Christopher Uweh

Professor DeAndre Favors

ACCCSMay22-289

31 October 2022

Summative Research Project: Penetration Test Proposal

**Executive Summary:**

Enterprises and consumers increasingly rely on computing networks because all users expect to exchange information at the speed of thought. With the evolution of technology, there has been a greater focus on ease of use. Routine tasks rely on computers for accessing, providing, or just storing information. Vigilant compliance may seem burdensome; however, the potential fines and reputational damage caused by insufficient security can be fatal. There is a sense of urgency on behalf of organizations such as Green Clothing Company (GCC) to secure these assets from likely threats and vulnerabilities. GCC provided information about its current organizational setup, which is a perfect starting point.

Hackers break into systems for various reasons. Understanding how and why malicious hackers attack and exploit systems is essential. Security professionals must guard their infrastructure against exploits by knowing the enemy—the malicious hacker(s)—who seek(s) to use the same infrastructure for illegal activities (Ethical Hacking Essentials). This assessment responsibly mimics real-world attack scenarios using gray box testing to provide GCC with data-driven insights.

**Information Gathering And Client Expectations:**

Popular depictions of hacking provide a false image of the true nature of the Enterprise Information Theft paradigm: Typically, a man in a hoodie furiously types code on a laptop, immediately gains access, and perpetrates malicious activities. Today's most dangerous threat actors exhibit incredible patience and restraint while conducting reconnaissance and creating custom toolkits designed for persistence: The Solarwinds hackers gained access, then hid in plain sight on the network for up to nine months (Temple-Raston). For a thorough Red Team assessment, GCC must agree to a test period of at least four weeks. High-value GCC stakeholders involved in the process must sign Non-Disclosure Agreements. Likewise, the Penetration team must sign a legally binding contract. The testers must meticulously document all changes made to GCC's infrastructure & provide remediation techniques to restore compromised systems. The objective of the test is to show where GCC's security fails & how to harden its posture. All activities and observations require documentation so GCC can accurately quantify organizational risk and implement Quarterly reviews.

**Scope & Tactics, Techniques, and Procedures (TTP):**

-Testing Location(s): Adjacent to a GCC Corporate Office Wi-Fi Access Point & Remote

-Testers: Red Team composed of Kenzie Academy Certified Ethical Hackers

-Security Testing Platforms: Kali Linux & ParrotOS

*Remote/Reconnaissance External Network Level:*

-Open Source Intelligence Gathering (OSINT) against Corporate General Employees, using Google Dorks, Whois Lookups

-Passive reconnaissance & Port enumeration of the non-Card Data Environment (CDE) GCC network(s), hosts, & users using Network Sniffers/Packet Analyzers such as dSniff Suite, NMAP & Wireshark.

*Corporate Adjacent Mobile Device/Internal Network Level:*

-Key Reinstallation Attack (KRACK) against Corporate General Employees using the Aircrack-ng suite

-Evil Twin/Rogue AP against Corporate General Employees using Hak5 Wi-Fi Pineapple

-Bluetooth Man in the Middle (MITM)/Impersonation attack against Corporate General Employees using Bettercap

-Device Hijacking & Botnet Creation against Corporate General Employees using Custom Built Botnet Trojans

*Remote/Social Engineering Internal Network(s):*

-Email phishing against Corporate General Employees & Store General Network Managers using Metasploit Framework

-Phone phishing against Corporate General Employees & Store General Network Managers using Metasploit Framework

*Remote/SIEM Response Internal Network-level:*

-Distributed Denial of Service (DDoS) of Managers' Workstations at all six GCC locations, using Exploited network infrastructure as Zombie Machines

-Active Scanning/Reconnaissance & Port enumeration using NMAP scanning against Corporate IT Network

-Patch Management Exploitation of Corporate IT Network infrastructure using Metasploit Framework

-Point of Sale (POS) Trojan Installation on CDE POS Network hosts using GCC's persistent VPN connection to Corporate.

**Expected Outcomes**

The TTPs employed in this test have overlapping features by design. Absolute security is not a realistic outcome in the current threat landscape: A determined threat actor only needs to find one flaw to breach a network, while defenders have to block every attempt 100% of the time. The Red Team's tools are primarily open-source and updated frequently by a thriving development community. GCC is trending in the right direction: With malware attacks and breaches announced at an incredible pace, a proactive mindset to Cybersecurity is a valuable commodity. The rationale for the TTPs used in this test follows:

-*Passive Recon via Google Dorks:* When an attacker uses passive reconnaissance techniques, they do not interact with the target directly. Instead, the attacker relies on publicly available information, news releases, or other no-contact methods. Google hacking refers to using advanced Google search operators to create complex search queries to extract sensitive or hidden information. Attackers then use the accessed information to find vulnerable targets. Using advanced Google hacking techniques, Footprinting involves locating specific text strings within search results using advanced operators in the search engine (Ethical Hacking Essentials: Academia Series).

-*Passive Recon via WhoIs Lookup*: By entering the target's domain or IP address. The domaintools.com service provides Whois information such as registrant information, email, administrative contact information, creation and expiry date, and a list of domain servers. SmartWhois, available at hp://www.tamos.com, gives information about an IP address, hostname, or domain, including information about the country, state or province, city, phone number, fax number, name of the network provider, administrator, and technical support contact information. It also helps in finding the owner of the domain, the owner's contact information, the owner of the IP address block, and the registered date of the domain. A vast wealth of knowledge is readily available for misuse without the targeted individual's knowledge (Ethical Hacking Essentials: Academia Series).

*- Passive Recon via Network Sniffers & Packet Analyzers such as dSniff Suite, NMAP & Wireshark:* Network sniffers allow surreptitious information gathering and network mapping of intended targets without his knowledge. dSniff is the Swiss army knife of privacy invasion. Attackers can gain a foothold on an intended network by using dSniff to perform ARP poisoning attacks. The attack allows the impersonation of legitimate users. The package ships with a handful of nasties: urlsnarf (to keep track of websites your network users are visiting), msgsnarf (to keep track of the instant messenger sessions of users on your LAN), mailsnarf (to keep track of the emails that users of your network are receiving), web spy (to follow a users web-surfing in realtime), dSniff (to capture user passwords for quite a few protocols), filesnarf (to capture NFSfiles), sshmitm (to launch a man-in-the-middle attack against SSH), etc. It can wreak havoc when used for illegitimate purposes, but it is a valuable tool in the hands of a capable systems administrator (Dhar)

Wireshark is a powerful packet capture and analysis tool. Wireshark lets you capture and interactively browse the traffic running on a computer network. This tool uses WinPcap to capture packets on supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. The captured files can be programmatically edited via the command line. A set of filters for customized data display can be refined using a display filter. As shown in the screenshot, attackers use Wireshark to sniff and analyze the packet flow in the target network and extract critical information about the target. (EHE 21)

NMAP: Nmap ("Network Mapper") is a network exploration and hacking security scanner. It allows you to discover hosts, ports, and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. It scans vast networks of literally hundreds of thousands of machines. Nmap includes many mechanisms for port scanning (TCP and UDP), OS detection, version detection, ping sweeps, etc. A security professional or an attacker can use this tool for specific needs (Ethical Hacking Essentials: Academia Series).These Passive Recon TTPs allow attackers to stalk an intended target and efficiently attack any vulnerable ports, etc. If GCC's internet-facing infrastructure has any gaps, they would be transversed.

*Key Reinstallation Attack (KRACK) against Corporate General Employees using the Aircrack-ng suite*: The key reinstallation attack (KRACK) represents an enormous risk vector that GCC must attempt to mitigate. The attack exploits the flaws in the implementation of the four-way handshake process in the WPA2 authentication protocol, which is used to establish a connection between a device and an AP. All secure Wi-Fi networks use the four-way handshake process to establish connections and generate a new encryption key that will be used to encrypt the network traffic.

The attacker exploits the four-way handshake of the WPA2 protocol by forcing Nonce reuse. In this attack, the attacker captures the victim's ANonce key that is already in use to manipulate and replay cryptographic handshake messages. This attack is perilous and could lead to immediate compromise of GCC infrastructure. This attack works against all modern protected Wi-Fi networks (both WPA and WPA2); personal and enterprise networks; and the ciphers WPA-TKIP, AES-CCMP, and GCMP. It allows the attacker to steal sensitive information such as credit card numbers, passwords, chat messages, emails, and photos. Any device that runs Android, Linux, Windows, Apple, OpenBSD, or MediaTek is vulnerable to some variant of the KRACK attack (Ethical Hacking Essentials: Academia Series).

-*Evil Twin/Rogue AP against Corporate General Employees using Hak5 Wi-Fi Pineapple*: Many wireless software tools and Access Points (APs) allow setting user-defined values for the MAC addresses and SSIDs of AP devices. An attacker can spoof the MAC address of the AP by programming a rogue AP to advertise the same identity information as that of the legitimate AP. An attacker connected to the AP as an authorized client can have full access to the network (Ethical Hacking Essentials: Academia Series). This threat vector represents a substantial risk for GCC because legitimate users on the Corporate Wi-Fi network likely would not notice. This threat is yet another method of gaining a foothold on the GCC network without setting triggering alarms.

*-Bluetooth Man in the Middle (MITM)/Impersonation attack against Corporate General Employees using Bettercap*: This attack has a lower probability of success because it relies on the victim enabling Bluetooth, but the severity is just as crucial. In a MITM/impersonation attack, attackers manipulate the data transmitted between devices communicating via a Bluetooth connection. During this attack, the devices intended to pair with each other unknowingly pair with the attacker's device, thereby allowing the attacker to intercept and manipulate the data (Ethical Hacking Essentials: Academia Series). If any GCC staff have Bluetooth enabled - as many people traditionally do - attackers could secretly exploit this to spy on anyone within range of the device. GCCs critical business intelligence could be disclosed and exposed.

*Device Hijacking & Botnet Creation using Botnet Trojans*: Most major information security attacks involve botnets. Attackers use botnet Trojans to infect many computers throughout a large geographical area to create a network of bots that can achieve control via a command-and-control (C&C) center. They trick regular computer users into downloading Trojan-infected files to their systems through phishing, SEO hacking, URL redirection, and other means. Once the user downloads and executes this Botnet Trojan in the system, it connects back to the attacker using IRC channels and waits for further instructions (Ethical Hacking Essentials: Academia Series). The purpose of creating a botnet in this test is to overwhelm the resources of the IT department with incident management duties while distracting them from the actual exploitation that will soon follow. At this point, the GCC IT staff would have various incidents to respond to, leaving them less able to mount an effective defense. While busy, their systems would be scanned for unpatched vulnerabilities, using active scanning and log deletion to clear their tracks.

*Social Engineering via email & phone scams*: Social engineering is one of the hardest threat vectors to defend against because of the myriad ways it can be deployed. Social engineering is the art of manipulating people to divulge sensitive information to use it to perform some malicious action. Despite security policies, attackers can compromise an organization's sensitive information by using social engineering, which targets people's weaknesses. Most often, employees are unaware of a security lapse on their part and inadvertently reveal the organization's critical information. Attackers could remotely target GCC Corporate employees and managers, pretending to be tech support dealing with incident response. A successful campaign would lead to extracting sensitive information. Social Engineering is yet another Persistence technique that allows malicious individuals to maintain prior access credentials and gain new ones to exploit.

*Point of Sale (POS) Trojan Installation on CDE POS Network* As the name indicates, point-of-sale (POS) Trojans are a type of fraudulent financial malware that target POS and payment equipment such as credit card/debit card readers. Attackers use POS Trojans to compromise such POS equipment and grab sensitive information regarding credit cards, such as credit card numbers, holder names, and CVV numbers (Ethical Hacking Essentials: Academia Series). The Payment Card Industry Data Security Standard was designed as a comprehensive list of best practice measures and processes for handling, processing, storing, and transmitting payment card data. The PCI DSS was formulated by the payment card companies such as Visa and Mastercard in response to the growing number of theft and misuse of payment card details. The first version of the PCI DSS was released in December 2004 and mandated a wide range of measures required to protect payment card data (Kedgley). Installing malware on GCC store infrastructure via the Corporate VPN represents a massive compliance failure that could be financially ruinous. This attack is particularly troublesome because VPNs inherently shield user activities online.

**Post Attack Remediation & Reporting**

Following a penetration test, a report is written specifically to the type of network penetration test performed for the client that details the process, the vulnerabilities and evidence collected, and recommendations for remediation. A data owner needs to understand the risk to their business that the vulnerabilities pose, and it is the job of the pen tester to provide them with a risk analysis that assists them in making the appropriate decision. Remediation may include implementing patches and updates. However, if internal vulnerabilities exist, it can also include implementing specific policies like Employee Use policies and IT Security policies. A successful network penetration test is not just one in which a successful breach occurs. If the tester cannot breach the network, it validates that the organization's current security posture is sufficient to deter, detect, or prevent attacks (Firch).

Works Cited

Dhar, Sumit. *Sniffers: Basics and Detection*. www.just.edu.jo/~tawalbeh/nyit/incs745/presentations/Sniffers.pdf.

*Ethical Hacking Essentials: Academia Series*. EC-Council, 2021.

Firch, Jason. “How to Perform a Successful Network Penetration Test.” *PurpleSec*, 10 Oct. 2022, purplesec.us/network-penetration-test.

Kedgley, Mark. *2016 Threat Predictions and Top Ten Cyber Security Tips to Keep You Safe*. 2016, www.newnettechnologies.com/whitepaper/NNT-Threat-Predictions-and-Top-Ten-Cyber-Security-Tips-Whitepaper.pdf.

Temple-Raston, Dina. “A ‘Worst Nightmare’ Cyberattack: The Untold Story of the SolarWinds Hack.” *NPR.org*, 16 Apr. 2021, www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

Vankirk, Shelby. “Internal and External Network Penetration Testing.” *EC-Council Cybersecurity Exchange*, 29 Sept. 2022, www.eccouncil.org/cybersecurity-exchange/penetration-testing/network-penetration-testing.