AN EVALUATION OF THE COBALT STRIKE FRAMEWORK FOR RED TEAM ENGAGEMENTS

Christopher P. Hendricks (cphendri@hawaii.edu) | APSC-486 CYBER | Spring 2022

UNIVERSITY of HAWAIʻI® WEST OʻAHU

Abstract

Following the increase in the sophistication and frequency of cyber-attacks in recent years, the demand for skilled cybersecurity experts has also continued to grow year-over-year. Despite an industry-wide awareness of the cybersecurity skills shortage, few organizations have developed long-term plans to address the persistent gap in hiring and retaining qualified personnel. In a global survey conducted by the Information Systems Security Association (ISSA) last year, 489 cybersecurity professionals were asked what actions an organization could take to address the ongoing skills shortage. The biggest response (39%) received was an increase in cybersecurity training so that candidates can be properly trained for their roles (ISSA, 2021). More specifically, the study indicates how cybersecurity professionals widely value hands-on experience and mentoring for skills development, with a majority stating this experience is even more important than the achievement of industry certifications. When combined with technical training courses, Red Team adversary emulation and attack simulations can help bridge this gap by providing the hands-on experience that cybersecurity professionals necessitate. This is achieved by essentially teaching defenders how to respond to threats as they would appear in real life and how to react to different, unpredictable situations in a collective and collaborative way. Furthermore, Red Team engagements can help mitigate the risks to an enterprise by challenging the assumptions made by defenders and identifying areas for improving an organization's operational defense. The purpose of this study was to investigate how Cyber Red Teams use adversary emulation frameworks – focusing primarily on post exploitation, lateral movement, and maintaining persistence – to challenge the detection and response capabilities of an organization. In particular, we will evaluate the efficacy of the popular Cobalt Strike framework in simulating the threats posed by Advanced Persistent Threat (APT) actors in a secure training environment and how it can be used to promote a proactive approach to enterprise network security.

Research & Design Collection

This project was conducted for research purposes for the University of Hawaii and involved the use of a cloud-based cyber range built on the Snap Labs platform. A Red Team Workstation (Kali Linux 2021.4, Cobalt Strike 4.5) aggressed the Domain Controller (Windows 10 Pro N Build 14393) and 5 User Workstations (Windows 10 Pro N Build 14393) in a simulated enterprise environment. An Assumed Breach model, wherein the threat is assumed to have already exploited vulnerabilities and gained privileged access, was used for all evaluations. This scenario model was arguably the most beneficial because it started scenarios further into the attack timeline and allowed defenders to focus primarily on Detection and Response (NIST, 2021). The Assumed Breach model is used most frequently by mature organizations because it frees Red Teams to explore higher impact goals and is more efficient when resources time, money, or staff are limited (Tubberville & Vest, 2020). Microsoft, for example, has an Assumed Breach security strategy for their cloud services and they utilize Red Teaming to enhance threat detection, response, and defense for its enterprise cloud services (Microsoft, 2021).

This evaluation examined the Cobalt Strike framework's effectiveness in simulating several TTPs posed by Advanced Persistent Threat (APT) actors and the feasibility of the platform based on the following security metrics:

Mean Time to Compromise (MTTC): used to measure how quickly a network can be penetrated. This type of metric produces time values as end results and was measured from initial access to the first callback from the Cobalt Strike Beacon *(see Table 1).*

Mean Time to Privilege Escalation (MTTP): used to measure how quickly an adversary can gain higher-level permissions on a system or network. This metric also produces a time value and was measured from the initial Beacon callback to the point when the Red Team elevates their privileges to a SYSTEM level account *(see Table 2).*

The TTP's emulated in this evaluation are mapped to MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) matrix:

T1059	Command and Scripting Interpreter
T1003	OS Credential Dumping
T1543.003	Create or Modify System Process: Windows Service
T1059.001	Command and Scripting Interpreter: PowerShell
T1055	Process Injection
T1055.012	Process Injection: Process Hollowing
T1018	Remote System Discovery
T1029	Scheduled Transfer
T1035	System Services: Service Execution
T1021.002	Remote Services: SMB/Windows Admin Shares

Exercises which involve Red Team engagements have the potential to provide unbiased feedback to organizations about their assumptions about themselves and the capabilities of their adversaries. They can also help organizations train, prioritize threats and vulnerabilities, anticipate adversary actions and reactions, and test defenses. Since its release in 2012, the most widely used framework for conducting these types of exercises has been Cobalt Strike.

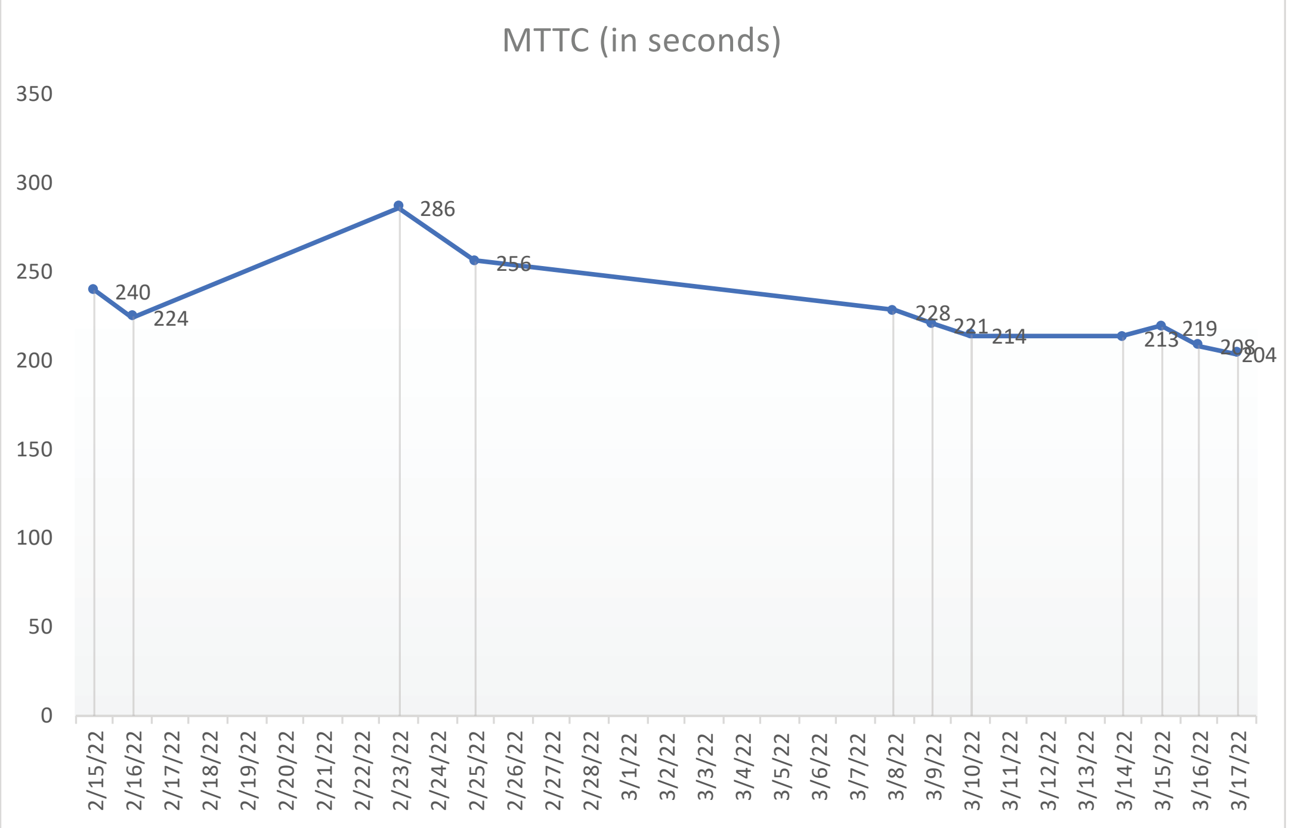


Table 1: Mean Time to Compromise (ave. 228.45 seconds)

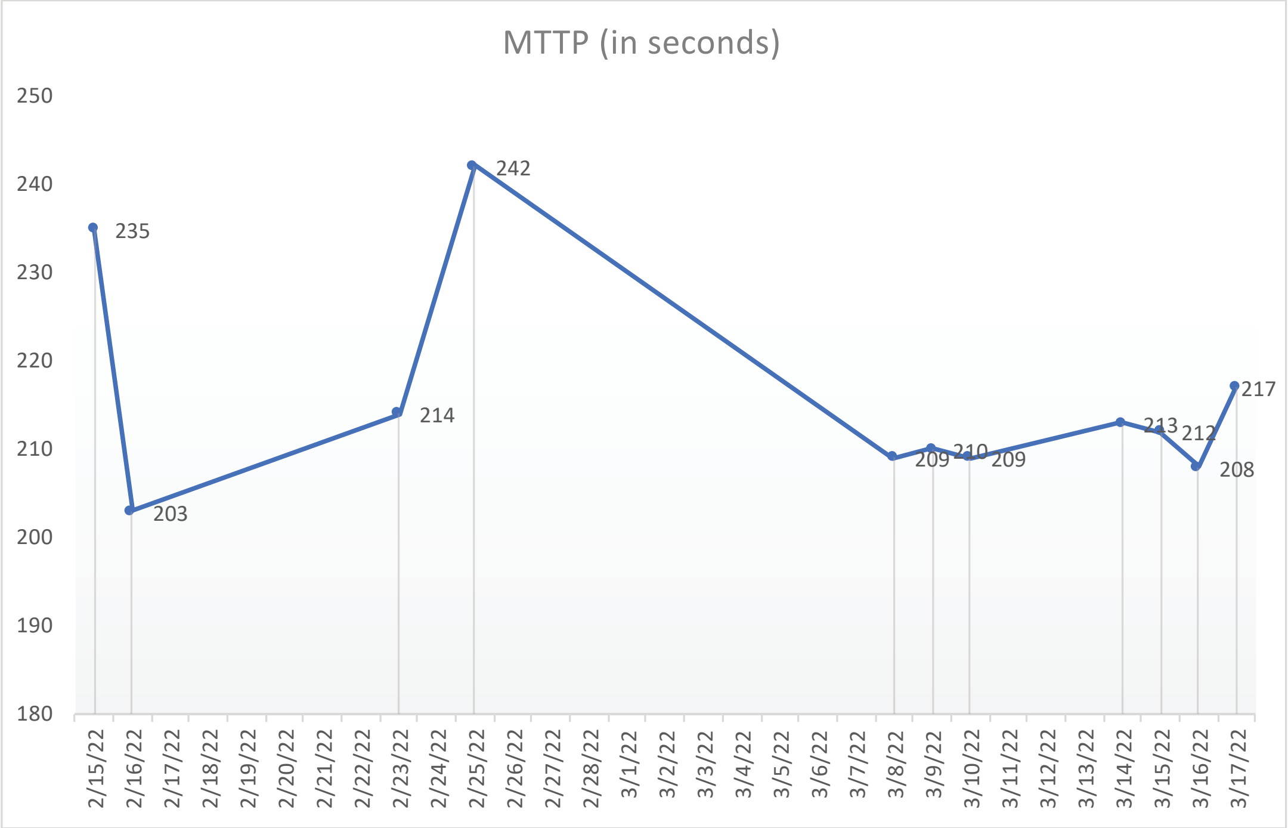
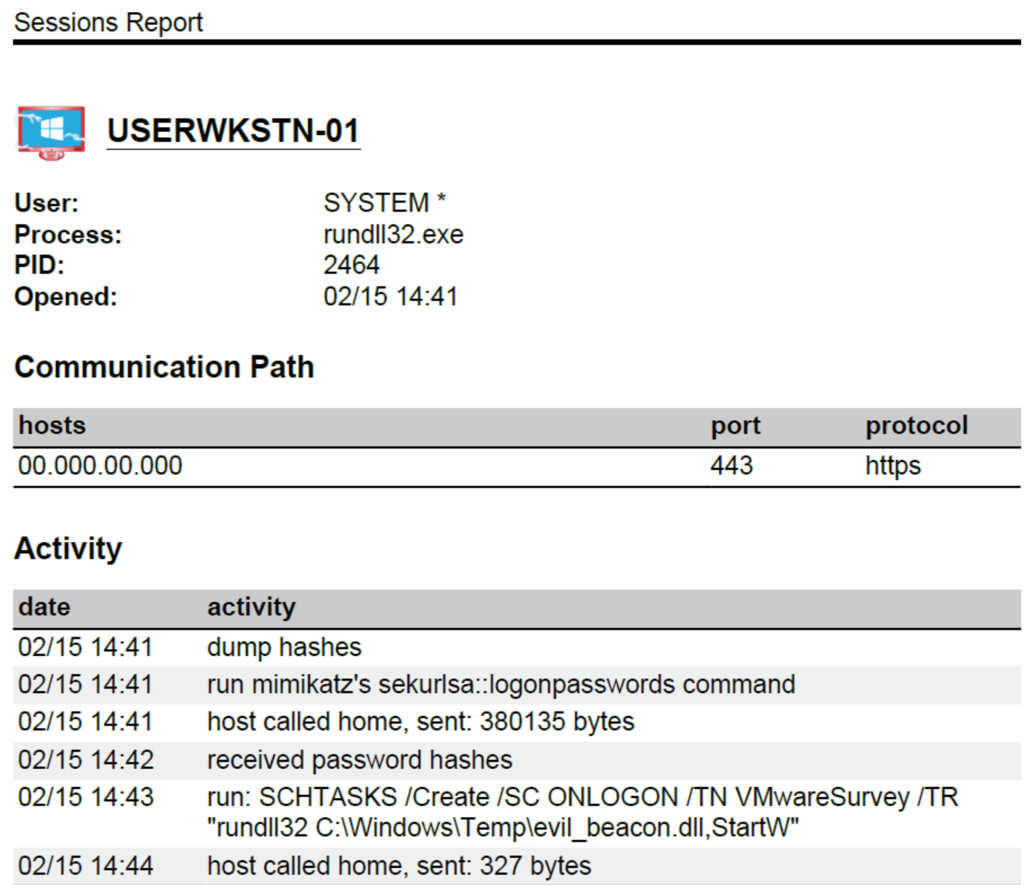


Table 2: Mean Time to Privilege Escalation (ave. 215.64 seconds)



Sessions Report

USERWKSTN-01

User:	SYSTEM *
Process:	rundll32.exe
PID:	2464
Opened:	02/15 14:41

Communication Path

hosts	port	protocol
00.000.00.000	443	https

Activity

date	activity
02/15 14:41	dump hashes
02/15 14:41	run mimikatz's sekurlsa::logonpasswords command
02/15 14:41	host called home, sent: 380135 bytes
02/15 14:42	received password hashes
02/15 14:43	run: SCHTASKS /Create /SC ONLOGON /TN VMwareSurvey /TR "rundll32 C:\Windows\Temp\evil_beacon.dll,StartW"
02/15 14:44	host called home, sent: 327 bytes

Figure 1: Red Team Activity Performed on a User Workstation

Conclusion

In investigating how Red Teams Operators use adversary emulation frameworks in a controlled virtual cyber range, we found that Cobalt Strike was both effective and accessible in simulating threats posed by Advanced Persistent Threat (APT) actors. Through our research, we found that it took an average of only 7 minutes and 24 seconds for a novice Red Team Operator to gain SYSTEM level privileges and emulate the 10 predetermined TTPs for this research. Furthermore, this evaluation reviewed the Vendor Documentation & Training Material, User Interface (UI) / User Experience (UX), Ease of Implementation, C2 Infrastructure, Exploit Library, Scalability, Resiliency, Logging and Reporting Options and found that Cobalt Strike is an incredibly effective framework for cyber threat emulation and Red Team Operations.