up events such as repeated authentication failures or unusual Kerberos requests. These combined controls transform scan detection into early warning signals of potential intrusions.

Comparative Synthesis and Conclusion

Taken together, the two labs illustrate the lifecycle of an intrusion. Nmap provides the reconnaissance foundation, identifying exposed services and potential entry points, while post-exploitation tools enable attackers to escalate privileges and move laterally through a domain. From a defensive perspective, both sets of tools should be used proactively. Running BloodHound or SharpHound reveals risky privilege relationships before adversaries exploit them, and conducting regular Nmap scans builds an accurate and continuously updated view of the environment. Microsoft's PTH guidance emphasizes an "assume breach" posture, where containment, detection, and response are prioritized alongside prevention (Microsoft, 2014, pp. 6–13). CIS similarly stresses limiting the attack surface of protocols such as RDP through secure gateways and segmentation (CIS, 2021, pp. 8–11).

Ultimately, the lesson is clear: organizations cannot simply block or ban these tools, because their defensive value is too great. Instead, they must implement layered defenses that protect credential stores, restrict privileged account use, monitor for reconnaissance and

credential theft artifacts, and regularly validate controls using the same techniques that adversaries rely on. By adopting this approach, defenders can reduce attacker mobility, increase detection opportunities, and significantly strengthen their security posture.

References

CIS. (2020). *Remote Desktop Protocol (RDP) - CIS Exploited Protocols Guide*. Center for Internet Security.

Diogenes, Y., & Ozkaya, E. (2022). *Cybersecurity – Attack and Defense Strategies* (3rd ed.) - Chapter 8 (Lateral Movement) and Chapter 9 (Privilege Escalation).

Microsoft Trustworthy Computing. (2012). *Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques*.

Microsoft Trustworthy Computing. (2014). *Mitigating Pass-the-Hash and Other Credential Theft, version 2*.

TryHackMe. (n.d.). *Post-Exploitation Basics*. <https://tryhackme.com/room/postexploit>.

TryHackMe. (n.d.). *Nmap*. <https://tryhackme.com/room/furthernmap>.