The Art of Cyber War: Understanding and Defending Against Modern Threats

Bruce Tyson

An Introduction to

BRUCE TYSON

Once upon a time, an IT director was tasked with creating a complex spreadsheet. To save time, this person downloaded a Microsoft Excel extension that simplified the task.

The extension contained an embedded virus which spread across the network, infecting every machine, displaying porn and downloading files.

Embarrassing and damaging, the mess took over a week to clean up. How do I know? I was that IT director.

Years later, I recall that experience as my personal introduction to cybersecurity. Not only have I amassed more that a decade of real-world security experience, but I have achieved mastery in the cybersecurity industry.

I earned the CompTIA Advanced Security Practitioner credential, the highest certification offered by that industry trade organization.

To support my work, I have earned the Product Management Professional (PMP) credential from the Project Management Institute (PMI).

Join me in the following pages to explore real-world cybersecurity threats along with an overview of their prevention.

The Art of Cyber War: Understanding and Defending Against Modern Threats

The Art of Cyber War: Understanding and Defending Against Modern Threats

By Bruce Tyson

The Art of Cyber War

Published in USA by CPG Publishing, SC

Published 2024

I dedicate this book to the millions of hackers out there who keep me on my toes.

Table of Contents

“In cybersecurity, the more you know, the safer you will be.”

- Unknown

Introduction

In today's world, where technology has become an integral part of our daily lives, the threat of cyber attacks looms large.

As a security expert with years of experience in the field, I have witnessed the evolution of these digital threats and the devastating consequences they can have on individuals, businesses, and governments alike.

In "The Art of Cyber War," I delve deep into the world of cyber attacks, exploring their various forms, some real-life scenarios, and suggestions for defending against them. I provide an overview of the current threat landscape and the strategies that organizations can employ to protect themselves from these ever-evolving dangers.

This book is a guide for security professionals and business owners who need an introduction to cybersecurity. It is an eye-opening read for anyone concerned about the safety of their personal and professional data.

By understanding the nature of cyber attacks and the tactics used by malicious actors, we can better defend ourselves against these threats and safeguard our digital world from the relentless onslaught of cyber criminals.

Man in the Middle

When a wire sent between an Israeli startup and a Chinese venture capital firm, IT experts were alerted to a serious problem: a Man in the Middle attack had resulted in a large financial loss, This case showed

> A man in the middle attack whereby every email sent by each side of the exchange was in reality sent to the attacker, who then edited the emails to include bogus information and banking details, then forwarded them from each lookalike domain to its original destination. (Bode)

> Resulting from the successful MitM attack, hackers fraudulently obtained $1 million. The attack also involved domain spoofing using "lookalike domains."

Also known as a "Person in the Middle" or "Adversary in the Middle" attacks Man-in-the-Middle (MitM) attacks involve an attacker positioning themselves between the communicating parties, making it appear as if they are communicating directly with each other, while the attacker secretly intercepts and potentially alters the messages exchanged.

MitM attacks can be carried out in various ways, such as intercepting Wi-Fi traffic or hijacking a session using a malicious server.

The attacker can use the intercepted information for various malicious purposes, such as stealing sensitive data, spreading malware, or phishing for login credentials. To protect against MitM attacks, users should implement secure communication protocols, such as HTTPS, and avoid connecting to public or unsecured Wi-Fi networks. Addition-

ally, using a Virtual Private Network (VPN) can help secure internet traffic and prevent attackers from intercepting communications.

Businesses can avoid MITM attacks using several precautionary measures:

- Verification via phone call.
- Retain logs.
- Secure email infrastructure.
- Use security tools to detect URL hijacking attempts.

MITM attacks fall under the broader category of interception attacks.

12

Bruce Tyson

Directory Traversal

Also known as a "path traversal attack," directory traversal involves an attacker who accesses "files and directories that are stored outside the web root folder" ("Path Traversal | OWASP Foundation").

A famous directory traversal attack successfully compromised the Jira help desk application. Also known as CVE-2019-14994,

> The...vulnerability allows an attacker, if able to access the customer portal, to traverse to the administrative portal and view issues within all Jira projects contained in the vulnerable instance. This could include Jira Service Desk projects, Jira Core projects, and Jira Software projects.(Sam Curry).

CVE-2021-41773, a path traversal exploit aimed at Apache web servers, allows attackers to map URLs to files outside the directories configured by Alias-like directives" (Surana). The attack installed Minero mining malware via the GitHub and Netlify repositories. Security experts have logged almost 3 million attempts to exploit this vulnerability. According to Imperva,

> The exploit allows an attacker to access restricted directories, execute commands, and view data outside of the web root folder where application content is stored.

Addressing Directory Traversal threats involves several counter measures:

- Inspecting internet traffic.
- Implementing security rules to block attackers.
- Signature analysis.
- Machine learning.
- Geo-IP blocking.

Bruce Tyson

Cross-Site Scripting

CVE-2023-6000 affected WordPress in March 2024, via a plugin called Popup Builder. Hackers used cross-site scripting (XSS) to affect at least 3,300 websites by compromising (Toulas).

In 2019, Fortnite, a massively popular multiplayer game, was found to have an XSS vulnerability that compromised the security of over 200 million users. The flaw was discovered in a retired, unguarded webpage, which allowed attackers to gain unauthorized access to user data. If this vulnerability had been combined with an insecure single sign-on (SSO) issue, hackers could have potentially redirected users to a counterfeit login page, stealing virtual currency and recording player conversations for potential future attacks ("Fortnite's 2019 XSS Vulnerability | Gab AI | an Uncensored and Unfiltered AI Platform") .

XSS is a vulnerability that allows an attacker to inject malicious scripts (usually JavaScript) into web pages viewed by other users. These scripts execute in the victim's browser, compromising their session, stealing sensitive data, or performing other malicious actions. Defending against XSS may involve one or more measures:

- **Exercise caution** while inserting untrusted or user-inserted data.

- **Input validation** and filtering against allowable values.
- **Output encoding** that prevents the use of active content.
- **Choosing** frameworks with care.
- **Setting** the HttpOnly flag.

Bruce Tyson

Cross-site request forgery (CSRF)

Cross-Site Request Forgery (CSRF) is a web security vulnerability that occurs when an attacker tricks a user into unknowingly performing actions on a trusted website. Here's how it works:

User Authentication: The web application authenticates the victim (e.g., logs them in).

Malicious Request: The attacker sends a request (e.g., via a link in an email or chat) that forces the victim's browser to perform an action on the trusted site.

State-Changing Actions: CSRF attacks target actions that change the server's state, such as transferring funds, changing email addresses, or making purchases.

Impact: If successful, CSRF can compromise user accounts or even the entire application.

Attackers used CSRF against TikTok in a well-known 2020 incident. Hackers caused the accounts of other users to send requests on their behalf (Dizdar).

Prevention Measures:

- **Use built-in CSRF protection in frameworks** (e.g., Joomla, Spring, Ruby on Rails).
- **Implement CSRF tokens** to validate requests.
- **Educate users** about safe browsing practices.

Virtual Machine (VM) Hopping

Virtual Machine Hyper Jumping (VM Jumping) is an attack method that exploits the hypervisor's weakness, allowing one virtual machine (VM) to be accessed from another. Essentially, it breaks the isolation between VMs that typically operate as separate entities. When successful, an attacker can compromise the VM's separation and protections, gaining access to the host computer, the hypervisor, and other VMs. People also refer to this technique as virtual machine guest hopping.

Real-life news stories about Virtual Machine hopping do not seem to exist. To compensate for that, I will explain how VM hopping works.

- **Double tags:** The attacker connects to an interface in access mode with the same VLAN as the native untagged VLAN on the trunk. They send a frame with two 802.1Q tags: the "inner" VLAN tag (the target VLAN) and the "outer" VLAN tag (the native VLAN). The switch removes the first (native VLAN) tag and forwards the frame with the second tag on its trunk interface, effectively "jumping" from the native VLAN to the victim's VLAN (Molenaar).

- **Switch spoofing:** The attacker sends Dynamic Trunking Protocol

(DTP) packets to negotiate a trunk with the switch. If the switch uses the default “dynamic auto” or “dynamic desirable” switchport mode, the attacker gains access to all VLANs. This misconfiguration should be avoided (Molenaar).

To prevent VM hyper jumping, consider:

- Using secure operating systems.
- Up-to-date security patches.
- Network segmentation techniques.
- Separate web-facing traffic from database traffic to prevent direct access between virtual machines.
- Use private VLANs to hide VMs and configure the gateway to communicate only with the gateway.

Bruce Tyson

Injection Attacks

An **injection attack** refers to a broad class of attack vectors sometimes referred to as "fabrication attacks" (McClanahan). In this type of attack, an attacker supplies untrusted input to a program. An interpreter then processed the input as part of a command or query, which ultimately alters the execution of the program. These attacks are particularly dangerous because they can lead to data theft, loss of data integrity, denial of service, and even full system compromise. The most common types of injection attacks include:

1. **SQL Injection (SQLi)**: The attacker injects malicious SQL code into a web application, potentially gaining unauthorized access to databases or executing arbitrary SQL commands.
2. **Cross-site Scripting (XSS)**: The attacker injects arbitrary scripts (usually JavaScript) into a legitimate website or application, which then executes inside the victim's browser. This can lead to account impersonation, defacement, or other security risks.
3. **Code Injection**: The attacker injects application code written in the application language. This code may be used to execute operating system commands with the privileges of the user running the web application, potentially leading to full system compromise.

4. **CRLF Injection**: The attacker injects unexpected CRLF (Carriage Return and Line Feed) characters to manipulate HTTP responses, potentially combining this with XSS attacks.
5. **Email Header Injection**: Similar to CRLF injections, this attack targets mail servers and can lead to spam relay or information disclosure.
6. **LDAP Injection**: The attacker injects LDAP (Lightweight Directory Access Protocol) statements to execute arbitrary LDAP commands.

Preventing injection vulnerabilities involves proper input validation, using prepared statements, and escaping user input to ensure secure execution of commands and queries. Regular security testing and awareness are crucial to safeguard against these risks.

Bruce Tyson

Interception Attacks

An interception attack occurs when a malicious actor intercepts and monitors communication between two parties without their knowledge. Essentially, it's like eavesdropping on conversations or data transmissions.

The attacker may gain unauthorized access to sensitive information such as passwords, financial data, or personal messages[2]. For instance, attackers can compromise critical data through techniques like packet sniffing and man-in-the-middle attacks.

To mitigate interception attacks, consider encrypting communications, avoiding untrusted Wi-Fi networks, and keeping your software up to date.

Interceptions differ from man-in-the-middle (MITM) attacks in that:

- In an interception attack, a malicious actor gains unauthorized access to private or confidential information.
- Common techniques include packet sniffing and eavesdropping.
- The attacker aims to obtain critical data (such as passwords or credit card numbers) or disrupt data exchanges on the network.

- Data confidentiality is the primary concern.

Types of interception attacks include:

Session Hijacking: This attack involves the attacker stealing a user's session ID, allowing them to impersonate the user and gain unauthorized access to their account.

Sniffing: Also known as packet sniffing, this involves the attacker using a packet sniffer tool to intercept and analyze data packets being transmitted over a network.

Rogue Wi-Fi Access Point: In this attack, the attacker sets up a fake Wi-Fi access point, tricking users into connecting to it. The attacker can then intercept and monitor the victim's internet traffic.

ARP Spoofing: This attack involves the attacker sending false ARP (Address Resolution Protocol) messages over a local network, causing traffic to be redirected to the attacker's machine.

DNS Spoofing: In DNS spoofing, the attacker alters the DNS records, redirecting traffic from the legitimate website to a malicious one.

Strategies to address interception attacks include avoiding untrusted Wi-Fi networks and installing software updates as they become available.

Email Spoofing

In November 2016, Belgian Crelan Bank suffered from an email spoofing attack that cost the bank more than €70 million. Carrying out the attack involved sending messages that appeared to come from bank executives, including the CEO. Everything about the emails looked legitimate and contained instruction for money transfers which were both urgent and confidential.

Employees receiving the spoofed emails followed the instructions in the emails, resulting in transferring funds to illicit accounts.

Attacks similar to the Crelan Bank incident continue to this day (and will likely continue into the indefinite future). Email spoofing attacks cause losses to businesses of every size.

Email spoofing is a deceptive technique employed by cyber attackers to manipulate the sender's email address, making it appear as though the message originated from a trusted or legitimate source. This malicious act is achieved by altering the 'From,' 'Reply-To,' or 'Return-Path' fields in the email header to deceive the recipient into believing the message is genuine and safe.

Attackers often exploit email spoofing to conduct phishing scams, aiming to trick recipients into divulging sensitive information or downloading

malicious content. The attacker's objective is to exploit the trust associated with the spoofed email address to deceive and manipulate the recipient into taking actions that can result in financial loss, identity theft, or the compromise of corporate or personal data.

Methods of defending against email spoofing attacks include:

- **Verification Procedures:** Always verify unusual requests through alternative communication channels.
- **Email Security:** Implement advanced email security measures to detect and block spoofed emails.
- **Employee Training:** Regularly train employees on recognizing and responding to phishing and spoofing attempts.
- **Monitoring:** Continuously monitor financial transactions for unusual activity.

Credential Stuffing

Criminals stole millions of user recoords from the genetic testing firm 23andMe in 2023. They used credential stuffing to gain access to 23andMe servers.

Credential stuffing is a type of cyberattack where attackers use automated systems to input stolen usernames and passwords into multiple websites to gain unauthorized access to user accounts.

Attackers acquire extensive lists of usernames and passwords from dat breach databases, phishing campaigns, and sources on the dark web. They then use credential stuffing tools to automatically test each credential to log into a website or application.

Email spoofing works because many people use the same username and password on multiple sites.

Once hackers get access to a site, they take over victim accounts to perform fraudulent transactions and other malicious activities.

Businesses can use practical measures to defend against credential stuffing attacks:

- **Multi-Factor Authentication (MFA):** Requiring additional verification beyond just a password makes it much harder for attackers to gain access, even if they have valid credentials.
- **Rate Limiting and IP Blocking:** Implementing rate limits and blocking IP addresses after multiple failed login attempts can hinder automated attacks.
- **Credential Screening:** Use services that check if user credentials have appeared in known breaches and prompt users to change their passwords if so.
- **Password Hygiene:** Encourage and enforce strong, unique passwords for each site. Password managers can help users manage different passwords for different accounts.
- **Behavioral Analysis:** Implement systems that analyze login patterns and detect unusual behavior, such as multiple login attempts from different locations in a short time.
- **CAPTCHA:** Deploy CAPTCHA challenges after a certain number of failed login attempts to prevent automated bots from continuing.
- **User Education:** Educate users on the dangers of reusing passwords across multiple sites and the importance of enabling MFA.

Bruce Tyson

Denial of Service

A Denial of Service (DoS) attack is a malicious attempt to overwhelm a target system or network with excessive traffic or requests, rendering it incapable of providing services to its intended users. This can be achieved by exploiting vulnerabilities in the system or by flooding it with bogus traffic.

There are two main types of DoS attacks: single-source and distributed. In a single-source attack, the attacker uses a single machine to generate a high volume of traffic or requests, while in a distributed attack, multiple compromised systems (botnets) are used simultaneously to amplify the attack's impact. The primary goal of a DoS attack is to disrupt normal operations and cause financial losses or reputational damage to the targeted organization.

An exceptional denial of service attack occurred in the context of the 2024 European elections.

> The European Parliament elections are already underway in the Netherlands and are set to begin in 26 more countries across the EU over the coming days, igniting politically motivated cyberattacks (Toulas).

Experts blamed that on Russian hactivism by an emerging hacking

group.

In another example of a DoS attack, experts uncovered a large botnet using AndroidTV boxes that hackers used to launch distributed denial of service attacks (Toulas).

To defend against a Denial of Service (DoS) attack, several measures can be implemented:

- **Use a Content Delivery Network (CDN):** A CDN distributes your website's content across multiple servers, reducing the risk of a single server being overwhelmed by excessive traffic.

- **Implement rate limiting:** This involves setting a limit on the number of requests a single IP address can make within a specific timeframe, preventing a single source from flooding your system.

- **Use a DoS mitigation service:** These services are designed to detect and filter out malicious traffic, allowing legitimate traffic to reach your systems.

- **Update and patch your systems regularly:** Ensuring that your systems are up-to-date with the latest security patches can help prevent attackers from exploiting known vulnerabilities.

- **Implement firewalls and intrusion detection systems:** These tools can help monitor and block suspicious traffic, providing an additional layer of protection against DoS attacks.

- **Have a backup plan:** In the event of a successful DoS attack, hav-

ing a disaster recovery plan in place can help minimize downtime and financial losses.

Authentication Bypass

When Apple released a biometric lock on iPhones which required a fingerprint to open the phone, people felt safe. In reality, however, hackers could readily bypass TouchID and gain access to the phone's contents. The hacker bragged to the website Ars Technica of how easily he could bypass Apple's authentication (Goodin).

Hackers use authentication bypass to can gain unauthorized access to a system or application without providing the required credentials. This can occur due to flaws in the authentication mechanism, such as weak or improperly implemented algorithms, or through the exploitation of vulnerabilities in the system's architecture.

Successful authentication bypass attacks can lead to unauthorized data access, modification, or deletion, as well as the potential for further system exploitation. As an information technology professional, it is crucial to ensure that all authentication mechanisms are properly implemented and regularly audited to prevent such vulnerabilities from being exploited.

To defend against an authentication bypass attack, consider implementing the following measures:

- **Use strong, well-implemented authentication mechanisms:** Ensure that your authentication system employs secure algorithms, such as bcrypt or scrypt, and is properly configured to prevent unauthorized access.

- **Regularly audit and update your authentication systems:**

Keep your authentication mechanisms up-to-date with the latest security patches and best practices to prevent vulnerabilities from being exploited.

- **Implement multi-factor authentication (MFA):** Requiring users to provide multiple forms of authentication, such as a password and a one-time code, can significantly reduce the risk of unauthorized access.

- **Monitor system logs and alerts:** Regularly review logs and alerts generated by your authentication systems to identify any suspicious activity or unauthorized access attempts.

- **Conduct regular security assessments and penetration testing:** Engage in regular assessments of your systems to identify and address potential vulnerabilities before they can be exploited.

- **Educate users on security best practices:** Ensure that users are aware of the importance of strong passwords, MFA, and other security measures to help prevent unauthorized access.

Supply Chain Attacks

A supply chain attack is a type of cyberattack in which an attacker targets a vulnerable component within a software or hardware supply chain to compromise the security of the final product or service. This can involve the manipulation of source code, the introduction of malicious components, or the exploitation of vulnerabilities in third-party dependencies.

When a business operates with good cybersecurity hygiene, hackers may attempt to gain access to their data through a supplier with poor cybersecurity practices. Criminals often choose supply chain attacks because they can access the data of many businesses through one supplier.

In 2024, hackers used a supply chain attack to cripple multiple British hospitals. Rather than directly attacking those health facilities, the criminals attacked a service provider, Synnovis. That company supplied pathology services and proved to have weak cybersecurity. Because of the attack, hospitals were forced to cancel an unspecified number of health-related procedures (Thomas et al.).

- **Implement Honeytokens:** These fake resources act as tripwires, alerting your organization to suspicious activity. When attackers interact with honeytokens, you receive advanced warnings and insights into their methods (Kost).

- **Secure Privileged Access Management:** Limit access to

critical systems and data. Regularly review and revoke unnecessary privileges.

- **Implement a Zero Trust Architecture (ZTA):** Assume no one is trustworthy by default. Verify and authenticate all access requests, even from trusted sources.

- **Make Cybersecurity Part of Organizational Culture:** Educate employees and vendors about security best practices. Foster a security-conscious mindset throughout your supply chain (Pecha).

Social Engineering

Social engineering is a technique used by cybercriminals to manipulate individuals into divulging sensitive information or performing actions that compromise the security of a system or organization. This can involve tactics such as phishing, pretexting, baiting, or tailgating, which rely on human psychology and trust to deceive victims. Social engineering attacks can be highly effective, as they exploit the weakest link in any security system: the human element.As an information technology professional, it is essential to educate users on the risks associated with social engineering attacks and to implement security measures, such as user training and access control, to help prevent successful attacks.

Below, you will see 10 types of social engineering. I intend to use this list for informational purposes. Other types of social engineering exist.

Phishing - "a type of cybercrime where attackers use various methods, such as fake emails or websites, to deceive individuals into providing sensitive information, like passwords or credit card details. The primary goal is to steal personal and financial data for malicious purposes" ("Phishing Definition | Gab AI | an Uncensored and Unfiltered AI Platform").

Whaling - "a strategic phishing attack, targeted towards high profile executives, that is disguised as a permitted email. An attacker can prod the target for information that helps them access sensitive areas of the network, passwords, or other user information" ("What Is a Whaling Attack? Examples and Statistics | Fortinet").

Baiting. A baiting attack exploits human nature by offering fake prizes or enticing opportunities to steal information or infect devices with malware. These attacks can occur online or offline.

Diversion Theft - "a cyberattack that originally occurred offline. In this scheme, a thief persuades a courier to pick up or drop off a package in the wrong location, deliver an incorrect package, or hand it to the wrong recipient. Over time, this tactic has also been adapted for online attacks, where cyber actors intercept and divert deliveries through digital means" ("Define Baiting Cyber Attack – Bing").

Business Email Compromise (BEC). - "Business email compromise (BEC)—also known as email account compromise (EAC)—is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business—both personal and professional" ("Business Email Compromise ").

Smishing - phishing via SMS, iMessage, or similar text messaging.

Quid Pro Quo - scam that involves the attacker posing as a legitimate entity, such as a company or government official, in order to persuade the victim to divulge sensitive information or perform a specific action. The attacker typically offers something of perceived value, like a prize or service, in exchange for the requested information or action.

Pretexting. - "Pretexting is a social engineering attack where the attacker creates a fabricated identity or scenario to persuade a victim to divulge confidential information, grant access to restricted systems, or perform actions they would otherwise not undertake" ("Pretexting") .

Tailgating/Piggybacking - an attack where unauthorized individuals follow authorized individuals into a restricted area. This could involve

main entrances, server-room entrances, or other sensitive locations.

In March of 2024, a construction company, Ryan Construction became a victim of social engineering. The case represents an unusual news story featuring whaling.

Incidentally, this cyber attack also involved a supply chain attack.

A hackers used whaling to redirect a large payment to Beck Properties to their own accounts.

> The payment was supposed to cover construction expenses for a new office and warehouse in South St. Paul. Instead, the project's developer, Beck Properties Minnesota, has been hit with more than $530,000 in liens by subcontractors who weren't paid for their work (Hughlett) .
>
> According to the suit: Rick Beck, one of Beck Properties' principals, received a billing notice via email from a Ryan project manager. A few hours later, he received another email "purporting" to be from the same Ryan executive.

To shorten a long story, the principal of Beck Properties approved the payment of $735,000 to Ryan Construction, which went to an unknown account.

Combatting social engineering of all types may involve several preventative measures:

- **Conduct regular security awareness training:** Educate your employees about the different types of social engineering attacks and how to identify and report them.

- **Implement strict access control policies:** Limit access to sensi-

tive data and systems to only those employees who need it for their job functions.

- **Use strong authentication methods:** Implement multi-factor authentication (MFA) and strong password policies to prevent unauthorized access to your systems.

- **Keep your systems up to date:** Regularly update your operating systems, applications, and security software to patch known vulnerabilities.

- **Monitor network activity:** Implement intrusion detection systems (IDS) and security information and event management (SIEM) tools to monitor your network for suspicious activity.

- **Encrypt sensitive data:** Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.

- **Implement email security measures:** Use email filtering and anti-phishing tools to block malicious emails and prevent employees from clicking on phishing links.

- **Conduct regular security audits:** Perform regular security audits to identify and address vulnerabilities in your systems and processes.

Develop an incident response plan: Create a plan that outlines the steps to take in the event of a security incident, including how to contain the attack and restore normal operations.

- **Foster a culture of security:** Encourage employees to report suspicious activity and create an environment where security is a shared responsibility.

- **Use a mantrap** a configuration that requires two sets of controlled-access doors to prevent tailgating attacks.

VLAN Hopping

VLAN hopping is a technique used by attackers to gain unauthorized access to different Virtual Local Area Networks (VLANs) within a network. VLANs are used to segment a network into multiple logical networks, allowing for better security, management, and performance. VLAN hopping can be achieved through various methods, including:

- **Switch spoofing:** Attackers can mimic a switch by sending spoofed VLAN tags to a switch, which can cause the switch to forward traffic from one VLAN to another.

- **Double tagging:** Some switches are vulnerable to double tagging attacks, where an attacker sends a packet with two VLAN tags. The first tag is stripped by the switch, and the second tag is used to access a different VLAN.

- V**LAN Trunking Protocol (VTP) attacks:** VTP is a protocol used to manage VLAN configurations across multiple switches. Attackers can exploit vulnerabilities in VTP to gain access to other VLANs.

- **Rogue DHCP server:** Attackers can set up a rogue DHCP server on the network, which assigns VLAN tags to clients, allowing them to access unauthorized VLANs.

To protect your network from VLAN hopping attacks, implement the following security measures:

- Configure switches to only allow authorized VLANs on specific ports.

- Disable unnecessary VLAN features, such as VTP and VLAN tagging on untrusted ports.

- Use port security to limit the number of MAC addresses allowed on a port.

- Monitor network traffic for unusual activity and implement intrusion detection systems (IDS) to detect and prevent VLAN hopping attempts.

Route Hijacking

Route hijacking, also known as BGP hijacking, is a type of cyber attack in which an attacker illegitimately takes control of Internet traffic by manipulating the Border Gateway Protocol (BGP) routing tables.

BGP is the protocol used by Internet Service Providers (ISPs) and other network operators to exchange routing information and determine the best paths for sending data packets across the Internet.

In a route hijacking attack, the attacker falsely advertises a more specific or more preferable route to a destination network, causing other routers to update their routing tables and redirect traffic to the attacker's network.

This can result in traffic being intercepted, monitored, or tampered with by the attacker. There are several types of route hijacking attacks:

Malicious hijacking: An attacker intentionally hijacks a route to intercept, modify, or block traffic for nefarious purposes, such as espionage, surveillance, or financial gain.

- **Accidental hijacking:** A network operator inadvertently advertises incorrect routing information, causing traffic to be misdirected to the wrong network.

- **Resource exhaustion:** An attacker overwhelms a target network by attracting a large amount of traffic, causing performance issues or even a complete network outage.

To protect against route hijacking attacks, network operators should implement the following security measures:

- **Implement BGP security features**, such as Resource Public Key Infrastructure (RPKI) and BGPsec, to validate the authenticity and integrity of routing information.

- **Monitor BGP routing tables** for suspicious activity and implement automated tools to detect and mitigate route hijacking attempts.

- **Maintain accurate and up-to-date routing information** to prevent accidental hijacks.

- **Implement network redundancy and failover mechanisms** to minimize the impact of route hijacking attacks on network availability and performance.

Bruce Tyson

Phishing

Phishing is a social engineering technique used by cybercriminals to deceive individuals into divulging sensitive information, such as login credentials, credit card details, or personal identification numbers. This is typically achieved through the use of fraudulent emails, text messages (smishing), voice calls (vishing), or websites that appear to be from legitimate sources, such as banks, government agencies, or well-known companies.

The attacker's goal is to trick the victim into providing the requested information, which can then be used for financial gain or other malicious purposes. As an information technology professional, it is crucial to educate users on the risks associated with phishing attacks and to implement security measures, such as email filtering and user training, to help prevent successful attacks.

LastPass, a leading password manager suffered a supply chain hack in November 2022 (Hill). During the following December, the company suffered from another brutal attack (Demers). The story continues into 2024 when LastPass users became victims of a sophisticated phishing campaign that tricked users into revealing their master password, compromising all their passwords saved in LastPass (Goodin).

Interestingly, the hackers who attacked LastPass did not need much expertise because the needed tools were sourced via a prebuilt phishing “kit”

available online, called CryptoChameleon. The attack used a sequence of smishing, vishing, and phishing to create an atmosphere destined to deceive many LastPass users.

LastPass and thousands of other businesses and millions of victims comprise the list of phishing victims. To defend against smishing, vishing, and phishing attacks, follow these best practices:

- **Educate yourself and your employees:** Learn to recognize the signs of phishing attacks, such as suspicious links, attachments, or requests for sensitive information.

- **Verify the sender:** Before clicking on any links or downloading attachments, verify that the sender is legitimate. Check the sender's email address, phone number, or website URL for any inconsistencies or suspicious elements.

- **Be cautious with attachments and links:** Avoid clicking on links or downloading attachments from unknown or suspicious sources. If you must open an attachment, scan it with antivirus software first.

- **Use strong authentication methods:** Implement multi-factor authentication (MFA) and strong password policies to protect your accounts from unauthorized access.

- **Keep your systems up to date:** Regularly update your operating systems, applications, and security software to patch known vulnerabilities.

- **Use security software:** Install and regularly update antivirus, anti-malware, and anti-phishing software on your devices.

- **Monitor network activity:** Implement intrusion detection sys-

tems (IDS) and security information and event management (SIEM) tools to monitor your network for suspicious activity.

- **Conduct regular security audits:** Perform regular security audits to identify and address vulnerabilities in your systems and processes.

- **Develop an incident response plan:** Create a plan that outlines the steps to take in the event of a security incident, including how to contain the attack and restore normal operations.

- **Foster a culture of security:** Encourage employees to report suspicious activity and create an environment where security is a shared responsibility.

Ransomware

Ransomware is a type of malicious software, or malware, designed to block access to a computer system or its data until a ransom is paid. It usually works by encrypting the victim's files, making them inaccessible, and then demanding payment in exchange for the decryption key. Ransomware attacks can target individuals, businesses, or even government organizations, and payment is typically demanded in the form of cryptocurrencies to ensure anonymity.

In May 2024, Ascension, a national healthcare provider, experienced a ransomware attack that shut down their networks and limited access to their electronic health records. In the aftermath of the attack, Ascension released a statement similar to most businesses that fall prey to ransomware attackers (Self).

> On May 8, Ascension detected unusual activity in our network systems, which we have determined is due to a ransomware attack. We continue to diligently investigate and address this ransomware attack, working closely with industry-leading cybersecurity experts to assist in our investigation and recovery efforts (“Cybersecurity Event Update”).

Ascension has neither released information about the amount of the ransomware demand, nor whether they paid that amount.

To defend against ransomware attacks, you can take several precautionary measures. These include:

- **Regularly update your operating system and software** with the latest security patches.

- **Use reputable antivirus and anti-malware software**, and keep it updated.

- **Implement strong, unique passwords** for all your accounts and enable two-factor authentication whenever possible.

- **Be cautious when opening email attachments** or clicking on links from unknown sources.

- **Regularly backup your important files** to an external drive or a secure cloud storage service.

- **Educate yourself and your employees** about the risks of ransomware and how to identify potential threats.

- **Consider using a Virtual Private Network (VPN)** for added security when browsing the internet.

Conclusion

As we have journeyed through the pages of "The Art of Cyber War," we have gained invaluable insights into the complex and developing world of cyber attacks.

By understanding the motivations and methods of cyber criminals, as well as the various forms of attacks they employ, we are better equipped to defend ourselves and our organizations against these threats.

It is crucial to remember that no security solution is foolproof, and the landscape of cyber threats will continue to evolve as technology advances. However, by staying vigilant, implementing best practices, and fostering a culture of security awareness, we can significantly reduce our risk of falling victim to cyber attacks.

In conclusion, "The Art of Cyber War," although not all-inclusive, serves as a guide to understanding and defending against modern cyber threats. By embracing the knowledge and strategies presented in this book, we can work together to create a safer, more secure digital world for ourselves and future generations.

Works Cited

Bode, Karl. “Hackers Trick Venture Capital Firm into Sending Them $1 Million.” *Www.vice.com*, 5 Dec. 2019, www.vice.com/en/article/mbmmaq/hackers-trick-venture-capital-firm-into-sending-them-dollar1-million. Accessed 19 May 2024.

“Business Email Compromise .” *FBI*, FBI, www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/business-email-compromise. Accessed 18 June 2024.

“Cybersecurity Event Update.” *Ascension.org*, 2024, about.ascension.org/cybersecurity-event. Accessed 16 June 2024.

Dahan, Marc. “What Are Compromised Credential Attacks?” *Comparitech.com*, Comparitech, 16 Feb. 2022,

www.comparitech.com/blog/information-security/compromised-credential-attacks/#:~:text=In%20late%202023%2C%20the%20genetic%20testing%20firm%2023andMe,of%20birth%2C%20genetic%20ancestry%20results%2C%20and%20geographical%20location. Accessed 11 June 2024.

"Define Baiting Cyber Attack - Bing." *Bing*, 2023, www.bing.com/search?q=define%20baiting%20cyber%20attack&qs=SYC&showconv=1&sendquery=1&FORM=ASCHT2&sp=1&lq=0. Accessed 18 June 2024.

Demers, Ben. "Struggling LastPass Suffers New Data Breach. Is Your Account at Risk?" *Kiplinger.com*, Kiplinger, 7 Jan. 2023, www.kiplinger.com/personal-finance/lastpass-hack. Accessed 16 June 2024.

Divya. "WordPress Plugin Flaw Exposes 200,000+ Websites to XSS Attacks." *GBHackers on Security | #1 Globally Trusted Cyber Security News Platform*, 12 Mar. 2024, gbhackers.com/wordpress-plugin-flaw/. Accessed 6 May 2024.

Dizdar, Admir. "CSRF Attacks: Real Life Attacks and Code Walkthrough." *Bright Security*, 17 Feb. 2021,

brightsec.com/blog/csrf-attack/. Accessed 9 June 2024.

Goodin, Dan. “Bypassing TouchID Was “No Challenge at All,” Hacker Tells Ars.” *Ars Technica*, Ars Technica, 24 Sept. 2013, arstechnica.com/information-technology/2013/09/touchid-hack-was-no-challenge-at-all-hacker-tells-ars/. Accessed 14 June 2024.

---. “LastPass Users Targeted in Phishing Attacks Good Enough to Trick Even the Savvy.” *Ars Technica*, Ars Technica, 18 Apr. 2024, arstechnica.com/security/2024/04/lastpass-users-targeted-in-phishing-attacks-good-enough-to-trick-even-the-savvy/. Accessed 16 June 2024.

Hill, Michael. “Timeline of the Latest LastPass Data Breaches.” *CSO Online*, CSO Online, Mar. 2023, www.csoonline.com/article/574291/timeline-of-the-latest-lastpass-data-breaches.html#:~:text=On%20November%2030%2C%202022%2C%20password%20manager%20LastPass%20informed,certain%20elements%20of

%20customers%E2%80%99%20information%20have%20been%20exposed. Accessed 16 June 2024.

Hughlett, Mike. “A $735,000 Payment to Ryan Construction Vanishes in an Apparent Cybercrime.” *Aol.com*, AOL, 15 Mar. 2024, www.aol.com/news/735-000-payment-ryan-construction-120000118.html. Accessed 15 June 2024.

Kost, Edward. “11 Ways to Prevent Supply Chain Attacks in 2024 (Highly Effective) | UpGuard.” *Upguard.com*, 2024, www.upguard.com/blog/how-to-prevent-supply-chain-attacks. Accessed 14 June 2024.

“Major Cyberattack Sees NHS London Hospitals Declare Critical Incident with Operations Cancelled.” *The Independent*, 4 June 2024, www.independent.co.uk/news/health/nhs-hospital-cyberattack-london-blood-tests-b2556383.html. Accessed 14 June 2024.

McClanahan, Patrick. “1.4 Attacks - Types of Attacks.” *Engineering LibreTexts*, 11 Jan. 2021, eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-

_Types_of_Attacks#:~:text=Examples%20of%20Interception%20attacks%3A%201%20Eavesdropping%20on%20communication.,capture%20data%20from%20a%20computer%20system%20or%20network. Accessed 11 June 2024.

Molenaar, Rene. “VLAN Hopping.” *NetworkLessons.com*, 8 Oct. 2015, networklessons.com/cisco/ccnp-switch/vlan-hopping. Accessed 15 June 2024.

Montalbano, Elizabeth. ““Ultimate” MiTM Attack Steals $1M from Israeli Startup.” *Threatpost.com*, Threatpost, 5 Dec. 2019, threatpost.com/ultimate-mitm-attack-steals-1m-from-israeli-startup/150840/.

“Path Traversal | OWASP Foundation.” *Owasp.org*, 2024, owasp.org/www-community/attacks/Path_Traversal. Accessed 5 May 2024.

Pecha, Petr. “What Are Supply Chain Attacks and How to Defend against Them.” *Goodaccess.com*, 24 Aug. 2023,

www.goodaccess.com/blog/supply-chain-attack-what-is. Accessed 14 June 2024.

"Phishing Definition | Gab AI | an Uncensored and Unfiltered AI Platform." *Gab AI*, 2019, gab.ai/c/66719690258449e9fd287c89. Accessed 18 June 2024.

"Pretexting." *Proofpoint*, 12 Mar. 2024, www.proofpoint.com/us/threat-reference/pretexting. Accessed 18 June 2024.

Sam Curry. "Analysis of CVE-2019-14994 – Jira Service Desk Path Traversal Leads to Massive Information Disclosure | Sam Curry." *Sam Curry | Web Application Security Researcher*, 26 Sept. 2019, samcurry.net/analysis-of-cve-2019-14994/. Accessed 5 May 2024.

Self, Matthew. "Ascension Restores Network after Ransomware Attack." *KSNT 27 News*, KSNT 27 News, 11 June 2024, www.ksnt.com/news/kansas/ascension-restores-network-after-ransomware-attack/. Accessed 16 June 2024.

Surana, Nitesh. "Vulnerabilities Exploited for Monero Mining Malware Delivered via GitHub, Netlify." *Trend Micro*, 3 Dec.

2021, www.trendmicro.com/fr_fr/research/21/l/vulnerabilities-exploited-for-monero-mining-malware-delivered-via-gitHub-netlify.html. Accessed 5 May 2024.

Thomas, Rebecca, et al. "Major Cyberattack Sees NHS London Hospitals Declare Critical Incident with Operations Cancelled." *The Independent*, 4 June 2024, www.independent.co.uk/news/health/nhs-hospital-cyberattack-london-blood-tests-b2556383.html. Accessed 14 June 2024.

Toulas, Bill. "Bigpanzi Botnet Infects 170,000 Android TV Boxes with Malware." *BleepingComputer*, BleepingComputer, 17 Jan. 2024, www.bleepingcomputer.com/news/security/bigpanzi-botnet-infects-170-000-android-tv-boxes-with-malware/. Accessed 14 June 2024.

---. "DDoS Attacks Target EU Political Parties as Elections Begin." *BleepingComputer*, BleepingComputer, 8 June 2024, www.bleepingcomputer.com/news/security/ddos-attacks-target-eu-political-parties-as-elections-begin/. Accessed 14 June 2024.

---. “Hackers Exploit WordPress Plugin Flaw to Infect 3,300 Sites with Malware.” *BleepingComputer*, BleepingComputer, 10 Mar. 2024, www.bleepingcomputer.com/news/security/hackers-exploit-wordpress-plugin-flaw-to-infect-3-300-sites-with-malware/. Accessed 3 June 2024.

“What Is a Whaling Attack? Examples and Statistics | Fortinet.” *Fortinet*, 2022, www.fortinet.com/resources/cyberglossary/whaling-attack#:~:text=A%20Whaling%20Attack%2C%20also%20known%20as%20Whaling%20Phishing%2C,of%20the%20network%2C%20passwords%2C%20or%20other%20user%20information. Accessed 18 June 2024.

“What Is Directory Traversal | Risks, Examples & Prevention | Imperva.” *Learning Center*, 20 Dec. 2023, www.imperva.com/learn/application-security/directory-traversal/#:~:text=Directory%20Traversal%20attacks%2C%20or%20path,sensitive%20files%20to%20gather%20data. Accessed 5 May 2024.