Feedback CCDC 2022 – Team 7 – Century College

Collegiate Cyber Defense Competition

2022 Midwest CCDC Qualification Feedback Report February 15, 2022

This report is to provide feedback and means of assessment to teams who have participated in the 2022 Midwest CCDC Qualifier on Febrary 5, 2022. Numbers are ratio to average scored by all teams at your event.

	Team #7
	Century College
Inject #1 Inventory	1.03
Inject #2 PortScan	0.00
Inject #3 Banner	0.81
Inject #4 06-WebInteg	0.82
Inject #5 NTP	0.00
Inject #6 PCAP	1.50
Inject #7 LnxPwd	0.96
Inject #8 WinPwd	1.53
Inject #9 AUP	0.90
Inject #10 CapPlan	0.00
Incident Reports	0.82
Red Team Score	0.34
Services	
ad-dns	1.11
bind-dns	1.17
ecom-http	1.20
mail-pop3	1.67
mail-smtp	1.84
splunk-http	1.36
Total Services	1.34

Chief Judge:

Competition Notes: Make sure to read injects completely and respond to all portions. | Keep things simple. Several cases of adding 3rd party software to accomplish things like NTP built into an OS which could introduce additional threat surface. | NTP - some had NTP within the network but didn't sync the NTP server to any external source. | If there is an exception to the inject, and you can't fully complete it as described, make a comment regarding that (i.e. why only 14 character min. pass on windows).

Red Team:

This year the red team relied on a few different vulnerabilities to get into the teams' systems. In general, attacks can be grouped into three primary categories:

1. Missing patches
2. Weak passwords
3. Misconfigurations

The attacks the red team used are no different. The most common issues that we used were:

1. EternalBlue, aka MS17-010, a Microsoft Windows exploit developed by the NSA and leaked by Shadow Brokers, and the most recent general wormable Windows exploit.
2. Zerologon, aka CVE-2020-1472, a vulnerability in the Active Directory netlogon that allows an attacker to gain access to a machine account, including that of the domain controller.
3. Guessing weak/default credentials. All teams changed their firewall passwords prior to the red team beginning their activity which was great! Most teams changed the credentials for the most obvious accounts, but several teams did have lower privileged accounts that were not changed. It is pretty common for systems to have privilege escalation attacks so even these can be impactful.

There wasn't anything very interesting for misconfigurations that we exploited this year.

Once we gained access to a system, attempt to escalate privileges if we weren't already administrators and then establish persistence. On Windows systems this could be things like issuing ourselves a golden ticket, dumping hashes that could be cracked, or simply used in pass-the-hash attacks, creating a new account, or changing the password on an existing account that we thought would not be detected, or installing a service that will phone home later. On Linux based systems we would usually install a service that phones home or create an account/change a password of an existing account. Generally, our goal at the beginning of the competition is to get access to as many systems as possible while maintaining as low of a profile as possible. Key to this is attempting to not interfere with normal system operations. Once we have access, we then attempt to get access to as many other systems as possible all while attempting to avoid getting caught. This is similar to how many real-world attacks occur, if an attacker does damage to a system, they will generally lose access to it and risk getting caught. Towards the end of the competition, we will then use the access that we gained earlier to take services out. This could be things like, locking out legit accounts, deleting/disabling services, or rendering systems unbootable and shutting them down. Generally, if you had issues with your systems prior to 2pm, it wasn't us, at least on purpose :-)

General recommendations:
1. Be sure to change credentials as soon as possible, a key part of this is knowing what is all out there.
2. Limit your attack surface. If a service isn't required, block it or turn it off. Generally, blocking the individual IPs/netblocks of systems detected as attackers isn't feasible in the real world and doesn't really work in the competition. Both real world attackers and the red team in CCDC can change their IPs when they want to and you risk blocking legitimate traffic. Also, in the real world, when you get to many rules enabled on your firewall, performance will be impacted. Instead, focus on providing the services that are required and limiting other access.
3. Apply the patches you can.

Feedback for specific teams (please send only to the referenced teams)
Team 7
Early in the competition we were able to break into your domain controller with the EternalBlue and Zerologon exploits. We were also able to guess credentials on your Fedora and Centos systems. From here we were able to establish persistence and maintained access throughout the competition.