THE SIX EVENTS OF THE ARMY CYBER FITNESS TEST

By Allison Moore, Data Scientist, Defense Threat Reduction Agency

To combat hostile cyber actors, military leaders at all echelons must understand the attack vectors used by cyber threat actors. The best way to truly understand these vectors is to become familiar with the tools a hostile actor uses when executing an offensive or reconnaissance cyber mission.

Despite the gravity of a very real threat to our network infrastructure, there are currently no standards for service members to follow to ensure they are "cyber conscious." As a result, we propose six cyber functions to serve as foundational areas to transform the military's cyber culture and enhance "unit cyber fitness," a readiness achieved by mastering levels of performance and standards, such as the Army Cyber Fitness Test (ACFT).

The six events of the Cyber Army Combat Fitness Test are Securing a Machine, Securing Data, Securing Network Traffic, Concealing Network Traffic, Understanding Social Engineering, and Managing Location Data. They include a baseline minimum standard—which is defensive by nature—and an advanced maximum standard that goes beyond simple cybersecurity and ventures into the realm of understanding actions taken by malicious actors in cyberspace. It is important to note unauthorized access to a network is illegal, and several of the tasks required to max the Cyber ACFT will require users to provide or establish their own target and/or attacking device.

EVENT 1: SECURING A MACHINE

MINIMUM - APPLY STRONG COMPUTER PHYSICAL SECURITY MEASURES.

We all know you should never leave your computer unattended in a public space, but there are additional measures you can take to secure access to your computer. This includes using separate administrator and user accounts, establishing strong passwords, and enabling good screen-lock settings. Although creating unique and complex passwords for all your accounts may seem inconvenient and challenging, a strong password manager can drastically reduce the annoyance while simultaneously increasing security.

MAXIMUM - EMPLOY A VIRTUAL MACHINE.

A virtual machine is essentially a computer within a computer. It uses a segregated portion of your computer's hardware to sandbox the virtual machine from your operating system. This allows users to run any operating system (i.e., Windows, Mac, Linux, etc.) in a manner that minimizes the likelihood of spillage of information from the virtual machine to the user's original operating system, and vice versa. Cybersecurity professionals and ethical hackers often use a virtual machine to test scripts and to create a target and/or attacking device for practice. If you find yourself wanting to practice some of the maxing events later but have another device to target legally, a virtual machine is probably a good solution.

Photo provided by Adobe Stock

EVENT 2: SECURING DATA

MINIMUM - ENCRYPT DATA.

Text encryption or other types of data inside an image file is known as steganography. There are many known vulnerabilities associated with basic password protection for files. File encryption may require a subscription or third-party software and regular maintenance. Using steganography adds an additional layer of protection for free. You can encrypt your data with a number of open-source software tools.

MAXIMUM - CRACK INTO A PASSWORD PROTECTED FILE.

A password-protected file is only as good as the password. To demonstrate the importance of selecting strong passwords and to develop an understanding of why certain criteria creates stronger passwords, you can create and hack into your own password-protected files.

Passwords usually are not stored as plaintext. They are stored as a hash, a unique combination of characters generated by a one-way function.[01] When you enter a password, the system checks if the hash of your entered text matches the stored hash of the true password. Salting involves adding characters to a password prior to hashing it, such that two identical passwords will have different salted hash values — thus, making them appear to be two different passwords. To crack passwords, hackers use a number of tools such as rainbow tables[02], dictionaries[03], and social engineering.

Photo provided by Adobe Stock

EVENT 3: SECURING NETWORK TRAFFIC

MINIMUM - ESTABLISH STRONG ROUTER SETTINGS.

The United States Special Operations Command (USSOCOM) provides a plethora of cybersecurity recommendations in Identity Management Smartcards.[04] After following USSOCOM Wi-Fi recommendations, you should also configure a firewall. Learn more about firewalls from InfoSec Institute.[05]

MAXIMUM - IDENTIFY/TRACE ABNORMAL NETWORK TRAFFIC.

When you go on the internet, your computer sends and receives network packets, small segments of data that form the totality of the information shared.[06] You can view all these packets using a packet sniffer—or protocol analyzer—that can help identify abnormal or suspicious network traffic Open-source packet analysis tools are well documented and offers useful tutorials.[07] They offer a user interface that provides an intuitive design to reduce the learning curve.

Photo provided by Adobe Stock

EVENT 4: CONCEALING NETWORK TRAFFIC

MINIMUM - EMPLOY A VIRTUAL PRIVATE NETWORK (VPN).

Survey data from NordVPN demonstrates an increasing trend in VPN use within the United States following the COVID-19 pandemic, with approximately one third of Americans choosing to use a personal VPN.[08] If you are in the subset of Americans who does not know what a VPN is, you can get more information about them from cyber security and tech news and research websites, such as cybernews.com.[09] A VPN essentially masks your IP address as you navigate the web and is one of the simplest tools you can employ to increase your security online.

MAXIMUM - ESTABLISH A CUSTOM PROXY CHAIN.

A proxy chain is a chain of proxy servers used to achieve the similar goal of masking the originating IP address. These are much more advanced than simply hitting 'connect' and are generally easiest to implement by using proxy chain tools.[10] Understanding the tools required to create a proxy chain will introduce users to some of the foundational knowledge hackers have.

Photo provided by Adobe Stock

EVENT 5: UNDERSTANDING SOCIAL ENGINEERING

MINIMUM - IDENTIFY SOCIAL ENGINEERING ATTEMPTS.

Social engineering involves manipulating people and exploiting their weaknesses. Social engineering aids bad actors during their attempts to gain access to systems or to gain information about their target. It can be done in any domain and is not limited to cyberspace. All basic users should be familiar with elicitation, shoulder surfing, baiting, tailgating, and phishing (and its variants).

MAXIMUM - ESTABLISH A REVERSE TCP CONNECTION.

A reverse TCP attack navigates around a firewall by socially engineering a target user into initiating a TCP connection (rather than the attacker initiating the connection). Once a user initiates the connection, an attacker can employ several malicious cyber activities. Kali Linux Metasploit is a common tool used to accomplish this task. Executing a reverse TCP connection without the knowledge and authorization of the target user is illegal. Maxing Event 5 will require you to establish a target and Linux attacker machine on your private network.

Photo provided by Adobe Stock

EVENT 6: MANAGING LOCATION DATA

MINIMUM - TURN OFF GEOTAGGING AND LOCATION SHARING.

Geotagging is the process applied to digital media that results in location and other data being applied as metadata to the media. You can turn off photo geotagging and location sharing settings on your devices by following the USSOCOM Identity Management Smartcards for your types of devices found under "Phones and Hardware." Check out the "Smartphone EXIF Removal" smartcard for more information on geotagging.[11]

MAXIMUM - GEOLOCATE A SPECIFIC DEVICE.

Although geolocating a specific device is no simple feat, you can make yourself an exceptionally hard target by minimizing your digital exposure and familiarizing yourself with the tools needed to track a device in time and space. It may be easiest to hack the password for a user's 'Find My Phone' functionality (check your device's Find Me function to see how well you locked down your location sharing). However, you can obtain geospatial information for a specific device using secured ingress platforms and some high-quality social engineering. Learn how from Loi Liang Yang.[12]

Photo provided by Adobe Stock

CONCLUSION

The minimum standards for the Cyber ACFT represent measures that are absolutely mission essential in protecting the joint force from hostile cyber actors. Although the minimum standards are not the only cyber events to be aware of, they provide a baseline for establishing a cyber-conscious foundation. As you progress through the events, you will find maxing the Cyber ACFT is quite difficult, as it demands a deeper understanding of networks and the tools available to malicious actors.

01 Ghosh, Riku, "Want to Know What is Hashing inCybersecurity? The Ultimate Guide," https://www.emeritus.org/blog/cybersecurity-what-is- hashing-in-cybersecurity/.

02 GeeksforGeeks, "Understanding Rainbow Table Attack," 10 February 2023, https://www.geeksforgeeks.org/understanding-rainbow-table-attack/.

03 GeeksforGeeks, "What isa Dictionary Attack," 4 July 2022, https://www.geeksforgeeks.org/what-is-a-dictionary-attack/.

04 United States Special Operations Command, "USASOC Identity Management," 14 November 2023, https: /www.soc.mil/IdM/publications/IdMpubs.html.

05 Gonzalez, Bianca, "Howto Configure a Network Firewall: Walkthrough," 13 March 2023, https://resources.infosecinstitute.com/topics/network-security-101/configure-network-firewall/.

06 Cloudflare, "What isa Packet?" https://www.cloudflare.com/learning/network-layer/what-is-a-packet/.

07 WireShark, "Wireshark Training," https: /www.wireshark.org/docs/.

08 Globytė, Ema, "NordVPNSurvey Shows: AThird of Americans Use a VPN," 28June 2023, https://nordvpn.com/blog/nordvpn-usage-surveyus/#:~:text=Two%20in%20three%20people%20(66.8,25%20and%2044%20years%20old.

09 Jankevičiūtė, Dovilė, "HowTo Set Up a VPN," 15 November 2023, https://cybernews.com/what-is-vpn/how-to-set-up-a-vpn/.

10 Kali Linux, "Proxychains-Ng: Packages and Binaries," https://www.kali.org/tools/proxychains-ng/.

11 United States Special Operations Command, "USASOC Identity Management," 14 November 2023, https://www.soc.mil/IdM/publications/IdMpubs.html.

12 Yang, Loi Liang, "Geolocation Tracking Via HTML5 and JavaScript. Track APhone's Location Over the Internet." https://www.youtube.com/watch?v=0kbvwUf5FLo&ab_channel=LoiLiangYang.