Contents

Index

Index

Index

The CIA Triad of Cybersecurity: Confidentiality, Integrity & Availability

The CIA Triad is a security model that helps people think about various parts of IT security:

- ✓ Confidentiality is concerned with unauthorized people seeing the contents of the data
- ✓ Integrity ensures that no unauthorized modifications are made to the information
- ✓ Availability is concerned with the data being accessible when and where it is needed

Security Teams – Color Coded

- ✓ Red Team: A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture

- ✓ Blue Team: A group of people responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers

- ✓ White Team: Acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission

- ✓ Purple Team: Comprised of both the blue and red teams to work together to maximize their cyber capabilities through continuous feedback and knowledge transfer between attackers and defenders

Threat + Vulnerability = Risk!

- ✓ In most cases, you will be unable to remove all risks! Instead, it would be best to mitigate the risk to a low enough level to **accept the residual risk**.

IP Address Basics

- ✓ **Private IP Addresses are in the range of 10.x.x.x, 172.16-31.x.x, or 192.168.x.x.** All others are considered Public IP Addresses.
- ✓ The IPv4 Localhost & Loopback IP is 127.0.0.1 while the IPv6 variant is ::1
- ✓ APIPA addresses (IPv6: Link-Local) are in the range of 169.254.x.x. APIPA is a Windows feature.
- ✓ IPv6 addresses comprise of 32 hexadecimal digits, while IPv4 addresses consist of 32-bits. Lastly, MAC addresses comprise of 12 hex digits.
- ✓ **IPv6 includes IPsec built into the protocol by default**. Additionally, IPv6 also provides an extended IP address range for networks, eliminating the need for using NAT.

Index

NIST, SANS & The Incident Response Lifecycle

NIST stands for National Institute of Standards and Technology. They're a U.S. government agency proudly proclaiming themselves as "one of the nation's oldest physical science laboratories". They work in all-things-technology, including cybersecurity, where they've become one of the two industry standard go-tos for incident response with their incident response steps, the other being SANS.

The NIST Incident Response Process contains four steps:

1. Preparation:
   - → During the preparation phase, the incident response team conducts training, prepares their incident response kits, and researches threats and intelligence.
   - → Preparation is key to rapid response: In this step you compile a list of all your assets: servers, networks, applications, and critical endpoints (like C-level laptops). Next, rank them by level of importance. Then monitor their traffic patterns so you can create baselines to be used for comparisons.
   - → Create a communication plan, with guidance on who to contact, how, and when based on each incident type. Get buy-in from everyone on the list to prevent hiccups or finger pointing later.
2. Detection and Analysis:
   - → During the detection and analysis phase, an organization focuses on monitoring and detecting any possible malicious events or attacks
   - → At this point in the process, a security incident has been identified. This is where you go into research mode
3. Containment, Eradication, and Recovery:
   - → Containment aims to stop the bleeding. Here is where you patch the threat's entry point.
   - → Eradication aims to remove the threat. If the threat gained entry from one system and proliferated into other systems, you'll have more work on your hands here.
   - → Recovery aims to get the system operational if it went down or simply back to business as usual if it didn't.
   - → A cybersecurity analyst must preserve evidence during the containment, eradication, and recovery phase: They must preserve forensic and incident information for future needs, prevent future attacks or bring up an attacker on criminal charges
   - → Restoration and recovery are often prioritized over analysis by business operations personnel, but taking time to create a forensic image is crucial to preserve the evidence for further analysis and investigation.
4. Post-Incident Activity:
   - → This step provides the opportunity to learn from your experience: Take a look at the incident with a humble but critical eye to identify areas for improvement.
   - → During the post-incident activity phase, the organization conducts after-action reports, creates lessons learned, and conducts follow-up actions to better prevent another incident from occurring.

Index

SANS stands for SysAdmin, Audit, Network, and Security. They're a private organization that, per their self-description, is "a cooperative research and education organization". Though more youthful than NIST, their sole focus is security, and they've become an industry standard framework for incident response.

The SANS Incident Response Process consists of six steps:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

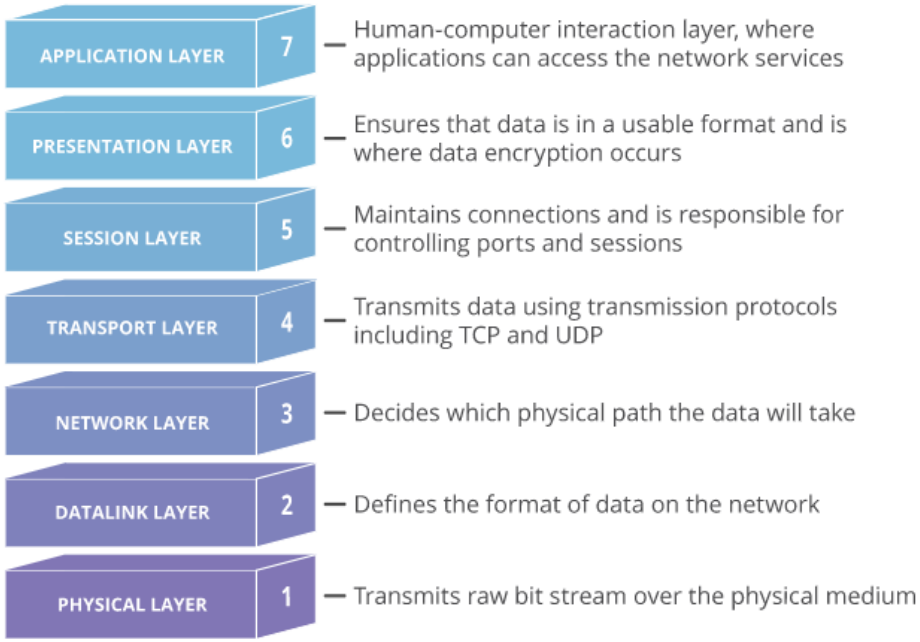
You can see NIST and SANS have all the same components and the same flow but different verbiage and clustering. If not in verbiage though, they are in agreement in spirit! Step three in particular is where NIST and SANS kind-of part ways in their similarities before agreeing again on the final step: NIST views the process of containment, eradication, and recovery as a singular step with multiple components while SANS views them as their own independent steps.

Index

ISO-OSI Model: A Recap

The Open Systems Interconnection model is a conceptual model created by the International Organization for Standardization and establishes a standard for computer communications over a network.

This model is comprised of 7 layers:



A Line A Layer:

1. User-apps are not a part of the Application Layer, protocols such as HTTPS & SMTP are!
2. The Presentation Layer is responsible for translation, encryption & compression. Ex: TLS/SSL.
3. The Session Layer ensures comms stay open for all data transmissions to complete. Ex: Sockets.
4. The Transport Layer is responsible for end-to-end comms and handles segmentation & reassembly and flow & error control. Example: TCP, UDP
5. The Network Layer facilitates comms across networks, breaks segments into packets and handles routing. Ex: IP, IPSec, ICMP, OSPF, RIP. QoS occurs at layers 2 & 3.
6. The Data-Link Layer is very similar to the network layer and facilitates intra-network comms, breaks packets into frames and handles flow & error control in intra-net comms. Examples: PPP, L2TP.
7. The Physical Layer comprises physical devices & signal conversions, converting data into bitstreams.

→ The widely implemented TCP/IP model combines the Application, Presentation and Session layers.
→ Data is encapsulated as it moves down the stack, and de-encapsulated as it moves up to the app layer
→ Async Transfer Mode (ATM) maps to the lowest 3-layers of the OSI model, and uses fixed-length 53-octet cells instead of variable IP-packets. Remember the equivalency of OSI Frames & ATM Cells as getting "framed" and put in a jail "cell"!
→ Remember the OSI order of Segments -> Packets -> Frames as the 'SPF' of sunscreen lotions! Also logically: TCP Segments, IP Packets and Data Frames.

Index

A Note on CVE

The Common Vulnerabilities and Exposures (CVE) system provides a reference method for publicly known information-security vulnerabilities and exposures. The United States' National Cybersecurity FFRDC, operated by The MITRE Corporation, maintains the system, with funding from the US National Cyber Security Division of the US Department of Homeland Security. The system was officially launched for the public in September 1999.

The Security Content Automation Protocol uses CVE, and CVE IDs are listed on MITRE's system as well as in the US National Vulnerability Database.

Identifiers:

MITRE Corporation's documentation defines CVE Identifiers (also called "CVE names", "CVE numbers", "CVE-IDs", and "CVEs") as unique, common identifiers for publicly known information-security vulnerabilities in publicly released software packages.

Historically, CVE identifiers had a status of "candidate" ("CAN-") & could then be promoted to entries ("CVE-"), however this practice was ended in 2005 and all identifiers are now assigned as CVEs. The assignment of a CVE number is not a guarantee that it will become an official CVE entry (e.g. a CVE may be improperly assigned to an issue which is not a security vulnerability, or which duplicates an existing entry).

CVEs are assigned by a CVE Numbering Authority (CNA). While some vendors acted as a CNA before, the name and designation were not created until February 1, 2005. There are three primary types of CVE number assignments:

1. The Mitre Corporation functions as Editor and Primary CNA
2. Various CNAs assign CVE numbers for their own products (e.g. Microsoft, Oracle, HP, Red Hat, etc.)
3. A third-party coordinator such as CERT Coordination Center may assign CVE numbers for products not covered by other CNAs

When investigating a vulnerability or potential vulnerability it helps to acquire a CVE number early on. CVE numbers may not appear in the MITRE or NVD CVE databases for some time (days, weeks, months or potentially years) due to issues that are embargoed (the CVE number has been assigned but the issue has not been made public), or in cases where the entry is not researched & written up by MITRE due to resource issues. **CVEs are for software that has been publicly released.**

In order to support CVE IDs beyond CVE-YEAR-9999 (aka the CVE10k problem) a change was made to the CVE syntax in 2014 and took effect on Jan 13, 2015. The new syntax is variable length and includes:

'CVE' prefix + Year + Arbitrary Digits

NOTE: The variable length arbitrary digits will begin at four fixed digits and expand with arbitrary digits only when needed in a calendar year, for example, CVE-YYYY-NNNN and if needed CVE-YYYY-NNNNN, CVE-YYYY-NNNNNN, and so on. This also means there will be no changes needed to previously assigned CVE-IDs, which all include a minimum of four digits.

Index

Security

Vulnerabilities & Exploit-Vectors

A Zero-Day Vulnerability is an unknown vulnerability, so a patch or virus definition has not been released yet. A zero-day vulnerability refers to a hole in software that is unknown to the vendor. Hackers then exploit this security hole before the vendor becomes aware and hurries to fix it. This exploit is therefore called a zero-day attack. Such attacks include infiltrating malware, spyware, or allowing unwanted access to user information.

Missing Patches are the most common vulnerability found on both Windows and Linux systems. When a security patch is released, attackers begin to reverse engineer the security patch to exploit the vulnerability. If your servers are not patched against the vulnerability, they can become victims of the exploit, and the server's data can become compromised.

Rogue Anti-Virus (Scareware) is a form **of malicious software** and internet fraud that misleads users into believing there is a virus on their computer and to pay money for a fake malware removal tool (that actually introduces malware to the computer). It is a form of Scareware that manipulates users through fear and a form of ransomware. *If the alert is displayed on a macOS system but appears to be meant for a Windows system, it is obviously a scam or fake alert and most likely a rogue anti-virus attempting to infect the system!*

Worms are standalone malware programs that **replicate themselves** to spread to other computers. Often, they use a computer network to spread, relying on security failures on the target computer to access it.

Virus: Similar to a worm, but a worm can spread on its own whereas a virus **needs a host program** or user interaction to propagate itself. May be programmed to carry out malicious actions, such as deleting files or changing system settings.

A Polymorphic Virus alters its binary code to avoid detection by antimalware scanners that rely on signature-based detection. It can avoid detection by changing its signature, and may do so on specific dates or times.

A Trojan is a type of malware that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network. To operate, a trojan will create numerous processes that run in the background of the system.

A Remote Access Trojan (RAT) is the most common type of trojan, which allows an attacker to control a workstation or steal information remotely.

A Rootkit is a set of software tools that enable an unauthorized user to control a computer system without being detected. A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. A rootkit is generally a collection of tools that enable administrator-level access to a computer or network. They can often disguise themselves to avoid detection. If a rootkit is suspected on a machine, it is best to reformat and reimage the system.

A Botnet is many internet-connected devices, each of which is running one or more bots. A 'bot' on the botnet is any machine that has been compromised such that the attacker can remotely control it & have it execute commands at their will. Such machines are thus named 'Zombies'. Botnets can be used to perform DDoS attacks, steal data, send spam, etcetera and allow the attacker to access the device and its connection.

Index

Ransomware is a **type of malware** designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Once infected, a system or its files are encrypted, and then the decryption key is withheld from the victim unless payment is received.

Evil Twin: An evil twin is **meant to mimic a legitimate hotspot** provided by a nearby business, such as a coffee shop that provides free Wi-Fi access to its patrons. An evil twin is a type of rogue wireless access point that masquerades as a legitimate Wi-Fi access point so that an attacker can gather personal or corporate information without the user's knowledge. This type of attack may be used to steal the passwords of unsuspecting users by monitoring their connections or phishing, which involves setting up a fraudulent website and luring people there.

Rogue Access Point: A rogue AP is an access point **installed on a network without the network owner's permission**. For example, if an employee connected a wireless access point to a wall jack in their office so that they can use their smartphone or tablet, this would be considered a rogue access point.

A Rogue DHCP Server is a DHCP server set up on a network by an attacker, or by an unaware user, and is not under the control of network administrators. Rogue DHCP servers are also commonly used by attackers for the purpose of network attacks such as an on-path or man-in-the-middle attack.

Universal Plug-and-Play (UPnP) is a protocol framework allowing network devices to **autoconfigure** services, such as allowing a games console to request appropriate settings from a firewall. UPnP is associated with **several security vulnerabilities and is best disabled** if not required. You should ensure that the router does not accept UPnP configuration requests from the external (internet) interface. If using UPnP, keep up-to-date with any security advisories or firmware updates from the router manufacturer.

An Active Mail Relay occurs when an SMTP server is configured in such a way that it allows anyone on the internet to send email through it, not just mail originating from your known and trusted users. Spammers can exploit this type of vulnerability to use your email server for their benefit.

Insecure Object Reference is a coding vulnerability & refers to when a reference to an internal implementation object, such as a file or database key, is exposed to users without any other access control.

Insufficient Logging and Monitoring allow attackers to achieve their goals without being detected due to the lack of monitoring and timely response by defenders.

The use of Insecure Functions occurs in the C language when legacy functions like strcpy() are used. These insecure functions can lead to buffer overflows and other exploits being successful against a program.

Virtual Machine Escape vulnerabilities are the **most severe** issue that may exist in a virtualized environment. In this attack, the attacker has access to a single virtual host and then leverages that access to intrude on the resources assigned to different virtual machines.

Cookie Security - Secure Attribute: When a cookie has the Secure attribute, the user agent includes the cookie in an HTTP request only if the request is transmitted over a secure channel (typically HTTPS). Although seemingly useful for protecting cookies from active network attackers, the Secure attribute protects only the cookie's confidentiality. Forcing the web application to use TLS or SSL does not force the cookie to be sent over TLS/SSL, so you still would need to set the Secure attribute on the cookie. Hashing the cookie provides integrity of the cookie, not confidentiality.

Index

A Golden Ticket is a Kerberos ticket that can grant other tickets in an Active Directory environment. Attackers who can create a golden ticket can use it to grant administrative access to other domain members, even to domain controllers.

Lateral Movement is an umbrella term for a variety of attack types. Attackers can extend their lateral movement by a great deal if they can compromise host credentials.

Pivoting is a process similar to lateral movement. When attackers pivot, they compromise one central host (the pivot) that allows them to spread out to other hosts that would otherwise be inaccessible.

Pass the Hash (PtH) is the process of harvesting an account's cached credentials when the user logs in to a single sign-on (SSO) system. This would then allow the attacker to use the credentials on other systems, as well.

Insecure Direct Object References (IDOR) are a cybersecurity issue that occurs when a web application developer uses an identifier for direct access to an internal implementation object but provides no additional access control and/or authorization checks. An attacker could change the userid number and directly access any user's profile page in this scenario. Example in a URL: "***https://test.site.com/profile.php?userid=1546***"

A Race Condition is a software vulnerability when the resulting outcome from execution processes is directly dependent on the order and timing of certain events. Those events fail to execute in the order and timing intended by the developer.

Weak or Default Configurations are commonly a result of incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information.

Improper Error-Handling can reveal implementation details that should never be revealed, such as detailed information that can provide hackers with important clues on the system's potential flaws.

Malware Beaconing: In the context of malware, beaconing is when malware periodically calls out to the attacker's C2 server to get further instructions on tasks to perform on the victim machine

An Indicator of Compromise (IoC) is an artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion. Typical IOCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs, or botnet command and control servers' domain names.

The HTTP TRACE/TRACK Methods are normally used to return the full HTTP request to the requesting client for proxy-debugging purposes and allow the attacker to access sensitive information in the HTTP headers. Since this only exposes information in the headers, it minimizes the risk to our system's data confidentiality.

The phpinfo Information Disclosure Vulnerability prints out detailed information on both the system and the PHP configuration. This information by itself doesn't disclose any information about the data stored within the system, though, so it isn't a great threat to our data's confidentiality.

A Logic Bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met, such as a specific date. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company.

Armored Viruses are a type of virus that use various techniques to protect themselves from being reverse engineered. This includes changing its code during execution and encrypting its payloads.

Index

Bluejacking sends unsolicited messages over Bluetooth to Bluetooth-enabled devices such as smartphones and tablets.

Bluesnarfing involves taking data from a smartphone or tablet over Bluetooth without permission.

Q: In 2014, Apple's implementation of SSL had a severe vulnerability that, when exploited, allowed an attacker to gain a privileged network position that would allow them to capture or modify data in an SSL/TLS session. This was caused by poor programming in which a failed check of the connection would exit the function too early. Based on this description, what is this an example of?

A: Improper Error Handling

This is an example of an improper error handling vulnerability. A well-written application must be able to handle errors and exceptions gracefully. The main goal must be for the application not to fail in a way that allows an attacker to execute code or perform an injection attack. One famous example of an improper error handling vulnerability is Apple's GoTo bug, as described above. For more details on this particular vulnerability, please see CVE-2014-1266.

Q: You are creating a script to filter some logs so that you can detect any suspected malware beaconing. Which of the following is NOT a typical means of identifying a malware beacon's behavior on the network?

A: The beacon's protocol

The beacon's protocol is not typically a means of identifying a malware beacon: A beacon can be sent over numerous protocols, including ICMP, DNS, HTTP, and numerous others. Unless you specifically knew the protocol being used by the suspected beacon, filtering out beacons by the protocol seen in the logs could lead you to eliminate malicious behavior prematurely.

Other factors like the beacon's persistence (if it remains after a reboot of the system) and the beacon's interval (how much time elapses between beaconing) are much better indicators for fingerprinting a malicious beacon.

The removal of known traffic by the script can also minimize the amount of data the cybersecurity analyst needs to analyze, making it easier to detect the malicious beacon without wasting their time reviewing non-malicious traffic.

Q: A cybersecurity analyst has received an alert that sensors continuously observe well-known call home messages at their network boundary. Still, the organization's proxy firewall is properly configured to successfully drop the messages before leaving the network. Which of the following is MOST likely the cause of the call home messages being sent?

A: An infected workstation is attempting to reach a Command & Control (C2) Server

A call home message is an indicator of compromise known as beaconing. Beaconing usually occurs after a stage 1 malware program has been implanted on an organization's workstation or server, but that isn't the most correct answer to this question. Instead, beaconing indicates that a workstation or server is infected

and tries to communicate with the attacker's command and control server. This beaconing will continue until the infected system (workstation or server) is found and cleared of the malware or until the botnet gives the infected host further instructions to perform (such as to attack).

"Malware is running on a company workstation or server" is incorrect because we do not have positive verification of that based on this scenario. A beacon does not have to be malware. For example, it can simply be a single ping packet or DNS request being sent out every day at a certain time using the Windows task scheduler.

Be careful on the exam to answer the question being asked and choose the "most" accurate answer: Since the call home signal is coming from the internal network and attempting to connect to an external server, it cannot be evidence of an attacker performing reconnaissance on your workstations.

Also, nothing in the question is indicative of an insider threat trying to exfiltrate information since a call home message is generally minimal in size and not large enough to exfiltrate data.

Q: You have been asked to scan your company's website using the OWASP ZAP tool. When you perform the scan, you received the following warning:

"The AUTOCOMPLETE output is not disabled in HTML FORM/INPUT containing password type input. Passwords may be stored in browsers and retrieved."

You begin to investigate further by reviewing a portion of the HTML code from the website that is listed below:

```
                                    ©2022 Dion Training

<form action="authenticate.php">
   Enter your username: <BR>
 <input type="text" name="user" value="" autofocus><BR>
   Enter your Password: <BR>
 <input type="password" name="pass" value=""
maxlength="32"><BR>
 <input type="submit" value="submit">
 </form>
```

Based on your analysis, which of the following actions should you take?

A: Tell the dev to review their code and implement a fix (This is NOT a false positive!)

Since your company owns the website, you can require the developer to implement a bug/code fix to prevent the form from allowing the AUTOCOMPLETE function to work on this website. The code change to perform is quite simple, simply adding "autocomplete=off" to the code's first line. The resulting code would be <form action="authenticate.php" autocomplete="off">.

Index

Buffer Overflows

A Buffer Overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. In this case, a buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code.

Buffer overflow is probably the best-known form of software security vulnerability (thus its own sub—section). Most software developers know what a buffer overflow vulnerability is, but buffer overflow attacks against both legacy and newly-developed applications are still quite common. Part of the problem is due to the wide variety of ways buffer overflows can occur, and part is due to the error-prone techniques often used to prevent them.

Buffer overflows are not easy to discover and even when one is discovered, it is generally extremely difficult to exploit. Nevertheless, attackers have managed to identify buffer overflows in a staggering array of products and components.

In a classic buffer overflow exploit, the attacker sends data to a program, which it stores in an undersized stack buffer. **The result is that information on the call stack is overwritten, including the function's return pointer.** The data sets the value of the return pointer so that when the function returns, it transfers control to malicious code contained in the attacker's data.

There are a variety of other types of buffer overflow, including Heap buffer overflow and Off-by-one Error among others. Another very similar class of flaws is known as Format string attack.

At the code level, buffer overflow vulnerabilities usually involve the violation of a programmer's assumptions. Many memory manipulation functions in C and C++ do not perform bounds checking and can easily overwrite the allocated bounds of the buffers they operate upon. Even bounded functions, such as strncpy(), can cause vulnerabilities when used incorrectly. A combination of memory-manipulation and mistaken assumptions regarding the size or makeup of some data is often the root cause of most buffer-overflows.

Buffer overflow vulnerabilities typically occur in code that:

- Relies on external data to control its behavior
- Depends upon properties of the data that are enforced outside of the immediate scope of the code
- Is so complex that a programmer cannot accurately predict its behavior

Q: Praveen is currently investigating activity from an attacker who compromised a host on the network. The individual appears to have used credentials belonging to a janitor. After breaching the system, the attacker entered some unrecognized commands with very long text strings and then began using the sudo command to carry out actions. What type of attack has just taken place?

A: Privilege Escalation

The use of long query strings points to a buffer overflow attack, and the sudo command confirms the elevated privileges after the attack. This indicates a privilege escalation has occurred.

Index

Threat Actors & Attacks

An Insider Threat is a type of threat actor assigned privileges on the system that cause an **intentional or unintentional** incident. Insider threats can be used as **unwitting** pawns of external organizations or make crucial mistakes that can open up exploitable security vulnerabilities. An insider threat is any current or former employee, contractor, or business partner who has or had authorized access.

A Known Threat is a threat that can be identified using a basic signature or pattern matching.

An Advanced Persistent Threat (APT) is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. In recent times, the term may also refer to non-state-sponsored groups conducting large-scale targeted intrusions for specific goals.

Such threat actors' motivations are typically political or economic. Every major business sector has recorded instances of cyberattacks by advanced actors with specific goals, whether to steal, spy, or disrupt. The purpose of these attacks is to install custom malware (malicious software).

The median "dwell-time", the time an APT attack goes undetected, differs widely between regions. FireEye reported the mean dwell-time for 2018 in the Americas as 71 days, EMEA as 177 days, and APAC as 204 days. Such a long dwell-time allows attackers a significant amount of time to go through the attack cycle, propagate, and achieve their objective.

Definitions of precisely what an APT is can vary, but can be summarized by their named requirements below:

- Advanced – Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include commercial and open-source computer intrusion technologies and techniques, **but may also extend to include the intelligence apparatus of a state**. While individual components of the attack may not be considered particularly "advanced" (e.g. common malware), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it. Operators may also demonstrate a deliberate focus on operational security that differentiates them from "less advanced" threats.
- Persistent – One of the operator's goals is to maintain long-term access to the target & the targeting is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful. If the operator loses access to their target they usually will reattempt access, **and most often, successfully**.
- Threat – **APTs are a threat because they have both capability and intent**. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized, and well-funded.

APT attack model: quietly gather information from compromised systems over an extended period of time. An APT is unlikely to conduct a DDoS attack, use worms to spread throughout the network, or use ransomware as part of their covert attacks.

Index

Hacktivists are usually political, but they are disorganized and don't have the level of sophistication needed to hack into a well-defended government computer network like the election system.

Organized Crime Groups may have the sophistication to conduct hacks in secure government systems, though they're usually more interested in conducting criminal actions to make money instead of politics.

Script Kiddies are low skilled hackers who can only use other people's tools. Elitist terminology.

Cross-Site Scripting (XSS) attacks are a type of **injection** in which malicious scripts are injected into otherwise benign and trusted websites. Cross-site scripting focuses on exploiting a user's workstation, not a server. If your website's HTML code does not perform input validation to remove scripts that may be entered by a user, then an attacker can create a popup window that collects passwords & uses that information to compromise other accounts further. Example: Submitting SQL code into an un-sanitized user form. Attackers may use a cross-site scripting vulnerability to bypass access controls such as the same-origin policy.

A Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated. An XSS will allow an attacker to execute arbitrary JavaScript within the victim's browser (such as creating pop-ups). A CSRF would allow an attack to induce a victim to perform actions they do not intend to perform. Think of it as cookie stealing and misuse.

CRLF Injection is a software **coding vulnerability** that occurs when an attacker injects an unexpected CRLF character sequence. The term CRLF refers to **Carriage Return (ASCII 13, \r) Line Feed (ASCII 10, \n).** They're used to mark the termination of a line but are dealt with differently in today's popular Operating Systems. For example: in Windows both a CR and LF are required to note the end of a line, whereas in Linux/UNIX a LF is only required. In the HTTP protocol, the CR-LF sequence is always used to terminate a line.

A CRLF Injection attack occurs when a user manages to submit a CRLF into an application. This is most commonly done by modifying an HTTP parameter or URL. Depending on how the application is developed, this can be a minor problem or a fairly serious security flaw.

Elaborating on the latter, let's assume a file is used at some point to read/write data to a log of some sort. If an attacker managed to place a CRLF, then can inject some sort of programmatic read method to the file. This could result in the contents being written to screen on the next attempt to use this file.

Another example is the "response splitting" attacks, where CRLFs are injected into an application & included in the response & interpreted by proxies, caches & some browsers as the end of a packet, causing mayhem.

SQL Injection is the placement of malicious code in SQL statements via web page input. SQL is commonly used against databases, but they are not useful when attacking file servers. For example, an attacker may try to dump the contents of the database by using this technique. **A common SQL injection technique is to insert an always true statement, such as 1 == 1, or, 7 == 7.**

Command Injection is an attack in which the goal is to execute arbitrary commands on the host operating system via a vulnerable application. **SQL injection is a specific type of command injection.**

XML Injection is an attack technique used to manipulate or compromise an XML application or service's logic.

LDAP Injection is a code injection technique used to exploit web applications into revealing sensitive user data or modify information represented in the LDAP (Lightweight Directory Access Protocol) data stores.

Index

ARP Spoofing / ARP Poisoning is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.

(The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite.)

IP Spoofing is the creation of IP packets that have a modified source address to either hide the identity of the sender, impersonate another computer system, or both. Thus, it's an on-path attack vector.

Session Hijacking, also known as TCP Session Hijacking, is a method of taking over a web user session by surreptitiously obtaining the session ID and masquerading as the authorized user. This attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the webserver.

A Distributed Denial-of-Service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.

A Denial-of-Service (DoS) attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet.

A SYN Flood is a variant of a Denial of Service (DOS) attack where the attacker initiates multiple TCP sessions but never completes the 3-way handshake. This uses up resources on the server since it cannot complete the handshake and keeps resources reserved for the attacker's computer while it awaits handshake completion.

A Reflective DNS attack is a two-step attack used in DDoS attacks. The attacker sends a large number of requests to one or more legitimate DNS servers while using a spoofed source IP of the targeted victim. The DNS server then replies to the spoofed IP and unknowingly floods the targeted victim with responses to DNS requests that it never sent.

A Smurf attack uses a single **ping with a spoofed source address sent to the broadcast address of a network**. This causes every device within the network to receive a single ping, which appears to come from the device with the spoofed source address. Each network device then responds to the spoofed address, causing the victim (whose address was spoofed) to be overwhelmed with the responses to the initial ping.

Wardialing (or War Dialing) is a technique to automatically scan a list of telephone numbers, **usually dialing every number in a local area code** to search for modems, computers, bulletin board systems (computer servers) and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers for guessing user accounts (by capturing voicemail greetings), or **locating modems** that might provide an entry-point into computer or other electronic systems. It may also be used by security personnel, for example, to detect unauthorized devices, such as modems or faxes, on a company's telephone network.

An On-Path Attack (previously known as a Man-in-the-Middle Attack) is a general term when a perpetrator positions himself in a conversation between a user and an application, either to eavesdrop or impersonate one of the parties, making it appear as if a normal exchange of information is occurring. For example, if your user and server are both in the United States (English language), but the attacker is performing the on-path attack from Russia, then the server will utilize the Russian language in the text since it sees the connection coming from a Russian IP address.

Index

A Wi-Fi Deauthentication Attack is a type of denial-of-service attack that targets communication between a user and a Wi-Fi wireless access point by sending a deauthentication frame to the victim's machine.

VLAN Hopping is an attack where the attacker is able to send traffic from one VLAN into another by either double tagging the traffic or conducting switch spoofing. The main goal here is to gain access to other VLANs. There are two primary methods of VLAN hopping: **switch spoofing** and **double tagging.**

In a Switch Spoofing Attack, an attacking host imitates a trunking switch by speaking the tagging and trunking protocols (e.g. Multiple VLAN Registration Protocol, IEEE 802.1q, Dynamic Trunking Protocol) used in maintaining a VLAN. Traffic for multiple VLANs is then accessible to the attacking host. Switch spoofing can only be exploited when interfaces are set to negotiate a trunk.

In a Double Tagging Attack, an attacker connected to an 802.1Q-enabled port prepends two VLAN tags to a frame that it transmits. The frame (externally tagged with VLAN ID that the attacker's port is really a member of) is forwarded without the first tag because it is the native VLAN of a trunk interface. The second tag is then visible to the second switch that the frame encounters. This second VLAN tag indicates that the frame is destined for a target host on a second switch. The frame is then sent to the target host as though it originated on the target VLAN, effectively bypassing the network mechanisms that logically isolate VLANs from one another. However, possible replies are not forwarded to the attacking host (**unidirectional flow**). Double Tagging can only be exploited on switch ports configured to use native VLANs: Trunk ports configured with a native VLAN don't apply a VLAN tag when sending these frames which allows an attacker's fake VLAN tag to be read by the next switch.

Password Spraying is a type of **brute-force attack** in which multiple user accounts are tested with a dictionary of common passwords. It attempts to crack various users' passwords by attempting a compromised password against multiple user accounts. It's an attack method that takes a large number of usernames and loops them with a single password. We can use multiple iterations using several different passwords**, but the number of passwords attempted is usually low compared to the number of users attempted**. This method avoids password lockouts, and it is often more effective at uncovering weak passwords than targeting specific users. If you see an example wherein one account is tested with many password, it's a brute force attack!

Impersonation is the act of pretending to be another person or system for fraud.

A Privilege Escalation attack aims to attain more privileges for a user or application that it is intended to receive by the administrator or developer. It involves exploiting a bug, design flaw, or a configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The elevated user or app can then perform unauthorized actions such as deleting files, viewing private information, or installing unwanted programs and viruses.

It usually occurs when a system has a bug that allows security to be bypassed or, alternatively, has flawed design assumptions about how it will be used. Privilege escalation occurs in two forms:

1. Vertical Privilege Escalation, also known as Privilege Elevation, where a lower privilege user or application accesses functions or content reserved for higher privilege users or applications (e.g. Internet Banking users can access site administrative functions or the password for a smartphone can be bypassed.)

2. Horizontal Privilege Escalation, where a normal user accesses functions or content reserved for other normal users (e.g. Internet Banking User A accesses the Internet bank account of User B)

Index

Directory Traversal or Path Traversal is an **HTTP attack** that allows attackers to access restricted directories & files and execute commands outside of the web server's root directory. By manipulating variables or URLs that reference files with “dot-dot-slash (../)” sequences and its variations or using absolute file paths, it may be possible to access arbitrary files and directories stored on the file system, including application source code or configuration and critical system files.

A Brute-Force Attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. In a traditional brute-force attack, the passcode or password is incrementally increased by one letter/number each time until the right passcode/password is found.

Credential Stuffing is the automated injection of breached username/password pairs to gain user accounts access fraudulently. This is a subset of the brute force attack category: large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account. The attacker can then hijack the account for their purposes. S

A Dictionary Attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.

A Rainbow Table is a precomputed list of possible hashes used when trying to speed up the process of password cracking.

A Hybrid Password Cracking Attack combines the **use of a brute-force attack with a dictionary attack** by using words from the dictionary's list as the basis for the brute-force attack. For example, if the diction had the word Jason in it, the hybrid attack might try Jason123, Jason!@#, and J@$0n as possible combinations based on the word Jason.

Q: Your workstation has fallen victim to an on-path attack. Upon investigation, you determine that the attack is occurring at layer 2 of the OSI model and is redirecting traffic destined for your workstation to the attackers' workstation instead. What type of attack was performed against your workstation?

A: ARP Spoofing

Q: You are developing a containment and remediation strategy to prevent the spread of an APT within your network. Your plan suggests creating a mirror of the company’s databases, routing all externally sourced network traffic to it, and gradually updating with pseudo-realistic data to confuse and deceive the APT as they attempt to exfiltrate the data. Once the attacker has downloaded the corrupted database, your company would then conduct remediation actions on the network and restore the correct database information to the production system. Which of the following types of containment strategies does the plan utilize?

A: Segmentation-based containment that deceives the attacker into believing their attack was successful

There are two types of containment: segmentation and isolation. This is an example of a segmentation-based containment strategy that utilizes deception. Segmentation-based containment is a means of achieving the isolation of a host or group of hosts using network technologies and architecture. As opposed

Index

to completely isolating the hosts, you might configure the protected segment to deceive him or her into thinking the attack is progressing successfully, such as in the database modification example. The scenario is not a hack-back approach since the APT is not directly attacked, only deceived. Isolation-based containment involves removing an affected component from whatever larger environment it is a part of. In this scenario, the original database was never isolated from the network, nor were any other affected assets during the deception.

Q: Which type of system would classify traffic as malicious or benign based on explicitly defined examples of malicious and benign traffic?

A: Machine Learning

Since this is a classic example of a classification usecase, machine learning suffices as an answer & deep learning need not be specified.

Q: A hacker successfully modified the sale price of items purchased through your company's website. During the investigation that followed, the security analyst verified the web server, and the Oracle database was not compromised directly. The analyst also found no attacks that could have caused this during their log verification of the Intrusion Detection System (IDS). What is the most likely method that the attacker used to change the items' sale price?

A: Changing Hidden Form Values (NOT XSS!)

Since there are no indications in the IDS logs, the database, or the server, it is most likely that the hacker changed hidden form values to change the items' price in the shopping cart.

Q: Your company is making a significant investment in infrastructure-as-a-service (IaaS) hosting to replace its data centers. Which of the following techniques should be used to mitigate the risk of data remanence when moving virtual hosts from one server to another in the cloud?

A: Use full-disk encryption:

This method will ensure that all data is encrypted and cannot be exposed to other organizations or the underlying IaaS provider.

Using a zero wipe is typically impossible because VM systems may move without user intervention during scaling and elasticity operations.

Data masking will not prevent your corporate data from being exposed by data remanence.

Spanning multiple disks will leave the data accessible, even though it would be fragmented, and would make the data remanence problem worse overall.

Index

Q: A cybersecurity analyst is reviewing the logs of a Citrix NetScaler Gateway running on a FreeBSD 8.4 server and saw the following output:

```
                                ©2022 Dion Training
  BEGIN LOG
 ------------
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"
------------
  END LOG
```

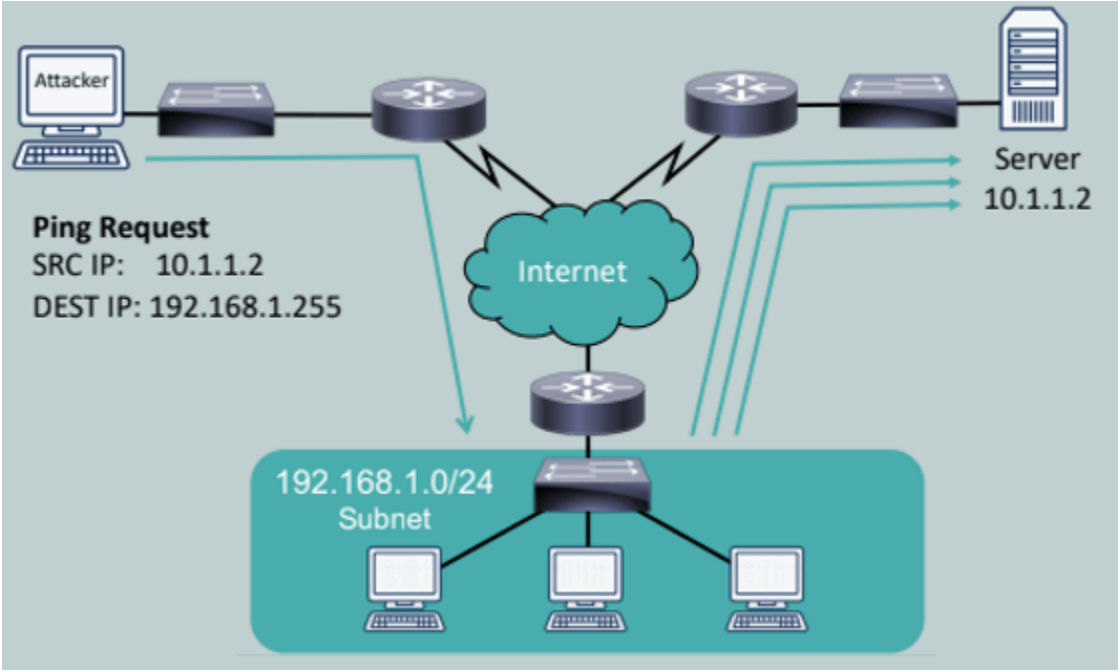
What type of attack was most likely being attempted by the attacker?

A: Directory Traversal

The example output provided comes from a remote code execution vulnerability being exploited in which a directory traversal is used to access the files.

Index

Q: Which of the following best describes the type of attack shown?



A: Smurf Attack

Note that the destination IP is the broadcast address of a /24 network, and the resulting three ping responses are sent to some other server altogether, making this a classic Smurf attack: sending a ping to the broadcast address of a network with a spoofed IP address, causing several ping response messages to be sent to the victim.

Q: You are analyzing the SIEM for your company's e-commerce server when you notice the following URL in the logs of your SIEM:


```
https://www.diontraining.com/add_to_cart.php?itemId=5"+per
ItemPrice="0.00"+quantity="100"+/><item+id="5&quantity=0
```

Based on this line, what type of attack do you expect has been attempted?

A: XML Injection. The original XML structure would be:

<addToCart> <item id="5" perItemPrice="50.00" quantity="1" /> </addToCart>.

By using the URL above, this would be modified to the following:

<addToCart> <item id="5" perItemPrice="0.00" quantity="10" /> <item id="5" perItemPrice="50.00" quantity="0" /> </addToCart>.

This line would allow 10 of the product at $0.00 to be added to the shopping cart, while 0 of the product at $50.00 is added to the cart. This defeats the integrity of the e-commerce store's add to cart functionality.

Index

Q: A security analyst is conducting a log review of the company's web server and found two suspicious entries:

```
                                                          ©2022 Dion Training
  BEGIN LOG
 -------------
[12Nov2020 10:07:23] “GET /logon.php?user=test’+oR+7>1%20—HTTP/1.1” 200 5825
[12Nov2020 10:10:03] “GET /logon.php?user=admin’;%20—HTT{/1.1” 200 5845
-------------
  END LOG
```

The analyst contacts the web developer and asks for a copy of the source code to the logon.php script. The script is as follows:

```
                                                    ©2022 Dion Training
<?php
include(‘../../config/db_connect.php’);
$user = $_GET[‘user’];
$pass = $_GET[‘pass’];
$sql = “SELECT * FROM USERS WHERE username = ‘$user’ AND password = ‘$pass’”;
$result = MySQL_query($sql) or die (“couldn’t execute query”);

if (MySQL_num_rows($result) !=0 ) echo ‘Authentication granted!’;
else echo ‘Authentication failed!’;
?>
```

Based on source code analysis, which type of vulnerability is this web server vulnerable to?

A: SQL Injection

Based on the log entries, it appears the attack was successful in conducting a SQL injection. Notice the escape character (') used in the log. A connection to the MySQL database is being used in the script, which could be exploited since no input validation is being performed.

Q: You are performing a web application security test, notice that the site is dynamic, and must be using a back-end database. You decide you want to determine if the site is susceptible to an SQL injection. What is the first character that you should attempt to use in breaking a valid SQL request?

A: Single quote

The single quote character (') is the character limiter in SQL. With a single quote,' you delimit strings, and therefore you can test whether the programmer has properly escaped the strings in the targeted application. If not escaped directly, you can end any string supplied to the application and add other SQL code after it. This is a common technique for SQL injections.

Index

Social-Engineering

Principles

Authority: Calling in and claiming to be the CEO or from the bank's helpdesk.

Intimidation: Claiming to be the from payroll and stating that paychecks won't clear because you're holding up the process.

Consensus or Social Proof: Claiming that someone from your department did this last week so you can assist this time. It relies on the fact that people want to fit in and conform: if a victim sees or believes others are performing some action, they will believe it is okay for them to do it.

Urgency / Scarcity: This needs to be done before a certain time / before something runs out. Urgency is focused on the element of time: an attacker encourages the victim to act quickly, which often leads to them making security mistakes. Urgency is related to scarcity, and the two are often effectively used together.

Familiarity / Liking / Trust: Familiarity is a social engineering technique that centers on assuming the identity of a close associate or a widely known organization, lulling you into a sense of comfort because they claim to have friends in common when in reality they've simply skimmed your Facebook & name dropped a few friends from there. Or, claiming to be from your company's IT department & helping everyone with this particular problem, all you have to do is click on some things on the screen and everything will be taken care of.

Q: Several users have contacted the help desk to report that they received an email from a well-known bank stating that their accounts have been compromised and they need to "click here" to reset their banking password. Some of these users are not even customers of this particular bank, though. Which of the following social engineering principles is being utilized as a part of this phishing campaign?

A: Familiarity

In the US, nearly 25% of Americans have a Bank of America account. For this reason, phishing campaigns often include emails pretending to be from Bank of America since 1 in 4 people who receive the email in the United States are likely to have an account. This makes them familiar with the bank name and is more likely to click on the email link. This email appears to be untargeted since it was sent to both customers and non-customers of this particular bank; it is best classified as phishing.

Q: You have just received a phishing email disguised to look like it came from support@diontraining.com asking you to send your username and password because your account has been locked out due to inactivity. Which of the following social engineering principles is being used in this email?

A: Trust

Trust is a commonly used social engineering technique during a social engineering campaign. It relies on making the email appear to have come from a trusted source, such as your IT support department or a company you frequently utilize. Often, the "display name" of the email is set to something like support@yourcompany.com or IT@yourcompany.com to trick you into replying. Trust can also be used by pretending to be someone you know and trust in real life, such as a coworker or family member.

Index

Attacks

Phishing is an **email-based social engineering attack** in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Phishing attacks target an indiscriminate large group of random people.

Vishing, aka "Voice Phishing", is the criminal practice of using social engineering over a telephone system to gain access to private personal and financial information from the public for the purpose of financial reward. It is also employed by attackers for reconnaissance purposes to gather more detailed intelligence on a target organization.

Smishing is the act of using SMS text messaging to lure victims into a specific course of action. Further, WRT OTPs, NIST's SP 800-63-3 recommends that SMS messages be deprecated as a means of delivering a second factor for multifactor authentication because they may be accessible to attackers: SMS is unable to be encrypted (at least without adding additional applications to phones) and SMS messages may be **accessible to attackers via VoIP** or other systems.

Spim is a type of spam targeting users of instant messaging (IM) services, SMS, or private messages within websites and social media.

Pretexting is a type of social engineering attack that involves a situation, or pretext, created by an attacker in order to lure a victim into a vulnerable situation and to trick them into giving private information, specifically information that the victim would typically not give outside the context of the pretext. In its history, pretexting has been described as the first stage of social engineering, and has been used even by authorities to aid in investigations. A specific example of pretexting is reverse social engineering, in which the attacker tricks the victim into contacting the attacker first.

Impersonation: Pretending or pretexting to be another person with the goal of gaining access physically to a system or building. Impersonation is used in the "SIM swap scam" fraud.

Pharming / DNS Spoofing / DNS Poisoning is a type of **social engineering attack** that redirects a request for a website, typically an e-commerce site, to a similar-looking but **fake website**. The attacker uses DNS spoofing to redirect the user to the fake site.

Shoulder Surfing is a type of social engineering technique used to obtain information such as personal identification numbers, passwords, and other confidential data by looking over the victim's shoulder. It's the attack method MOST likely to be used by a malicious employee or insider trying to obtain another user's passwords or other sensitive information!

Piggybacking attack is a social engineering attempt by cyber threat actors in which they trick employees into helping them gain unauthorized access to the company premises.

Tailgating is when an unauthorized person physically follows an authorized person into a restricted area.

The big difference between tailgating and piggybacking is permission: With tailgating, the authorized person doesn't know the unauthorized person is walking behind them. With Piggybacking, the authorized person will allow the unauthorized person to enter the secure area using the authorized person's access credentials.

Index

Study tip for Piggybacking vs Tailgating - Think of a person attempting a Piggybacking attack: they'll generally be very polite and sweet to get through and that's why you may be fooled into allowing them in. Now think of a cute little piggy giving you the "oink oink" and not being able to resist taking it in. *If it's stupid but works…!*

Cognitive Password Attacks: Cognitive Passwords are a form of knowledge-based authentication requiring a user to answer a question, presumably something they intrinsically know, to verify their identity: **If you post a lot of personal information about yourself online, this password type can easily be bypassed.** For example, during the 2008 elections, Vice Presidential candidate Sarah Palin's email account was hacked because a high schooler used the "reset my password" feature on Yahoo's email service using the information that was publicly available about Sarah Palin (like her birthday, high school, and other such information).

Q: A penetration tester hired by a bank began searching for the bank's IP ranges by performing lookups on the bank's DNS servers, reading news articles online about the bank, monitoring what times the bank's employees came into and left work, searching job postings (with a special focus on the bank's information technology jobs), and even searching the corporate office of the bank's dumpster. Based on this description, what portion of the penetration test is being conducted?

A: Passive Information Gathering

Passive Information Gathering consists of numerous activities where the penetration tester gathers open-source or publicly available information without the organization under investigation being aware that the information has been accessed.

Active Information Gathering starts to probe the organization using DNS Enumeration, Port Scanning, OS Fingerprinting techniques and even social engineering techniques!

Index

Always Use Protection…Suites & Software!

Heuristic Analysis is a method employed by many computer anti-virus programs designed to detect previously unknown computer viruses & new variants of viruses already in the wild. This is behavior-based detection & prevention, so it should detect previously unrecognized threats and stop them from spreading.

Host-based Intrusion Detection Systems (HIDS) are devices or software applications that monitor a system for malicious activity or policy violations. Any malicious activity or violation is typically reported to an administrator or collected centrally using a security information and event management system.

Unified Threat Management (UTM) Platforms enforce a variety of security-related measures, combining the work of a **firewall, malware scanner, and intrusion detection/prevention**. A UTM centralizes the threat management service, providing simpler configuration and reporting than isolated applications spread across several servers or devices.

Defense in Depth is an approach to cybersecurity in which a **series of defensive mechanisms are layered** to protect valuable data and information.

A Security Information and Event Management (SIEM) system provides **real-time analysis of security alerts** generated by applications and network hardware. SIEM is a term for software products and services combining security information management (SIM) and security event management (SEM). **A SIEM can consolidate syslog, SNMP, and event log data into a single repository.**

Security Orchestration, Automation, and Response (SOAR) is used to facilitate incident response, threat hunting, and security configuration by orchestrating automated runbooks and delivering data enrichment. A SOAR may be implemented as a standalone technology or integrated within a SIEM as a next-gen SIEM. A SOAR can scan the organization's store of security and threat intelligence, **analyze it using machine/deep learning techniques**, and then use that data to automate and provide data enrichment for the workflows that drive incident response and threat hunting.

Data loss Prevention (DLP) Software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in use (endpoint actions), in-motion (network traffic), & at rest (data storage). DLP can thus reside in multiple places: an endpoint DLP would reside on workstations and devices and examine everything transferred into or out of the device; a network-based DLP would examine network packets for data-in-transit; DLP can be present on servers and can be used to block access to certain kinds of hardware, such as USB-drives on workstations/servers; Cloud-based DLP could monitor data flows on the lookout for pre-defined strings and could block data from going to certain URLs or malware/viruses from traversing the network; lastly, DLP can be used for filtering the content of emails too!

The Microsoft Configuration Manager provides remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory. In previous Windows versions, you could use the Microsoft Baseline Analyzer (MSBA), but that is no longer supported since the introduction of Windows 10.

Microsoft Configuration Manager was formerly known as Microsoft Endpoint Configuration Manager (MECM), System Center Configuration Manager (SCCM) and Systems Management Server (SMS)

Index

Update Compliance Tool can be used in an Azure environment to monitor your device's Windows updates, Windows Defender anti-virus status, and the up-to-date patching status across all of your Windows 10 workstations.

Endpoint Security includes software host-based firewalls, host-based intrusion protection systems (HIPS), and anti-virus software.

Anti-malware software is a program that scans a device or network for known viruses, Trojans, worms, and other malicious software.

Firewalls are **network security devices** that monitor & filter incoming & outgoing network traffic based on an organization's previously established security policies. An Access Control List could define what ports, protocols, or IP addresses the ethernet port could be utilized. According to the best practices of firewall configurations, you should include an implicit deny at the end of your ACL rules. This will ensure that anything not specifically allowed in the rules above is blocked.

Microsoft's Group Policy Object (GPO) is a collection of Group Policy settings that defines what a system will look like and how it will behave for a defined group of users. A Group Policy is the primary administrative tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization. In an active directory environment, Group Policy is applied to users or computers based on their membership in sites, domains, or organizational units.

Secure Boot is a security system offered by the Unified Extensible Firmware Interface (UEFI) forum. It is designed to **prevent a computer from being hijacked by a malicious OS**. Under secure boot, UEFI is configured with **digital certificates from valid OS vendors**. The system firmware checks the OS boot loader using the stored certificate to ensure that it has been digitally signed by the OS vendor. This prevents a boot loader that has been changed by malware (or an OS installed without authorization) from being used. Also used to ensure that compromised BIOS images are not present and loaded up.

A Behavior-based Analysis Tool can capture/analyze normal behavior and then alert when an anomaly occurs. Configuring a behavior-based analysis tool requires more effort to set up properly, but it requires less work and manual monitoring once it is running. These tools can be used to detect unexpected output from an application being managed or monitored.

Signature-based Detection is a process where a unique identifier is established about a known threat so that the threat can be identified in the future.

Measured Boot is a feature where a log of all boot actions is taken and stored in a trusted platform module for later retrieval and analysis by anti-malware software on a remote server. It's an OS feature designed to detect malware that is loaded early in the system startup process or before the operating system can load itself.

Master Boot Record Analysis is used to capture the hard disk's required information to support a forensic investigation. It would not detect malware during the system's boot-up process.

Startup Control would be used to determine which programs will be loaded when the operating system is initially booted, but this would be too late to detect malware loaded during the pre-startup and boot process.

Advanced Anti-Malware Solutions are programs that are loaded within the operating system. Therefore, they are loaded too late in the startup process to be effective against malicious boot sector viruses and other BIOS/UEFI malware variants.

Index

Q: Which type of antivirus scan provides the best protection for a typical home user?

A: On-access scans

On-access scans are a type of antivirus scan where the AV software intercepts operating system calls to open files to scan the file before allowing or preventing the file from being opened. On-access scans reduce performance somewhat but are essential to maintaining effective protection against malware. Weekly and daily scans are good to use, but they are not as effective in preventing infections as an on-access scan. A system administrator normally conducts safe mode scans after malware is found by an on-access, daily, or weekly scan.

Q: A cybersecurity analyst has deployed a custom DLP signature to alert on any files that contain numbers in the format of a social security number (xxx-xx-xxxx). Which of the following concepts within DLP is being utilized?

A: Exact data match

Q: A corporate workstation was recently infected with malware. The malware was able to access the workstation's credential store and steal all the usernames and passwords from the machine. Then, the malware began to infect other workstations on the network using the usernames and passwords it stole from the first workstation. The IT Director has directed its IT staff to develop a plan to prevent this issue from occurring again. Which of the following would BEST prevent this from reoccurring?

A: Install an anti-virus or anti-malware solution that uses heuristic analysis

The only solution that could stop this from reoccurring would be to use an anti-virus or anti-malware solution with heuristic analysis. The other options (monitor SYSLOG server logs, install a HIDS or UTM) might be able to monitor and detect the issue but not stop it from spreading.

Q: A network administrator, Tamera, follows the best practices to implement firewalls, patch management, and security policies on his network. Which of the following should be performed to verify that the security controls are in place?

A: Penetration Testing

Penetration testing or Pentesting is the practice of testing a computer system, network, or web application in order to find vulnerabilities that an attacker could exploit. It can be used to ensure all security controls are properly configured and in place.

Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. Testing AAA might be a part of a larger penetration test, but by itself it would not test the firewalls and patch management systems sufficiently.

Index

A Disaster Recovery Test (DR test) is the examination of each step in a disaster recovery plan as outlined in an organization's business continuity/disaster recovery planning process. A disaster recovery test would not test the firewalls, patch management, or security policies.

A Single Point-of-Failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. A single point of failure test is used to identify a single point of failure in the network or system, and it is not designed to test the network's firewalls, patch management, or security policies.

Q: Which of the following is not normally part of an endpoint security suite?

A: VPN (NOT IPS): A VPN is not typically considered an endpoint security tool as it's a network security tool.

Q: A network technician is selecting the best way to protect a branch office from as many different threats from the Internet as possible using a single device. Which of the following should meet these requirements?

A: Configure a UTM Device

Since this is a branch office and you want to protect it from as many threats as possible, using a Unified Threat Management (UTM) device would be best as a UTM will protect you from most things using a single device.

Q: You are investigating a suspected compromise. You have noticed several files that you don't recognize. How can you quickly and effectively check if the files have been infected with malware?

A: Submit the files to an open-source intelligence provider like VirusTotal.

The best option is to submit them to an open-source intelligence provider like VirusTotal. VirusTotal allows you to quickly analyze suspicious files and URLs to detect types of malware. It then automatically shares them with the security community, as well. Disassembly and static analysis would require a higher level of knowledge and more time to complete. Running the Strings tool can help identify text if the code is not encoded in a specific way within the malware, but you have to know what you are looking for, such as a malware signature. You should never scan the files using a local anti-virus or anti-malware engine if you suspect the workstation or server has already been compromised because the scanner may also be compromised.

Q: Ryan needs to verify the installation of a critical Windows patch on his organization's workstations. Which method would be the most efficient to validate the current patch status for all of the organization's Windows 10 workstations?

A: Use an endpoint manager to validate patch status for each machine on the domain

Index

Q: You have been asked to recommend a capability to monitor all of the traffic entering and leaving the corporate network's default gateway. Additionally, the company's CIO requests to block certain content types before it leaves the network based on operational priorities. Which of the following solution should you recommend meeting these requirements?

A: Install a NIPS on the internal interface and a firewall on the external interface of the router

The firewall on the external interface will allow the bulk of the malicious inbound traffic to be filtered before reaching the network. Then, the NIPS can be used to inspect the traffic entering the network and provide protection for the network using signature-based or behavior-based analysis. A NIPS is less powerful than a firewall and could easily "fail open" if it is overcome with traffic by being placed on the external interface.

We would not want to rely on a NIDS on the external interface alone since it can only monitor and not provide the content blocking capabilities needed.

Q: You are reviewing a rule within your organization's IDS. You see the following output:


```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
msg: “BROWSER-IE Microsoft Internet Explorer
CacheSize exploit attempt”;
flow: to_client,established;
file_data;
     content:"recordset"; offset:14; depth:9;
     content:".CacheSize"; distance:0; within:100;
     pcre:"/CacheSize\s*=\s*/";
     byte_test:10,>,0x3ffffffe,0,relative,string;
max-detect-ips drop, service http;
reference:cve,2016-8077;
classtype: attempted-user;
sid:65535;rev:1;
```

Based on this rule, which of the following malicious packets would this IDS alert on?

A: A malicious inbound TCP packet

The rule header is set to alert only on TCP packets based on this IDS rule's first line. The flow condition is set as "to_client, established," which means that only inbound traffic will be analyzed against this rule and only inbound traffic for connections that are already established. Therefore, this rule will alert on an inbound malicious TCP packet only when the packet matches all the conditions listed in this rule.

Index

This rule is an example of a Snort IDS rule. For the exam, you do not need to create your own IDS rules, but you should be able to read them and pick out generic content like the type of protocol covered by the signature, the port to be analyzed, and the direction of flow.

Q: Which of the following security controls provides Windows system administrators with an efficient way to deploy system configuration settings across many devices?

Options: GPO, Anti-malware, Patch management, HIPS

A: GPO

Q: A cybersecurity analyst is working at a college that wants to increase its network's security by implementing vulnerability scans of centrally managed workstations, student laptops, and faculty laptops. Any proposed solution must scale up and down as new students and faculty use the network. Additionally, the analyst wants to minimize the number of false positives to ensure accuracy in their results. The chosen solution must also be centrally managed through an enterprise console. Which of the following scanning topologies would be BEST able to meet these requirements?

A: Active scanning engine installed on the enterprise console

Since the college wants to ensure a centrally-managed enterprise console, an active scanning engine installed on the enterprise console would best meet these requirements. The college's cybersecurity analysts could then perform scans on any devices connected to the network using the active scanning engine at the desired intervals.

Agent-based scanning would be ineffective since the college cannot force the agents' installation onto each of the personally owned devices brought in by the students or faculty.

A cloud-based or server-based engine may be useful, but it won't address the centrally-managed requirement.

Passive scanning is less intrusive but is subject to a high number of false positives.

Q: As a cybersecurity analyst conducting vulnerability scans, you have just completed your first scan of an enterprise network comprising over 10,000 workstations. As you examine your findings, you note that you have less than 1 critical finding per 100 workstations. Which of the following statement does BEST explain these results?

A: An uncredentialed scan of the network was performed

Uncredentialed scans are generally unable to detect many vulnerabilities on a device. When conducting an internal assessment, you should perform an authenticated (credentialed) scan of the environment to determine the network's vulnerability posture most accurately: Credentialed scans log into a system and retrieve their configuration information and therefore provide the best results if you want to determine if the target's configuration settings are correct.

Index

In most enterprise networks, if a vulnerability exists on one machine, it also exists on most other workstations since they use a common baseline or image.

If the scanner failed to connect to the workstations, an error would have been generated in the report.

Q: You are working as a junior cybersecurity analyst and utilize a SIEM to support investigations into ongoing incidents. The SIEM is configured to collect data from numerous sources across the network, including network sensors, routers, switches, firewalls, hosts, and servers. Unfortunately, due to the number of data sources, you have data about a particular event being detected by different sensors and devices. Which of the following must you ensure to make sense of all the data being collected by your SIEM before analyzing it?

A: Data Correlation (NOT Data Sanitization!)

Data correlation is the first step in making sense of data from across numerous sensors. This will ensure the data is placed concerning other pieces of data within the system. For example, if your IDS detected an incident, host logs were collected, and your packet capture system collected the network traffic, the SIEM could be used to correlate all three pieces of information from these different systems to allow an analyst to understand the event better, to identify a pattern more clearly and take action. Data correlation should be performed as soon as the SIEM indexes the data.

Q: Dion Training wants to implement technology within their corporate network to BEST mitigate the risk that a zero-day virus might infect their workstations. Which of the following should be implemented FIRST?

A: Application Allow List! (NOT IDS, which only log and do not prevent)

As all other programs are blocked from running, this makes it the BEST mitigation against a zero-day.

Q: A cybersecurity analyst just finished conducting an initial vulnerability scan and is reviewing their results. To avoid wasting time on results that are not related to actual vulnerabilities, the analyst wants to remove any false positives before remediating the findings. Which of the following is an indicator that something in their results would be a false positive?

A: Items classified by the system as 'Low' or 'For Informational Purposes Only'

When conducting a vulnerability scan, it is common for the report to include some findings that are classified as "low" priority or "for informational purposes only." These are most likely false positives and can be ignored by the analyst when starting their remediation efforts.

"An HTTPS entry that indicates the web page is securely encrypted" is not a false positive but a true negative (a non-issue).

A scan result showing a different version from the automated asset inventory should be investigated and is likely a true positive. A finding that shows the scanner compliance plug-ins are not up-to-date would likely also be a true positive that should be investigated.

Index

Stateful vs Stateless Firewalls

Stateless firewalls are designed to protect networks based on static information such as source and destination. Whereas *stateful* firewalls filter packets based on the full context of a given network connection, stateless firewalls filter packets based on the individual packets themselves.

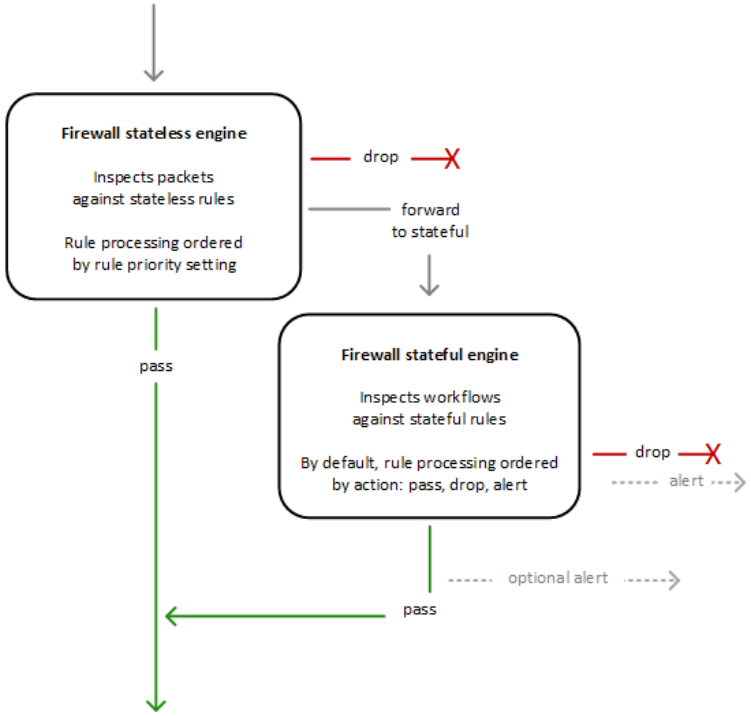
Stateless firewalls check individual packets before deciding whether or not to permit them, while stateful firewalls are able to track the movement of packets around a network, building profiles to better recognize safe & unsafe connections at the source.

Nice analogy by EnterpriseNetworkingPlanet: "*Firewalls are like club bouncers—they decide who gets in and stays out. Stateful firewalls are the experienced bouncer, who knows precisely who is coming and going and can recognize familiar faces. They keep track of all the connections that pass through them, ensuring that only authorized traffic is allowed to pass.*

Stateless firewalls, on the other hand, are the rookie bouncer who just checks ID at the door without keeping track of comings and goings. They don't recognize any connections and simply check each packet individually to see if it matches their predetermined ruleset."

Stateless rules engine – Inspects each packet in isolation, without regard to factors such as the direction of traffic, or whether the packet is part of an existing, approved connection. This engine prioritizes the speed of evaluation.

Stateful rules engine – Inspects packets in the context of their traffic flow, allows you to use more complex rules, and allows you to log network traffic and to log 'Network Firewall' firewall alerts on traffic. Stateful rules consider traffic direction. The stateful rules engine might delay packet delivery in order to group packets for inspection.



AWS Network Firewall – Rules Engine

Q: A network administrator needs to install a centrally located firewall that needs to block specific incoming and outgoing IP addresses without denying legitimate return traffic. Which type of firewall should the administrator install?

A: A Stateful Network-based Firewall

Index

Q: A firewall technician at Dion Training configures a firewall to allow HTTP traffic as follows:

Source IP	Zone	Dest IP	Zone	Port	Action
Any	Untrust	Any	DMZ	80	Allow

Dion Training is afraid that an attacker might try to send other types of network traffic over port 80 to bypass their security policies. Which of the following should they implement to prevent unauthorized traffic from entering through the firewall?

A: Application-aware firewall

An application-aware firewall can make decisions about what applications are allowed or blocked by a firewall, as opposed to simply using IP addresses and port numbers, by applications by inspecting the data contained within the packets. A stateless packet inspection firewall allows or denies packets into the network based on the source and destination IP address or the traffic type (TCP, UDP, ICMP, etc.).

A stateful packet inspection firewall monitors the active sessions and connections on a network. The process of stateful inspection determines which network packets should be allowed through the firewall by utilizing the information it gathered regarding active connections as well as the existing ACL rules. Neither a stateless nor stateful inspection firewall operates at layer 6 or layer 7, so they cannot inspect the contents of the packet to ensure it contains HTTP traffic and nor other types of network traffic.

HTTPS (SSL/TLS) would allow for an encrypted communication path between the webserver and the client, but this would not prevent an attacker from sending other network protocol data over port 80 and bypassing the firewall rules.

Q: A new piece of malware attempts to exfiltrate user data by hiding the traffic and sending it over a TLS-encrypted outbound traffic over random ports. What technology would be able to detect and block this type of traffic?

A: Application-aware firewall

Q: Your deep packet inspection firewall is dropping portions of your packet flow as it enters or leaves the network. The network is configured to use HSRP to load balance traffic across two network devices in a high availability cluster. Which of the following issues would cause your network security devices, such as your firewalls, to drop packet flows and cause intermittent network connectivity to your clients?

A: Asymmetric Routing

Q:A network technician wants to allow HTTP traffic through a stateless firewall. The company uses the 192.168.0.0/24 network. Which of the following ACLs should the technician implement?

A: PERMIT SCRIP 192.168.0.0/24 SPORT: ANY DSTIP: ANY DPORT: 80

Index

Q: Riaan's company runs critical web applications. During a vulnerability scan, Riaan found a serious SQL injection vulnerability in one of their web applications. The system cannot be taken offline to remediate the vulnerability. Which of the following compensating controls should Riaan recommend using until the system can be remediated?

A:Web Application Firewall (WAF)

WAF (web application firewall) is the best option since it can serve as a compensating control and protect against web application vulnerabilities like an SQL injection until the application can be fully remediated.

Vulnerability scanning could only be used to detect the issue. Therefore, it is a detective-control, not a compensating control. Encryption would not be effective in stopping an SQL injection.

An intrusion prevention system (IPS) is designed to protect network devices based on ports, protocols, and signatures. It would not be effective against an SQL injection and is not considered a compensating control for this vulnerability.

Detection Techniques

Behavior-based Detection (or Statistical- or Profile-based Detection) means that the engine is trained to recognize baseline traffic or expected events associated with a user account or network device. Anything that deviates from this baseline (outside a defined level of tolerance) generates an alert.

Heuristic Analysis determines whether several observed data points constitute an indicator and whether related indicators make up an incident depending on a good understanding of the relationship between the observed indicators.

Human Analysts are typically good at interpreting context but work painfully slowly, in computer terms, and cannot hope to cope with the sheer volume of data and traffic generated by a typical network.

Anomaly Analysis is the process of defining an expected outcome or pattern to events and then identifying any events that do not follow these patterns. This is useful in tools and environments that enable you to set rules.

Trend Analysis is not used for detection but instead to better understand capacity and the system's normal baseline.

Behavioral-based detection differs from anomaly-based detection: *Behavioral-based detection records expected patterns concerning the entity being monitored (in this case, user logins). Anomaly-based detection prescribes the baseline for expected patterns based on its observation of what normal looks like.*

Q: Alexa is an analyst for a large bank that has offices in multiple states. She wants to create an alert to detect if an employee from one bank office logs into a workstation located at an office in another state. What type of detection and analysis is Alexa configuring?

A: Behavior

Index

Managed Security Service Providers (MSSP)

Q: Nicole's organization does not have the budget or staff to conduct 24/7 security monitoring of their network. To supplement her team, she contracts with a managed SOC service. Which of the following services or providers would be best suited for this role?

A: MSSP

A Managed Security Service Provider (MSSP) provides Security as a Service (SECaaS). IaaS, PaaS, and SaaS (infrastructure, platform, and software as a service) do not include security monitoring as part of their core service offerings. Security as a service or a Managed Service Provider (MSP) would be better suited for this role.

This question may seem beyond the exam scope. Still, the objectives allow for it: "other examples of technologies, processes, or tasks about each objective may also be included on the exam although not listed or covered". The exam tests the equivalent of 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of this examination's content. Therefore, questions like this are fair game on test day. That said, your goal isn't to score 100% on the exam; it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

Trusted Platform Module (TPM)

Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software cannot tamper with the security functions of the TPM.

The TPM provides random number generation, secure generation of cryptographic keys, remote attestation, binding, and sealing functions securely.

Index

Wireless Network Security

WEP: The Wired Equivalent Privacy (WEP) encryption system **is based on the RC4 encryption cipher**. WEP uses a **40-bit encryption key and a 24-bit initialization vector by default, creating a 64-bit key**. Newer versions of WEP support a 128-bit key size. A larger encryption key creates stronger encryption and is more difficult to attack. WEP is **considered weak by today's standards** and should be replaced by WPA2 or strong encryption schemes.

WPA: Wi-Fi Protected Access (WPA) is an improved encryption scheme for protecting Wi-Fi communications designed to **replace WEP**. WPA uses the **RC4 cipher and a Temporal Key Integrity Protocol (TKIP)** to overcome the vulnerabilities in the older WEP protection scheme.

WPA2: Wi-Fi Protected Access 2 Pre-Shared Key or WPA2-PSK is a system of encryption used to authenticate users on wireless local area networks using a shared password as the key. WPA2-PSK [AES] is the recommended secure method of making sure no one can listen to your wireless data while it is being transmitted back and forth between your router and other devices on your network. WPA2 replaced the original version of WPA after the completion of the 802.11i security standard.

WPA2 features an improved method of key distribution and authentication for enterprise networks via WPA2 Enterprise, though the pre-shared key method is still available for home and small office networks via WPA2 Personal. WPA2 uses the **improved AES cipher with counter mode with Cipher-block Chaining Message Authentication Protocol (CCMP)** for encryption. WPA2 Enterprise requires a RADIUS authentication server to be used with individual usernames and passwords for each client, rather than a PSK.

WPA3: Wi-Fi protected access version 3 (WPA3) has **replaced WPA2 as the most secure** wireless encryption method. WPA3 uses the **Simultaneous Authentication of Equals (SAE)** password-based authentication & password-authenticated key agreement method to increase the security of pre-shared keys, and **replaces the 4-way handshake used in WPA-**based wireless networks. The SAE handshake is also known as the **dragonfly handshake**.

WPA3 provides an **enhanced open mode** that encrypts transmissions from a client to the access point when using an open network.

WPA3 Enterprise mode supports the use of AES with the Galois Counter Mode Protocol (GCMP-256) for the highest levels of encryption. AES GCMP is a high-performance mode of operation for symmetric encryption that supports **Authenticated Encryption with Associated Data (AEAD)**. Management protection frames protect unicast and multicast management action frames to protect against eavesdropping and forgery in WPA3-based wireless networks.

WPS: The Wi-Fi Protected Setup (WPS) is a **mechanism for auto-configuring a WLAN securely** for home users. On compatible equipment**, users push a button** on the access point and connect adapters to associate them securely. WPS is subject to brute force attacks against the PIN used to secure them, making them vulnerable to attack. The 8-digit PIN is susceptible to brute-force attacks as WPS, checks each half of the PIN individually, reducing the number of possible combinations from a maximum of 100,000,000 to only 11,000.

A WEP Attack is a **brute force password attack** conducted against a wireless network that relies on WEP for its encryption and security.

Index

Q: Which of the following encryption types was used by WPA to better secure wireless networks than WEP?

A: TKIP

Q: The administrator would like to use the strongest encryption level possible using PSK without utilizing an additional authentication server. What encryption type should be implemented?

A: WPA Personal or WPA2 Personal

Since he wishes to use a pre-shared key and not require an authentication server, WPA personal is the most secure choice. WPA2 Enterprise is incorrect since the requirement was for a PSK, whereas WPA2 Enterprise requires a RADIUS authentication server to be used with individual usernames and passwords for each client. MAC filtering does not use a password or pre-shared key (PSK). WEP uses a pre-shared key to secure a wireless network, but WPA uses a stronger encryption standard than WEP.

Q: Which attack utilizes a wireless access point made to look as if it belongs to the network by mimicking the corporate network's SSID to eavesdrop on the wireless traffic?

A: Evil Twin, as it's impersonating an official WAP by mimicking the SSID of the corporate network

Q: Joanne is having a drink at the coffee shop near her office. She takes out her Windows 10 laptop & connects it to the coffee shop's wireless network to check her email. Which type of network should she select to hide their computer from other devices on the network & prevent file sharing with other patrons?

A: Public

When connecting to a network for the first time, the user must select if it is a public or private network. A public network will hide your computer from other devices on the network & prevent file & printer sharing. A private network is considered trusted, allows the computer to be discoverable to other devices on the network, & supports the use of file & printer sharing. In older versions of Windows, there were also Home & Work network types, but those have since been merged into public & private network types, as well.

Least Privilege vs Zero-Trust

Least privilege is the concept and practice of **restricting access rights** for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.

Privilege itself refers to the authorization to bypass certain security restraints.

Zero-trust is a security framework that requires all users, whether in or outside the organization's network, to be authenticated, authorized, and **continuously validated** for security configuration and posture before being granted or keeping access to applications and data.

Index

Threat Hunting is the utilization of insights gained from threat research and threat modeling to proactively discover evidence of adversarial **TTP (Threats, Techniques, and Procedures)** within a network or system.

Penetration Testing uses active tools and security utilities to evaluate security by simulating an attack on a system. A penetration test verifies that a threat exists, actively tests, and bypasses security controls, and finally exploits vulnerabilities on the system.

- An Unknown Environment Penetration Test **requires no previous information** and usually takes the approach of an **uninformed attacker.** The penetration tester has no prior information about the target system or network in an unknown environment penetration test. **These tests provide a realistic scenario** for testing the defenses, but they can be costlier and more time-consuming to conduct as the tester is examining a system from an outsider's perspective.
- A Partially Known Environment Tester has the **user's access and knowledge levels, potentially with elevated privileges on a system**. These partially known environment penetration testers typically have some knowledge of a network's internals, potentially including design and architecture documentation and an account internal to the network.
- A Known Environment Test is known by several different names, including **clear-box, open-box, auxiliary, or logic-driven testing**. It falls on the **opposite end of the spectrum from an unknown environment test** because the penetration testers have **full access to source code, architecture documentation, and so forth**. A known environment penetration tester can also perform **static code analysis**, so familiarity with source code analyzers, **debuggers**, and similar tools are necessary for this type of testing.
- *A Semi-Trusted Environment Test is made-up term & may be used as a distractor on the test!*

Hardening is usually the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle, a single-function system is more secure than a multipurpose one. Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling or removal of unnecessary services. **Stealthing is a made-up tersm on the exam!**

Information Assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.

Incident Response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident, or security incident. The goal is to handle the situation to limit damage and reduce recovery time and costs.

Password Authentication Protocol (PAP): A username and password are used as part of the PAP authentication system. A username and password are also considered a knowledge factor in an authentication system.

Geofences are a virtual perimeter for a real-world geographic area. Geofencing does not use shared passwords for security, it uses GPS coordinates or other location-based data.

Index

A Jump-box System is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them. A Jumpbox would create network segmentation between an organization's network and devices managed independently by a third-party.

A Bastion Host is a special-purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application. For example, a proxy server and all other services are removed or limited to reduce the threat to the computer.

An Airgap System is a network or single host computer with unique security requirements that may physically be separated from any other network. Physical separation would prevent a system from accessing the remote administration interface directly and require an airgap system to reach the private cloud. The only way to cross an air gap is to have a physical device between these systems, such as using a removable media device to transfer files between them.

Q: You want to provide controlled remote access to the remote administration interfaces of multiple servers hosted on a private cloud. What type of segmentation security solution is the best choice for this scenario?

A: Jumpbox (NOT Bastion Host!)

Installing a jumpbox as a single point of entry for the administration of servers within the cloud is the best choice for this requirement. The jumpbox only runs the necessary administrative port and protocol (typically SSH). Administrators connect to the jumpbox then use the jumpbox to connect to the admin interface on the application server. The application server's admin interface has a single entry in its ACL (the jumpbox) and denies any other hosts' connection attempts.

HMAC-based One-Time Password (HOTP) is a **one-time password algorithm for token-based authentication** based on Hash-based Message Authentication Codes (HMAC). The token could be a fob-type device or implemented as a smartphone app. The token does not have an expiration under HOTP, but an improved version known as TOTP does include token expirations. One issue with HOTP is that tokens can be allowed to persist unexpired, raising the risk that an attacker might obtain one and decrypt data in the future.

*↳ In cryptography, a Message Authentication Code (MAC), sometimes known as an **authentication tag**, is a short piece of information used for authenticating a message. In other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed. The MAC value protects a message's data integrity, as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.*

Time-based One-Time Password (TOTP) is a computer algorithm that generates a **one-time password that uses the current time** as a source of uniqueness**. TOTP is a refinement of the HOTP:** involves receiving a one-time-use, shared-secret password, usually, through a token-based key fob or smartphone app, that automatically expires after a short period of time (for example, 60 seconds). In TOTP, the HMAC is built from the shared secret plus a value derived from the device's and server's local timestamps.

Context-based Authentication can consider several factors before permitting access to a user, including their location (e.g., country, GPS location, etc.), the time of day, and other key factors to minimize the threat of compromised credentials from being utilized by an attacker.

Index

A Cloud Access Security Broker (CASB) can be used to prevent unauthorized use of cloud services from the local network.

Proxy Servers: A proxy server is a **web server that acts as a gateway** between a client application. To route all of the workstation's internet traffic to the proxy server, a technician should configure the proxy server address under the Connections tab of the Internet Options section of the Control Panel.

A Reverse Proxy is positioned at the cloud network edge & directs traffic to cloud services **if the contents of that traffic comply with the policy.** This does not require the configuration of the users' devices. This approach is only possible if the cloud application has proxy support. You can deploy a reverse proxy & configure it to listen for client requests from a public network, like the internet. The proxy then creates the appropriate request to the internal server on the corporate network & passes the server's response back to the external client. They are not generally intended to obfuscate the source of communication, nor are they necessarily specific to the cloud.

The Default Gateway parameter is the IP address of a router to which packets destined for a remote network should be sent by default.

The Subnet Mask is used to identify the host identifier and the network identifier uniquely in combination with the IP address. The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or a remote network.

Q: You are configuring a Windows 10 Professional workstation to connect to the Dion Training domain. To provide additional security to its users, Dion Training requires that all uses route their internet traffic through a server located at 10.0.0.15 for inspection before it is sent to the internet. Once inspected, the server will route the traffic to the WAN router whose IP is 10.0.0.1. Which of the following settings should be configured on the workstation to achieve this?

A: Under Internet Options, configure the proxy server address as 10.0.0.15

The Internet Options section of the Control Panel allows a technician to manage the Internet settings for their computers, including the security settings, access settings, and add-on control settings. Using Internet Options, a technician can set the homepage of the browser, set up the proxy server connection details, and change the trust and security settings used by the system. Remember it as "IO" for input/output of traffic!

DHCP Snooping is a layer 2 security technology incorporated into the OS of a capable (managed) network switch that drops DHCP traffic determined to be unacceptable. This prevents unauthorized (rogue) DHCP server from offering IP addresses to clients. DHCP Snooping validates that DHCP messages are from trusted sources, building & maintaining a DHCP Snooping Binding Database of untrusted hosts with leased IP addresses, and utilizes that DB to validate subsequent requests from untrusted hosts.

Dynamic ARP Inspection (DAI) is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings.

Windows Internet Name Service (WINS) is a legacy computer name registration and resolution service that maps computer NetBIOS names to IP addresses.

Index

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service. RADIUS is an application-layer client/server protocol, with a server component usually running as a background process on UNIX or Windows. The RADIUS protocol utilizes an obfuscated password created from the shared secret and creates an MD5 hash of the authentication request to protect the communications.

Terminal Access Controller Access-Control System or TACACS+ is a AAA (accounting, authorization, and authentication) protocol **developed by CISCO** to provide AAA services for access to routers, network access points, & other networking devices. It's a remote authentication protocol, which allows a remote access server to communicate with an authentication server to validate user access onto the network. **TACACS+ allows a client to accept a username & password & pass a query to a TACACS+ authentication server. TACACS+ is an older username and login system that uses authentication to determine access, while RADIUS combines authorization AND authentication.**

Q: Which of the following provides accounting, authorization, and authentication via a centralized privileged database, as well as challenge/response and password encryption?

A: TACACS+

Q: Dion Training uses an authentication protocol to connect a network client to a networked file server by providing its authentication credentials. The file server then uses the authentication credentials to issue an authentication request to the server running this protocol. The server can then exchange authentication messages with the file server on behalf of the client. Throughout this process, a shared secret is used to protect the communication. Which of the following technologies relies upon the shared secret?

A: RADIUS

Q: Your company wants to provide a secure SSO solution for accessing both the corporate wireless network and its network resources. Which of the following technologies should be used?

&

Q: A company is installing several APs for a new wireless system that requires users to authenticate to the domain. The network technician would like to authenticate to a central point. What solution would be BEST to achieve this?

A: RADIUS

With RADIUS & SSO configured, users on the network can provide their user credentials one time when they initially connect to the wireless access point or another RADIUS client and are then automatically authenticated to all of the network's resources. The Remote Authentication Dial-in User Service (RADIUS) is used to manage remote & wireless authentication infrastructure. Users supply authentication information to RADIUS client devices, such as WAPs. The client device then passes the authentication data to an AAA server that processes the request. The Terminal Access Controller Access Control System (TACACS+) is a proprietary alternative to RADIUS developed by Cisco for handling authentication.

Index

Q: A technician has finished configuring AAA on a new network device. However, the technician cannot log into the device with LDAP credentials but can with a local user account. What is the MOST likely reason for the problem?

A: Shared secret key is mismatched

AAA through RADIUS uses a Server Secret Key (a shared secret key). A secret key mismatch could cause login problems. A shared secret is a text string that serves as a password between hosts.

Challenge-Handshake Authentication Protocol (CHAP) is used to authenticate a user or network host to an authenticating entity. CHAP is an authentication protocol but does not provide authorization or accounting.

Kerberos is a network authentication protocol designed to provide strong mutual authentication for client/server applications using secret-key cryptography developed by MIT. Kerberos is a computer network authentication protocol that works **based on tickets** to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. **Kerberos is used in Windows Active Directory domains for authentication.**

A Network Tap is used to create a physical connection to the network that sends a copy of every packet received to a monitoring device for capture and analysis.

A DMZ (Demilitarized Zone), a type of screened subnet, is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network such as the Internet.

Q: Jack is assessing the likelihood of reconnaissance activities being performed against his organization. Which of the following would best classify the likelihood of a port scan being conducted against his DMZ?

A: High

Since Jack's DMZ would contain systems and servers exposed to the Internet, there is a high likelihood that they are constantly being scanned by potential attackers performing reconnaissance.

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is an XML-based markup language for security assertions.

Active Directory Federation Services (ADFS) is a software component developed by Microsoft that can run on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries.

The Lightweight Directory Access Protocol (LDAP) uses a client-server model for mutual authentication. LDAP is used to enable access to a directory of resources (workstations, users, information, etc.). TLS provides mutual authentication between clients and servers. Since Secure LDAP (LDAPS) uses TLS, it provides mutual authentication of the client and the server.

Q: Which of the following network devices would be considered a perimeter device and installed at the outermost part of the network?

A: Firewall

Index

Q: Your company has just installed a new web server that will allow inbound connections over port 80 from the internet while not accepting any connections from the internal network. You have been asked where to place the web server in the network architecture and configure the ACL rule to support the requirements. The current network architecture is segmented using a triple-homed firewall to create the following three zones: ZONE INTERFACE, IP address ---------- PUBLIC, eth0, 66.13.24.16/30 DMZ, eth1, 172.16.1.1/24 PRIVATE, eth2, 192.168.1.1/24 Based on the requirements and current network architecture above, where should you install the webserver and how should you configure it?

A: Put the server in the DMZ with an inbound rule from eth0 to eth1 that allows port 80 traffic to the server's IP

Router Advertisement Guard: In an IPv6 deployment, routers periodically multicast Router Advertisement (RA) messages to announce their availability and convey information to neighboring nodes that enable them to be automatically configured on the network. RA messages are used by Neighbor Discovery Protocol (NDP) to detect neighbors, advertise IPv6 prefixes, assist in address provisioning, and share link parameters such as maximum transmission unit (MTU), hop limit, advertisement intervals, and lifetime. Hosts listen for RA messages for IPv6 address autoconfiguration and discovery of link-local addresses of the neighboring routers, and can also send a Router Solicitation (RS) message to request immediate advertisements.

RA messages are unsecured, which makes them susceptible to attacks on the network that involve the spoofing (or forging) of link-layer addresses. The IPv6 Router Advertisement Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement guard messages that arrive at the network device platform.

A Honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a website) that appears to be a legitimate part of the site which contains information or resources of value to attackers. It is actually isolated, monitored, and capable of blocking or analyzing the attackers. This is similar to police sting operations, colloquially known as "baiting" a suspect. A honeypot is a single machine and cannot detect threats against an entire network.

A Remote Access Server (RAS) or remote desktop gateway is a type of server that provides a suite of services to connect users to a network or the Internet remotely.

The Domain Name System Security Extensions (DNSSEC) is a suite of extension specifications by the Internet Engineering Task Force for securing data exchanged in the Domain Name System in IP networks.

MAC Filtering: MAC addresses are permanently burned into the network interface card by the manufacturer and serve as the device's physical address, therefore WAPs can utilize MAC filtering to ensure only known network interface cards are allowed to connect to the network. If a hacker changes their MAC address to a trusted MAC address though, they can easily bypass this security mechanism. MAC filtering is considered a good security practice as part of a larger defense-in-depth strategy, but it won't stop a skilled hacker for long!

A Wildcard Certificate is a public key certificate that can be used with multiple subdomains of a domain. This saves money and reduces the management burden of managing multiple certificates, one for each subdomain. A single wildcard certificate for *.diontraining.com will secure all these domains (www.diontraining.com, mail.diontraining.com, ftp.diontraining.com, etc.).

Index

Sponsored Authentication of guest wireless devices requires a guest user to **provide valid identification when registering their wireless device** for use on the network. This requires that an employee validates the guest's need for access, known as sponsoring the guest.

Q: An organization wants to choose an authentication protocol that can be used over an insecure network without implementing additional encryption services. Which of the following protocols should they choose?

A: Kerberos

The Kerberos protocol is designed to send data over insecure networks while using strong encryption to protect the information. RADIUS, TACACS+, and PAP are all protocols that contain known vulnerabilities that would require additional encryption to secure them during the authentication process.

Q: The corporate network uses a centralized server to manage credentials for all of its network devices. What type of server is MOST likely being used in this configuration?

A: RADIUS or TACACS

Q: You are notified by an external organization that an IP address associated with your company's email server has been sending spam emails requesting funds as part of a lottery collection scam. An investigation into the incident reveals the email account used was Connor from the sales department and that Connor's email account was only used from one workstation. You analyze Connor's workstation and discover several unknown processes running, but NetFlow analysis reveals no attempted lateral movement to other workstations on the network. Which containment strategy would be most effective to use in this scenario?

A: Isolate the workstation computer by disabling the switchport and resetting Connor's username/password

Isolation of Connor's computer by deactivating the port on the switch should be performed instead of just unplugging the computer. This would guarantee that Connor won't just plug the computer back into the network as soon as you leave his desk.

While we are unsure of the issue's initial root cause, we know it is currently isolated to Connor's machine. So, it's better to isolate just Connor's machine instead of the entire network segment in this scenario. Isolating the network segment, without evidence indicating the need to do so, would have been overkill and overly disruptive to the business.

Reimaging Connor's device may destroy data that could have otherwise been recovered and led to a successful root cause analysis, and thus should be avoided.

There is also insufficient evidence in this scenario to warrant disciplinary action against Connor, as he may have clicked on a malicious link by mistake. He should receive remedial cybersecurity training, his workstation's hard drive forensically imaged for later analysis, and then his workstation should be remediated or reimaged.

Index

Q: The management at Steven's work is concerned about rogue devices being attached to the network. Which of the following solutions would quickly provide the most accurate information that Steve could use to identify rogue devices on a wired network?

A: Router & Switch-based MAC Address Reporting (NOT a discovery scan via a port scanner!)

The best option is MAC address reporting from a source device like a router or a switch. If the company uses a management system or inventory process to capture these addresses, then a report from one of these devices will show what is connected to the network even when they are not currently in the inventory. This information could then be used to track down rogue devices based on the physical port connected to a network device.

Q: Which of the following categories of controls are firewalls, intrusion detection systems, and a RADIUS server classified as?

A: Technical (NOT Administrative!) Controls

Technical controls are implemented as a system of hardware, software, or firmware. Administrative controls involve processes and procedures. Compensating controls are controls that are put in place to cover any gaps and reduce the risk remaining after using other controls.

Q: What is a major security risk that could occur when you comingle hosts/servers with different security requirements in a single network?

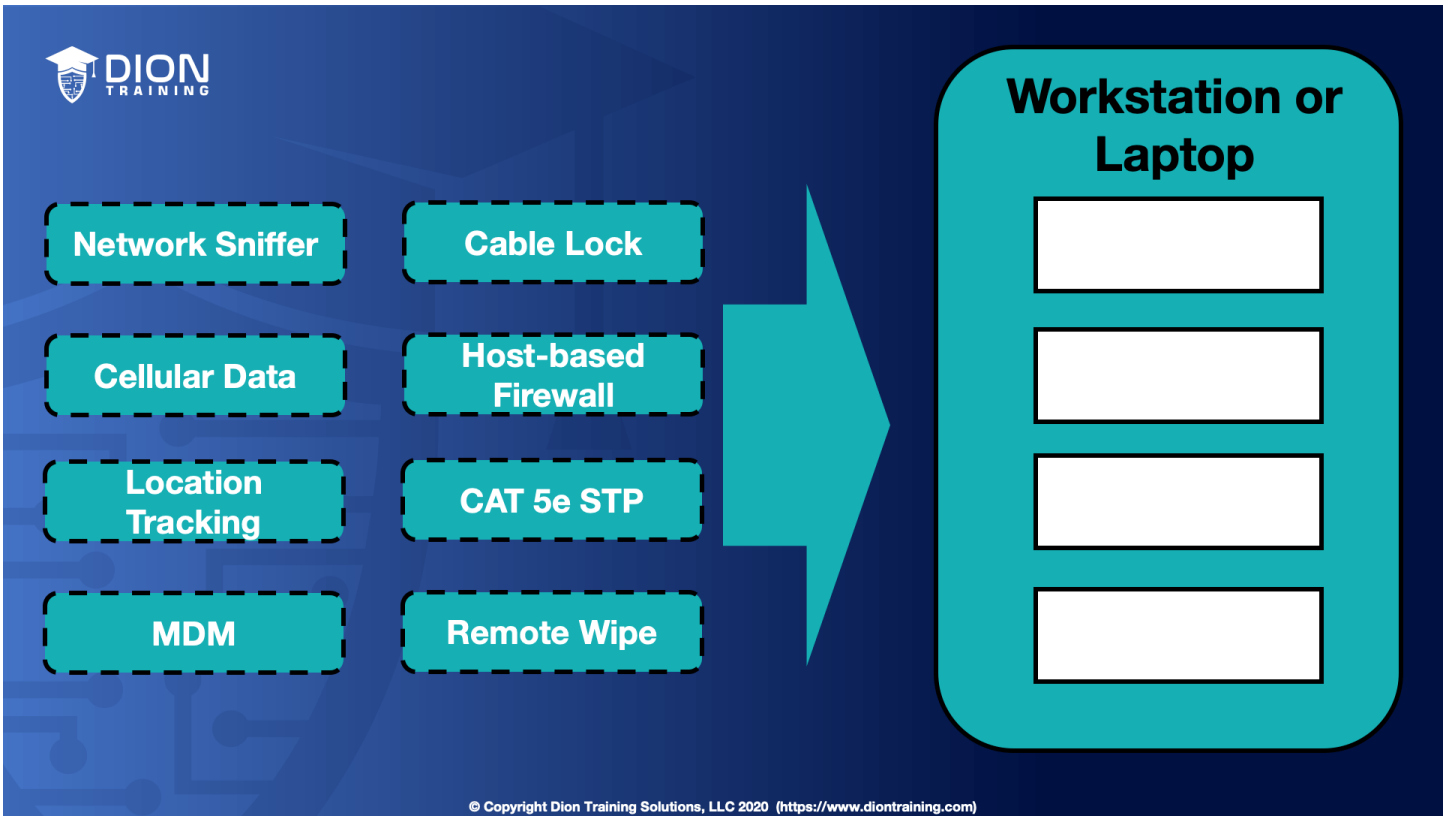
A: Security policy violations (NOT Privilege Creep!)

A network is only as strong as its weakest link (or host/server). When you comingle hosts/servers, there is a large risk that security policy violations could occur. This is because users may be used to following a less stringent security policy for one set of machines and carry over those procedures to a machine that should have had stronger security policies.

***Privilege creep** often occurs when an employee changes job responsibilities within an organization and is granted new privileges. While employees may need to retain their former privileges during a period of transition, those privileges are rarely revoked and result in an unnecessary accumulation of access privileges.*

Index

Q: Using the image provided, select four security features that you should use with a workstation or laptop within your organization?



A: Host-based firewall, Network sniffer, Cable lock, CAT5e STP

If you install a network sniffer, you will be able to capture any network traffic used on the network for later analysis.

If you use a CAT 5e STP cable for your network connection, you will minimize EMI risk and reduce data emanations.

Regardless, I think this answer is mostly incorrect as they chose CAT5e STP over remote wipe for laptops!

Index

Point-to-Point Tunnelling

Point-to-Point Protocol (PPP) is a data link layer (layer 2) communication protocol between two routers directly without any host or any other networking in between. It can provide loop connection authentication, transmission encryption, and data compression.

PPP is **used over many types of physical networks**, including serial cable, phone line, trunk line, cellular telephone, specialized radio links, ISDN, and fiber optic links such as SONET. Since IP packets cannot be transmitted over a modem line on their own without some data link protocol that can identify where the transmitted frame starts and where it ends, Internet service providers (ISPs) have used PPP for customer dial-up access to the Internet.

Two derivatives of PPP, Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over ATM (PPPoA), are used most commonly by ISPs **to establish a digital subscriber line (DSL)** Internet service LP connection with customers.

The Point-to-Point Tunneling Protocol (PPTP) is an **obsolete method for implementing VPNs**. PPTP has many well-known security issues. PPTP uses a TCP control channel and a Generic Routing Encapsulation (GRE) tunnel to encapsulate PPP packets. Many modern VPNs use various forms of UDP for this same functionality. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement any and all security functionalities.

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol **used to support VPNs** or as part of the delivery of services by ISPs. It uses **encryption ('hiding') only for its own control messages** (using an optional pre-shared secret), and does not provide any encryption or confidentiality of content by itself. Rather, it provides a tunnel for Layer 2 (which may be encrypted), and the tunnel itself may be passed over a Layer 3 encryption protocol such as IPsec.

L2TP has its origins primarily in two older tunneling protocols for point-to-point communication: Cisco's Layer 2 Forwarding Protocol (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). A new version of this protocol, L2TPv3 [RFC 3931 - 2005] provides additional security features, improved encapsulation, and the ability to carry data links other than simply Point-to-Point Protocol (PPP) over an IP network (for example: Frame Relay, Ethernet, ATM, etc.).

Index

A Virtual Private Network (VPN) is a mechanism for creating a secure connection between a computing device and a computer network, or between two networks, using an insecure communication medium such as the public Internet. A VPN can extend a private network (one that disallows or restricts public access), enabling users to send and receive data across public networks as if their devices were directly connected to the private network. The benefits of a VPN include security, reduced costs for dedicated communication lines, and greater flexibility for remote workers. VPNs are also used to bypass internet censorship. **Encryption is common, although not an inherent part of a VPN connection.**

A VPN is created by establishing a virtual point-to-point connection through the use of tunneling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic (as it does in the OpenVPN project and SoftEther VPN project) or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL**. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.**

OpenVPN uses the OpenSSL encryption library extensively, as well as the TLS protocol, and contains many security and control features. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls.

Q: Which protocol is used to establish a secure and encrypted VPN tunnel that can be initiated through a web browser?

A: SSL !

While IPsec is heavily used in VPNs, it's not used in browser-initiated ones! An SSL VPN is a type of virtual private network that uses the Secure Sockets Layer protocol in a standard web browser to provide secure, remote-access VPN capability. In modern browsers and servers, it is more common to use TLS (transport layer security) which is the successor to SSL.

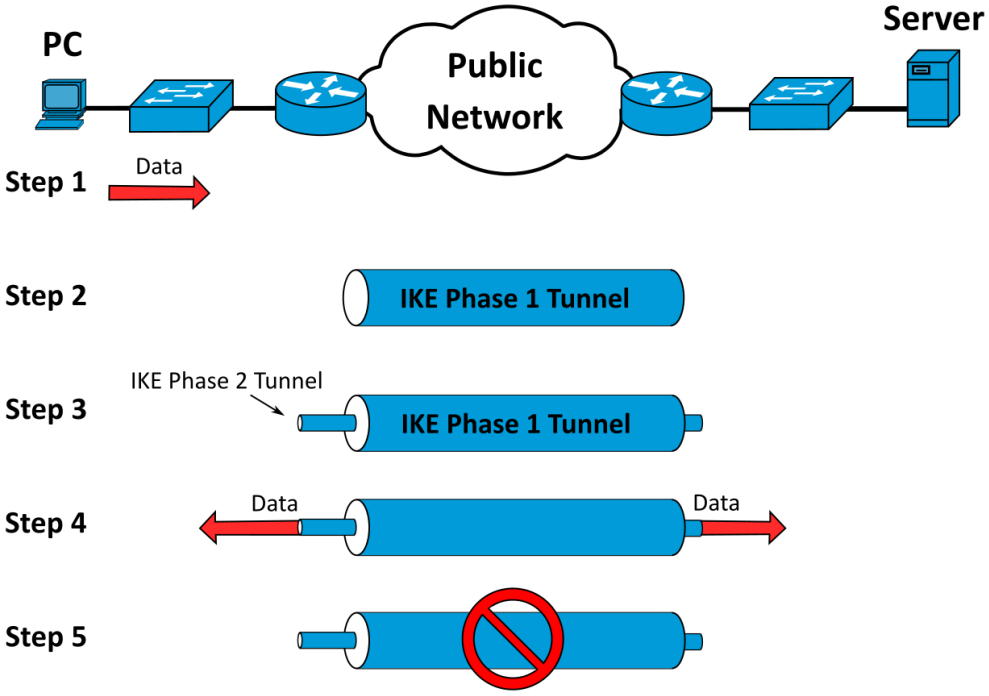
Note that the use of PPTP and SSL are discouraged for VPN security!

Index

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates & encrypts packets of data to provide secure, encrypted communication between two computers over an IP network. **It's used in VPNs.**

IPsec was initially **developed by the IETF for IPv6**, which was required in all standards-compliant implementations of IPv6 before RFC 6434 made it only a recommendation. This standards-based security protocol is also widely used with IPv4 and the Layer 2 Tunneling Protocol (L2TP). Its design meets most security goals: availability, integrity, and confidentiality. **IPsec uses encryption, encapsulating an IP packet inside an IPsec packet**. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.

Internet Key Exchange (IKE, sometimes IKEv1 or IKEv2, depending on version) is **the protocol used to set up a Security Association (SA) in the IPsec protocol suite.** IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication – either pre-shared or distributed using DNS (preferably with DNSSEC) – and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. In addition, a security policy for every peer which will connect must be manually maintained.



*IKE phase one's purpose is to **establish a secure authenticated communication channel by using the Diffie–Hellman** key exchange algorithm to generate a shared secret key to encrypt further IKE communications. This negotiation **results in one single bi-directional ISAKMP security association**. The authentication can be performed using either pre-shared key (shared secret), signatures, or public key encryption.] **Phase 1 operates in either Main Mode or Aggressive Mode**: Main Mode protects the identity of the peers and the hash of the shared key by encrypting them; Aggressive Mode does not.*

*During IKE phase two, **the IKE peers use the secure channel established in Phase 1 to negotiate Security Associations on behalf of other services like IPsec**. The negotiation results in a minimum of two unidirectional security associations (one inbound and one outbound). Phase 2 operates only in Quick Mode.*

Index

Internet Security Association and Key Management Protocol (ISAKMP) is used for negotiating, establishing, modifying & deleting Security Association (SAs), cryptographic keys & related parameters in IPSec protocol.

Most IPsec implementations consist of an IKE daemon that runs in user space and an IPsec stack in the kernel that processes the actual IP packets: User-space daemons have easy access to mass storage containing configuration information, such as the IPsec endpoint addresses, keys and certificates, as required. Kernel modules, on the other hand, can process packets efficiently and with minimum overhead—which is important for performance reasons.

The IKE protocol uses UDP packets, usually on port 500, and generally requires 4–6 packets with 2–3 round trips to create an ISAKMP security association (SA) on both sides. The negotiated key material is then given to the IPsec stack. For instance, this could be an AES key, information identifying the IP endpoints and ports that are to be protected, as well as what type of IPsec tunnel has been created. The IPsec stack, in turn, intercepts the relevant IP packets if and where appropriate and performs encryption/decryption as required. Implementations vary on how the interception of the packets is done—for example, some use virtual devices, others take a slice out of the firewall, etc.

WireGuard is a communication protocol and free and open-source software that implements encrypted VPNs, and was designed with the goals of ease of use, high speed performance, and low attack surface. **It aims for better performance and more power than IPsec and OpenVPN**, two common tunneling protocols. The WireGuard protocol **passes traffic over UDP**.

WireGuard uses the following:

- X25519 for key exchange
- ChaCha20 for symmetric encryption
- Poly1305 for message authentication codes
- SipHash for hashtable keys
- BLAKE2s for cryptographic hash function
- UDP-based only

Elaborating on them in-depth below (for the computer-science enthusiast only!):

→ **X25519 for key exchange:**

Curve25519 is an elliptic curve used in elliptic-curve cryptography (ECC) offering 128 bits of security (256-bit key size) and designed for use with the elliptic curve Diffie–Hellman (ECDH) key agreement scheme. It is one of the fastest curves in ECC, and is not covered by any known patents. The reference implementation is public domain software.

The original Curve25519 paper defined it as a Diffie–Hellman (DH) function. Daniel J. Bernstein has since proposed that the name Curve25519 be used for the underlying curve, and the name X25519 for the DH function.

Index

→ **ChaCha20 for symmetric encryption:**

*↳ Salsa20 and the closely related ChaCha are **stream ciphers** developed by Daniel J. Bernstein. Both ciphers are **built on a pseudorandom function** based on add-rotate-XOR (ARX) operations — 32-bit addition, bitwise addition (XOR) and rotation operations.*

*↳ A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, **each plaintext digit is encrypted one at a time** with the corresponding digit of the keystream, to give a digit of the ciphertext stream. Since encryption of each digit is dependent on the current state of the cipher, it is also known as state cipher. In practice, a digit is typically a bit, and the combining operation is an exclusive-or (XOR).*

*↳ In cryptography, a Pseudorandom Function Family (PRF) is a collection of efficiently-computable functions which **emulate a random oracle** in the following way: no efficient algorithm can distinguish (with significant advantage) between a function chosen randomly from the PRF family and a random oracle. Pseudorandom functions are vital tools in the construction of cryptographic primitives, especially secure encryption schemes.*

*↳ In cryptography, a random oracle is an **oracle** (a theoretical black box) that responds to every unique query with a (truly) random response chosen uniformly from its output domain. If a query is repeated, it responds the same way every time that query is submitted.*

*↳ In complexity theory and computability theory, an oracle machine is an abstract machine used to study decision problems. It can be visualized as a Turing machine with a **black box**, called an oracle, which is able to solve certain problems in a single operation. The problem can be of any complexity class. Even undecidable problems, such as the halting problem, can be used.*

↳ In science, computing, and engineering, a black box is a system which can be viewed in terms of its inputs and outputs (or transfer characteristics), without any knowledge of its internal workings. Its implementation is "opaque" (black). The term can be used to refer to many inner workings, such as those of a transistor, an engine, an algorithm, the human brain, or an institution or government.

→ **Poly1305 for message authentication codes:**

*↳ Poly1305 is a **universal hash family** designed by Daniel J. Bernstein for use in cryptography. As with any universal hash family, Poly1305 can be used as a **one-time message authentication code to authenticate a single message using a key shared** between sender and recipient, like a one-time pad can be used to conceal the content of a single message using a shared key.*

*↳ In mathematics and computing, universal hashing (in a randomized algorithm or data structure) refers to **selecting a hash function at random from a family of hash functions** with a certain mathematical property (see definition below). This guarantees a low number of collisions in expectation, even if the data is chosen by an adversary. Many universal families are known (for hashing integers, vectors, strings), and their evaluation is often very efficient. Universal hashing has numerous uses in computer science, for example in implementations of hash tables, randomized algorithms, and cryptography.*

Index

→ **SipHash for hashtable keys:**

↳ *SipHash is an add–rotate–XOR (ARX) based family of pseudorandom functions created by Jean-Philippe Aumasson and Daniel J. Bernstein in 2012, in response to a spate of* ***"hash flooding" denial-of-service attacks (HashDoS)*** *in late 2011. Although designed for use as a hash function to ensure security, SipHash is* ***fundamentally different*** *from cryptographic hash functions like SHA in that it is* ***only suitable as a message authentication code****: a keyed hash function like HMAC.*
That is, SHA is designed so that it is difficult for an attacker to find two messages X and Y such that SHA(X) = SHA(Y), even though anyone may compute SHA(X).
SipHash instead guarantees that, having seen Xi and SipHash(Xi, k), an attacker who does not know the key k cannot find any information about k or SipHash(Y, k) for any message Y ∉ {Xi} which they have not seen before.

> ↳ *Hash flooding (aka HashDoS) is a denial-of-service attack that uses hash collisions to exploit the worst-case (linear probe) runtime of hash table lookups. It was originally described in 2003. To execute such an attack, the attacker sends the server multiple pieces of data that hash to the same value and then tries to get the server to perform slow lookups. As the main focus of hash functions used in hash tables was* ***speed instead of security****, most major programming languages were affected, with new vulnerabilities of this class still showing up a decade after the original presentation.*
> *To prevent hash flooding without making the hash function overly complex,* ***newer keyed hash functions*** *are introduced, with the security objective* ***that collisions are hard to find as long as the key is unknown****. They may be slower than previous hashes, but are still much easier to compute than cryptographic hashes. As of 2021,* ***Daniel J. Bernstein's SipHash (2012) is the most widely-used*** *hash function in this class. (Non-keyed "simple" hashes remain safe to use as long as the application's hash table is not controllable from the outside.)*

→ **BLAKE2s for cryptographic hash function:**

↳ *BLAKE is a cryptographic hash function based on Daniel J. Bernstein's ChaCha stream cipher. Like SHA-2, there are two variants differing in the word size: one that uses 32-bit words, used for computing hashes up to 256 bits long, and one that uses 64-bit words, used for computing hashes up to 512 bits long.*
↳ *BLAKE2 is a cryptographic hash function based on BLAKE, created by Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, and Christian Winnerlein. The design goal was to replace the widely used, but broken, MD5 and SHA-1 algorithms in applications requiring high performance in software.*
↳ *BLAKE2b is faster than MD5, SHA-1, SHA-2, and SHA-3, on 64-bit, x86-64, and ARM architectures and is the successor of BLAKE-512. BLAKE2s is the successor of BLAKE-256.*

→ **UDP-based only:**

↳ *Self-explanatory!*

Index

→ Security Assertions Markup Language (SAML) is an XML-based framework for exchanging security-related information such as user authentication, entitlement, and attributes
→ SAML is often used in conjunction with SOAP
→ SAML is a solution for providing Single Sign-On (SSO) and federated identity management: It allows a Service Provider (SP) to establish a trust relationship with an Identity Provider (IdP) so that the SP can trust the identity of a **user (the principal)** without the user having to authenticate directly with the SP
→ The principal's **User Agent (typically a browser)** requests a resource from the Service Provider (SP)
→ The resource hosts can be referred to as the Service Provider or the Relying Party (RP). Both provide services to members of a federation.
→ If the user agent does not already have a valid session, the SP redirects the user agent to the Identity Provider (IdP)
→ The IdP requests the principal's credentials if not already signed in and, if correct, provides a SAML response containing one or more assertions
→ The SP verifies the signature(s) and (if accepted) establishes a session and provides access to the resource

Q: Which of the following does a User-Agent request a resource from when conducting a SAML transaction?

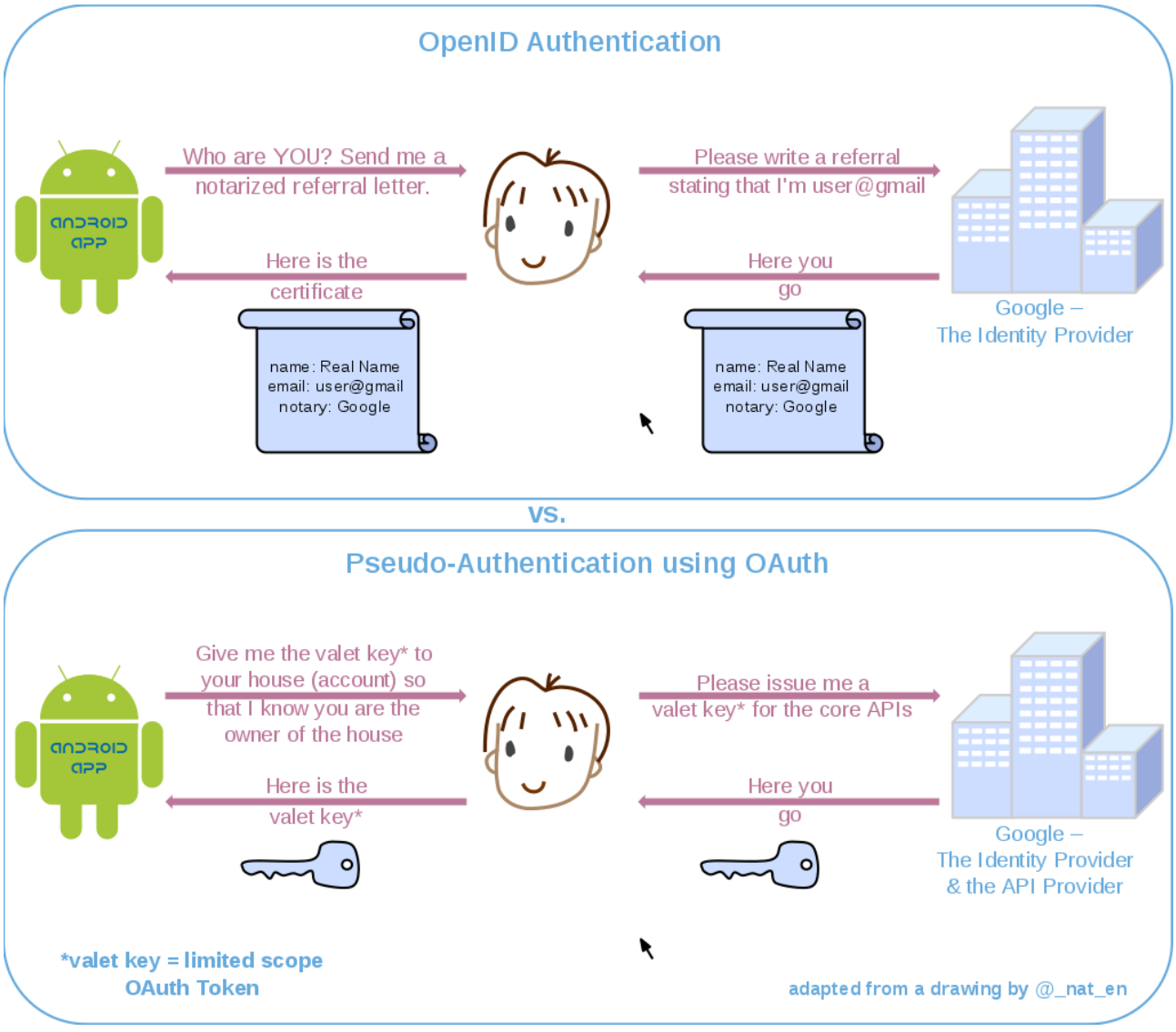
A: Service Provider (SP) [NOT an Identity Provider, IdP!]

Index

OAuth or "Open Authorization" is an open standard for access delegation, commonly **used as a way for internet users to grant websites or applications access to their information on other websites but without giving them the passwords.** This mechanism is used by companies such as LinkedIn, Amazon, Google, Facebook, Microsoft, and Twitter to permit the users to share information about their accounts with third-party applications or websites.

Generally, OAuth provides clients a "secure delegated access" to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without providing credentials. **Designed specifically to work with Hypertext Transfer Protocol (HTTP), OAuth essentially allows access tokens to be issued to third-party clients by an authorization server, with the approval of the resource owner.** The third party then uses the access token to access the protected resources hosted by the resource server.

OAuth began in November 2006 when Blaine Cook was developing the Twitter OpenID implementation. **OAuth is a service that is complementary to and distinct from OpenID:**



Index

The OAuth 1.0 protocol was published as RFC 5849, an informational Request for Comments, in April 2010. Since 31 August 2010, all third-party Twitter applications have been required to use OAuth.

The OAuth 2.0 framework was published considering additional use cases and extensibility requirements gathered from the wider IETF community. Albeit being built on the OAuth 1.0 deployment experience, **OAuth 2.0 is not backwards compatible with OAuth 1.0**. OAuth 2.0 was published as RFC 6749 and the Bearer Token Usage as RFC 6750, both standards track Requests for Comments, in October 2012.

OAuth 2 is explicitly designed to authorize claims and not to authenticate users. The implementation details for fields and attributes within tokens are not defined. Open ID Connect (OIDC) is an authentication protocol that can be implemented as special types of OAuth flows with precisely defined token fields.

The OAuth 2.1 Authorization Framework is in draft stage and consolidates the functionality in the RFCs of OAuth 2.0, OAuth 2.0 for Native Apps, Proof Key for Code Exchange, OAuth 2.0 for Browser-Based Apps, OAuth Security Best Current and Bearer Token Usage.

Q: Which protocol is paired with OAuth2 to provide authentication of users in a federated identity management solution?

A: OpenID Connect

Q: Which of the following technologies is NOT a shared authentication protocol?

A: LDAP

LDAP can be used for single sign-on but is not a shared authentication protocol. OpenID, OAuth, and Facebook Connect are all shared authentication protocols. Open ID Connect (OIDC) is an authentication protocol that can be implemented as special types of OAuth flows with precisely defined token fields. OAuth is designed to facilitate the sharing of information (resources) within a user profile between sites.

Index

802.1X & Network Access Control (NAC)

IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over wired IEEE 802 networks & over 802.11 wireless networks, which is known as "EAP over LAN" or EAPOL.

Extensible Authentication Protocol (EAP) is an authentication framework frequently used in network and internet connections. EAP is in wide use. For example, in IEEE 802.11 (Wi-Fi) the WPA and WPA2 standards have adopted IEEE 802.1X (with various EAP types) as the canonical (official) authentication mechanism.

802.1X authentication involves three parties: a supplicant (client device / software), an authenticator, and an authentication server:

1. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator.

2. The authenticator is a network device such as an Ethernet switch or wireless access point that provides a data link between the client and the network and can allow or block network traffic between them.

3. The authentication server supporting RADIUS & EAP protocols is a trusted server that can receive and respond to requests for network access, and can tell the authenticator if the connection is to be allowed, and various settings that should apply to that client's connection or setting. In some cases, the authentication server software may be running on the authenticator hardware.

Network Access Control (NAC) is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user / system authentication and network security enforcement. **A basic form of NAC is the 802.1X standard.**

Network access control is a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices when they initially attempt to access the network.

When a computer connects to a computer network, it is not permitted to access anything unless it complies with a business defined policy, including anti-virus protection level, system update level and configuration. NAC might integrate the automatic remediation process (fixing non-compliant nodes before allowing access) into the network systems, allowing the network infrastructure such as routers, switches, and firewalls to work together with back-office servers and end user computing equipment to ensure the information system is operating securely before interoperability is allowed.

Access to the network will be given according to the profile of the person and the results of a posture/health check. For example, in an enterprise the HR department could access only HR department files if both the role and the endpoint meet anti-virus minimums.

Index

Q: Dion Training allows its visiting business partners from CompTIA to use an available Ethernet port in their conference room to establish a VPN connection back to the CompTIA internal network. The CompTIA employees should obtain internet access from the Ethernet port in the conference room, but nowhere else in the building. Additionally, if any of the Dion Training employees use the same Ethernet port in the conference room, they should access Dion Training's secure internal network. Which of the following technologies would allow you to configure this port and support both requirements?

A: Implement NAC

In this scenario, implementing NAC can identify which machines are known and trusted Dion Training assets and provide them with access to the secure internal network. NAC could also determine unknown machines (assumed to be those of CompTIA employees) and provide them with direct internet access only by placing them on a guest network or VLAN. While MAC filtering could be used to allow or deny access to the network, it cannot by itself control which set of network resources could be utilized from a single ethernet port.

Q: Which of the following IEEE specifications describes the use of network authentication?

A: 802.1x

The IEEE 802.1x standard is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. This defines port security. The user's identity is determined based on their credentials or certificate, which is confirmed by the RADIUS server.

Q: Users connecting to an SSID appear to be unable to authenticate to the captive portal. Which of the following is the MOST likely cause of the issue?

A: RADIUS

Captive portals usually rely on 802.1x, and 802.1x uses RADIUS for authentication

Q: A company needs to implement stronger authentication by adding an authentication factor to its wireless system. The wireless system only supports WPA with pre-shared keys, but the backend authentication system supports EAP and TTLS. What should the network administrator implement?

A: 802.1x using EAP with MSCHAPv2

Since the backend uses a RADIUS server for back-end authentication, the network administrator can install 802.1x using EAP with MSCHAPv2 for authentication. The Extensible Authentication Protocol (EAP) is a framework in a series of protocols that allows for numerous different mechanisms of authentication, including things like simple passwords, digital certificates, and public key infrastructure. Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) is a password-based authentication protocol that is widely used as an authentication method in PPTP-based (Point to Point Tunneling Protocol) VPNs and can be used with EAP.

Index

Physical Location

Asset IDs should be used to uniquely identify each piece of hardware tracked in an asset management database. An asset management database can be configured to store as much or as little information as is deemed necessary. Typical data would be type, model, serial number, asset ID, location, user(s), value, and service information. Tangible assets can be identified using an identification number, barcode label, or Radio Frequency ID (RFID) tag attached to the device.

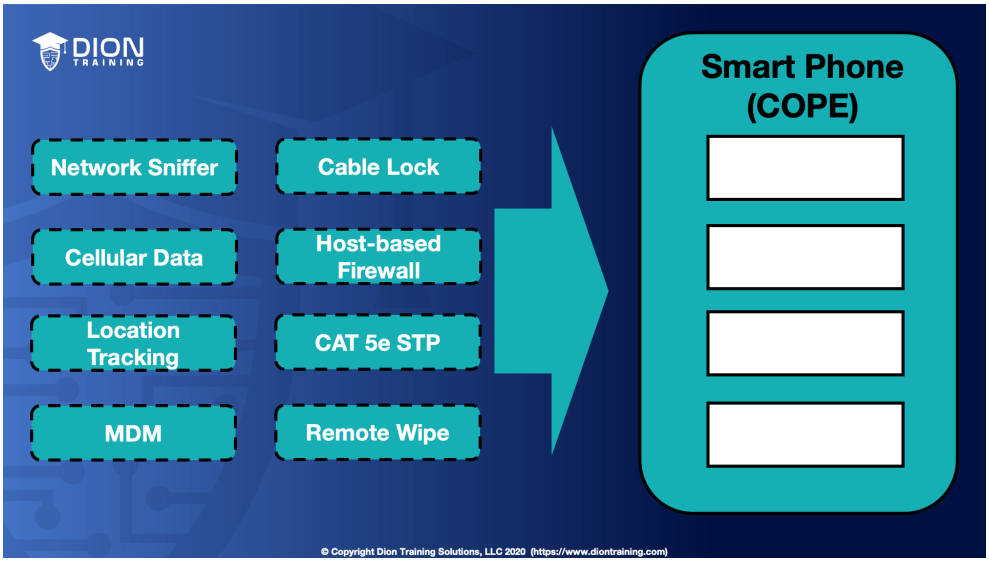
MAC Addresses can be used to identify every device on the local area network uniquely if an Asset ID is not available, but **would not be useful when trying to identify monitors** since they do not use a MAC address.

IP Addresses are a logical identifier, but are frequently changed when using a network with DHCP and cannot be used to reliably identify a piece of hardware.

Physical Location of a device is not a unique way of identifying an asset since many pieces of hardware may be located in the space location. Additionally, **virtual machines cannot easily be tracked using their physical location.**

RFID Tags are chips programmed with asset data: when in range of a scanner, the chip powers up and signals the scanner. The scanner alerts management software to update the device's location. As well as asset tracking, this allows the management software to track the device's location, making theft more difficult.

Q: Using the image provided, select four security features that you should use with a smartphone provided through a COPE policy in your organization?



A: Cellular data, Remote wipe, Location tracking, MDM

By using cellular data, your users will be able to avoid connecting to Wi-Fi networks for connectivity!

Index

Physical Identification & Access

A server lock is a physical locking mechanism installed on a server cabinet to prevent unauthorized from accessing the servers. The server lock could be a cipher lock, biometric lock, or a simple keyed lock depending on the level of security needed.

USB lock prevents unauthorized data transfer through USB ports, reducing the risk of data leakage, data theft, computer viruses, and malware by physically locking and blocking the USB Ports.

A smart card, chip card, PIV (Personal Identity Verification) card, or integrated circuit card is a physical, electronic authorization device used to control access to a resource. It is typically a plastic credit card-sized card with an embedded integrated circuit chip. In high-security environments, employee badges may contain a smart card embedded chip that must be inserted into a smart card reader to log in or access information on the system. **Often, smart cards are used as part of a multifactor authentication system in which the smart card and a PIN need to be entered for system authentication to occur**.

Smart/PIV cards often contain a digital certificate embedded within them that's presented to the system when inserted into the smart card reader. When combined with a PIN, the smart card can be used as a multi-factor authentication mechanism. The PIN unlocks the card and allows the digital certificate to be presented to the system.

A proximity card is a contactless card that usually utilizes RFID to communicate with the reader on a physical access system. These are commonly used to access secured rooms (such as server rooms) or even a building itself (such as at an access control vestibule). Some smart cards contain proximity cards within them.

An entry control roster is an administrative control used to log each person entering/leaving a secure room.

A mantrap, security mantrap portal, airlock, sally port or access control vestibule is a physical security access control system comprising a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens.

The Kensington Lock is a small hole found on almost every portable computer or laptop made after 2000. It allows a cable lock to be attached to a portable computer or laptop to lock it to a desk and prevent theft. These locks often use a combination lock or **padlock** type of locking system. These locks do not affect the user's ability to use the laptop or device. It only prevents them from moving the laptop from the area.

A Key Fob generates a random number code synchronized to a server. The code changes every 60 seconds or so. This is an example of an OTP. A SecureID token is an example of a key fob that is produced by RSA.

Biometrics are any biological identifying features stored as digital data that can be used to authenticate a user. Typical features used include facial pattern, iris, retina, or fingerprint pattern, and signature recognition. This requires a relevant scanning device, such as a fingerprint reader, and a database of biometric information for authentication to occur.

The Crossover Error Rate (CER) describes the point where the False Reject Rate (FRR) and False Accept Rate (FAR) are equal. CER is also known as the Equal Error Rate (EER). The Crossover Error Rate describes the overall accuracy of a biometric system.

Index

Q: Which type of authentication method is commonly used with physical access control systems and relies upon RFID devices embedded into a token?

A: Proximity Cards

Q: You want to ensure that only one person can enter or leave the server room at a time. Which of the following physical security devices would BEST help you meet this requirement?

A: Access Control Vestibule

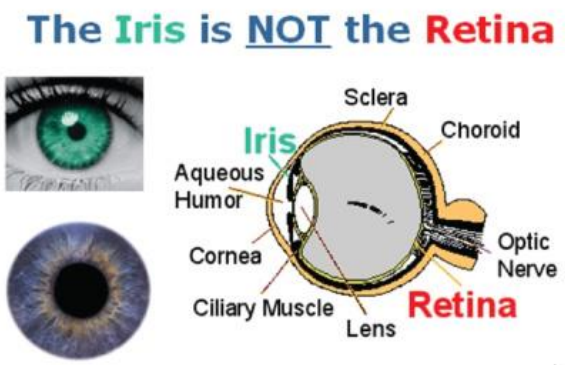
Video monitoring is a passive security feature, so it won't prevent two people from entering at once. The thumbprint reader or cipher lock will ensure that only an authorized user can open the door, but it won't prevent someone from piggybacking and entering with them.

Q: You are working for a government contractor who requires all users to use a PIV device when sending digitally signed and encrypted emails. Which of the following physical security measures is being implemented?

A: Smart Card (See PIV? Think "smart card" for the exam!)

Q: Which of the following biometric authentication factors uses an infrared light shone into the eye to identify the pattern of blood vessels?

A: Retinal Scan (NOT Iris Scan!)

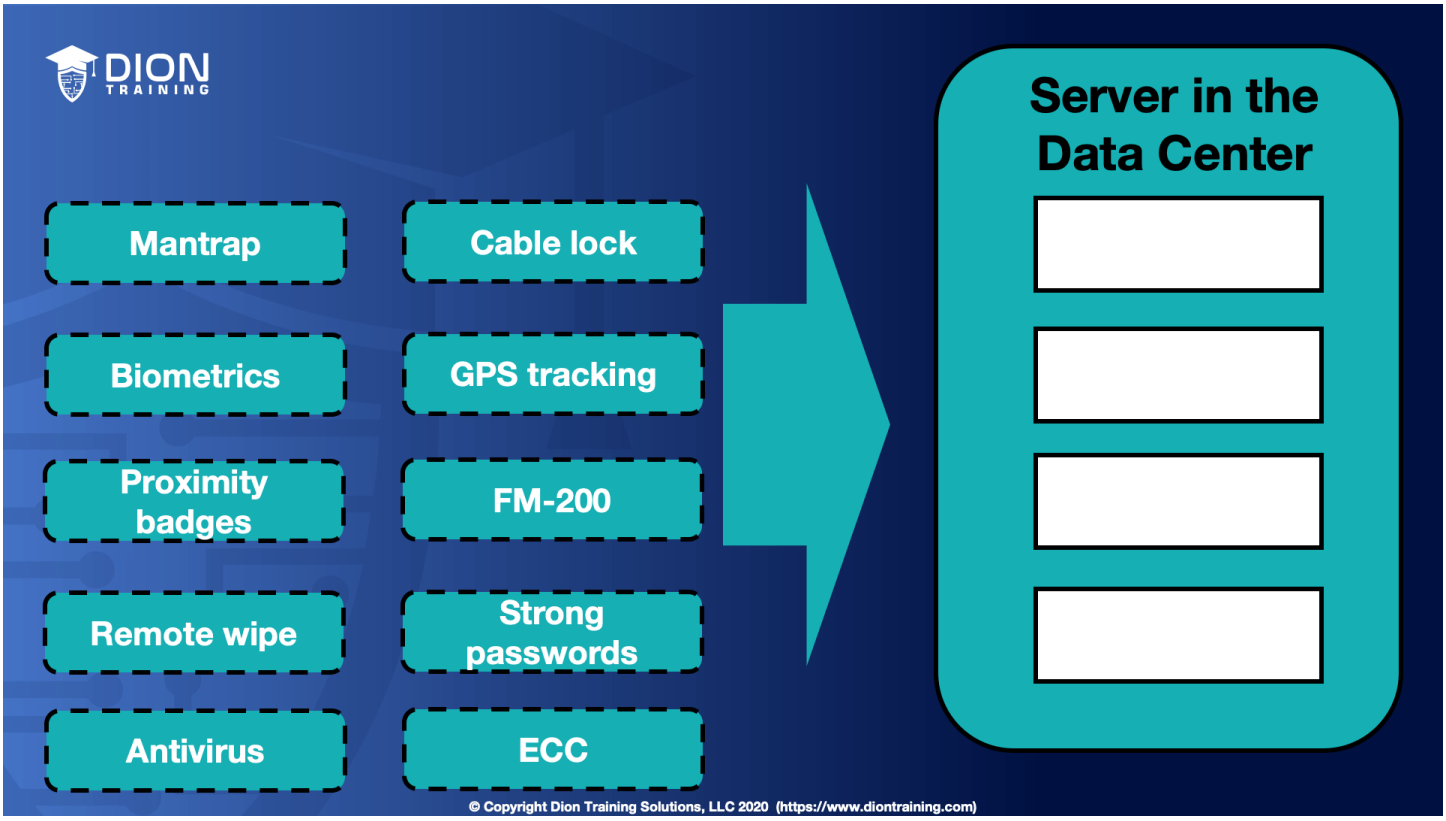


Q: Dion Training is concerned with the possibility of employees accessing another user's workstation in secured areas without their permission. Which of the following would BEST be able to prevent this from happening?

A: Require biometric identification for user logins (NOT security cameras! How will you see the screen?!)

Index

Q: (Sample Simulation – On the real exam for this type of question, you would have to fill in the blanks by dragging and dropping them into place.)



Using the image provided, select four security features that you should use to best protect your servers in the data center. This can include physical, logical, or administrative protections.

A: FM-200, Biometric locks, Mantrap & Antivirus

FM-200 is a fire extinguishing system commonly used in data centers and server rooms to protect the servers from fire. Biometric locks are often used in high-security areas as a lock on the access door. Additionally, biometric authentication could be used for a server by using a USB fingerprint reader. Mantraps often are used as part of securing a data center as well. This area creates a boundary between a lower security area (such as the offices) and the higher security area (the server room). Antivirus should be installed on servers since they can use signature-based scans to ensure files are safe before being executed.

Index

A 'Kill Chain' is originally a military term and concept, and identifies the structure of an attack. To do so, it consists of:

1. Identification of the target
2. Dispatching of forces to the target
3. Initiation of attack on the target
4. Destruction of target

Queue eagle screeching in the distance

Conversely, breaking an opponent's kill chain is a defensive measure undertaken as a pre-emptive action.

The "cyber kill chain" is a sequence of stages required for an attacker to successfully infiltrate a network and exfiltrate data from it. Each stage demonstrates a specific goal along the attacker's path. Designing your monitoring and response plan around the cyber kill chain model is an effective method because it focuses on how actual attacks happen.

Lockheed-Martin Cyber Kill Chain

"The Lockheed Martin cyber kill chain provides a general life cycle description of how attacks occur but does not deal with the specifics of how to mitigate them."

Lockheed Martin recently adapted the above kill-chain concept to information security, using it as a method for modeling intrusions on a computer network. The cyber kill chain model has seen some adoption in the information security community. However, acceptance is not universal, with critics pointing to what they believe are fundamental flaws in the model.

Computer scientists at Lockheed-Martin corporation described a new "intrusion kill chain" framework / model to defend computer networks in 2011. **They wrote that attacks may occur in phases and can be disrupted through controls established at each phase.** Since then, the "cyber kill chain" has been adopted by data security organizations to define phases of cyberattacks, from early reconnaissance to the goal of data exfiltration. The kill chain can also be used as a management tool to help continuously improve network defense.

The Lockheed Martin cyber kill chain implicitly assumes a unidirectional workflow. Therefore, it fails to consider that an adversary may retreat during an attack.

According to Lockheed Martin, threats must progress through several phases in the model while defensive courses of action can be taken at each phase:

Index

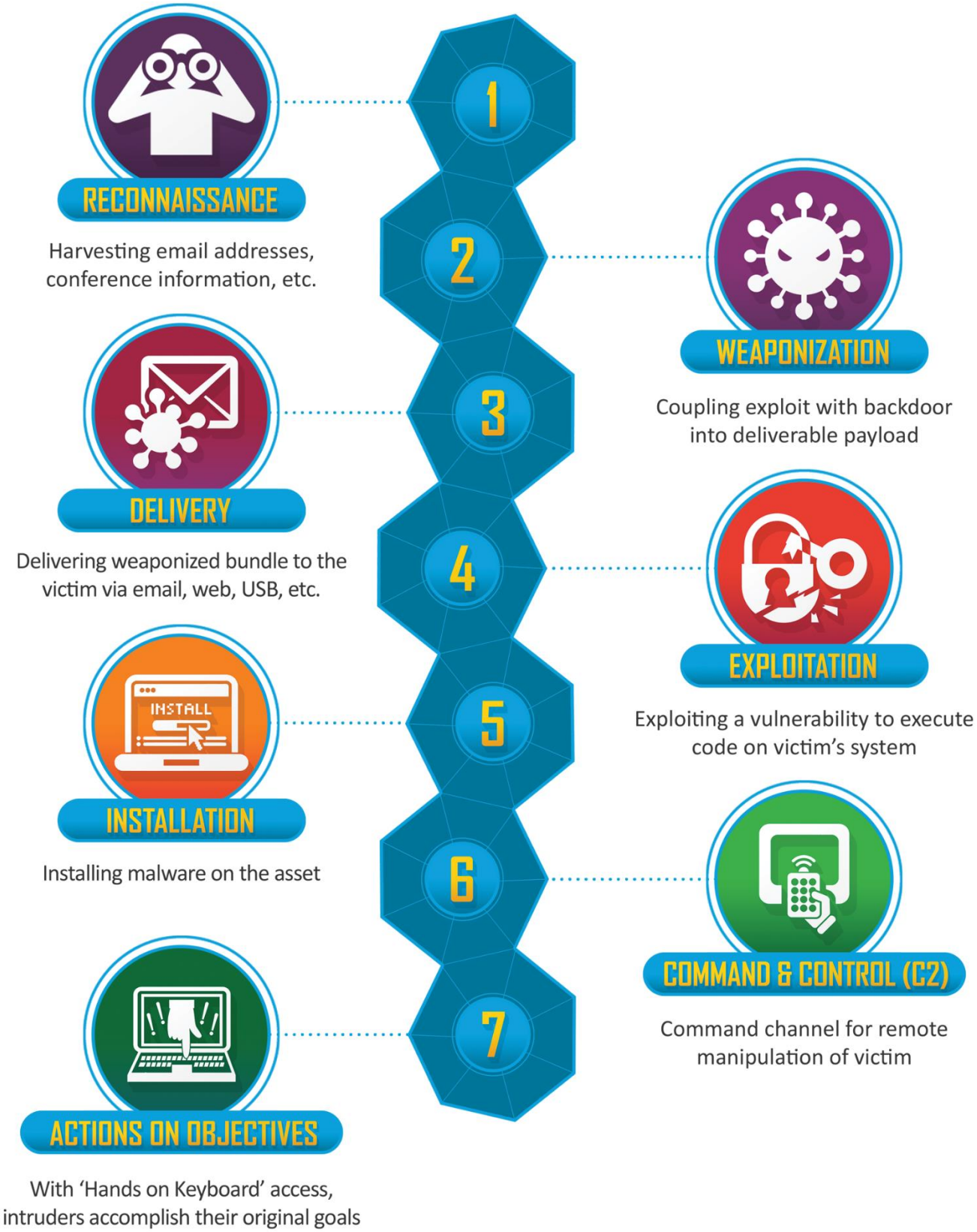
No.	Kill Chain Phase	Defensive Countermeasures
1.	Reconnaissance: Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network.	Detect: Determine whether an intruder is present.
2.	Weaponization: Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities. Packaged into a deliverable payload, such as a PDF of MS Office file	Deny: Prevent information disclosure and unauthorized access.
3.	Delivery: Intruder transmits weapon to target (e.g., via e-mail attachments, websites, or USB drives)	Disrupt: Stop or change outbound traffic (to attacker).
4.	Exploitation: Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.	Degrade: Counter-attack command and control.
5.	Installation: Malware weapon installs access point (e.g., "backdoor") usable by intruder.	Deceive: Interfere with command and control.
6.	Command and Control: Malware enables intruder to have "hands on the keyboard" persistent access to target network.	Contain: Network segmentation changes
7.	Actions on Objective: Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.	Too late, grab some cheap liquor and pray

Critiques

Among the critiques of Lockheed Martin's cyber kill chain model as a threat assessment and prevention tool is that the first phases happen outside the defended network, making it difficult to identify or defend against actions in these phases!

Similarly, this methodology is said to reinforce traditional perimeter-based & malware-prevention based defensive strategies. Others have noted that the traditional cyber kill chain isn't suitable to model the insider threat. This is particularly troublesome given the likelihood of successful attacks that breach the internal network perimeter, which is why organizations "need to develop a strategy for dealing with attackers inside the firewall. They need to think of every attacker as [a] potential insider".

Index

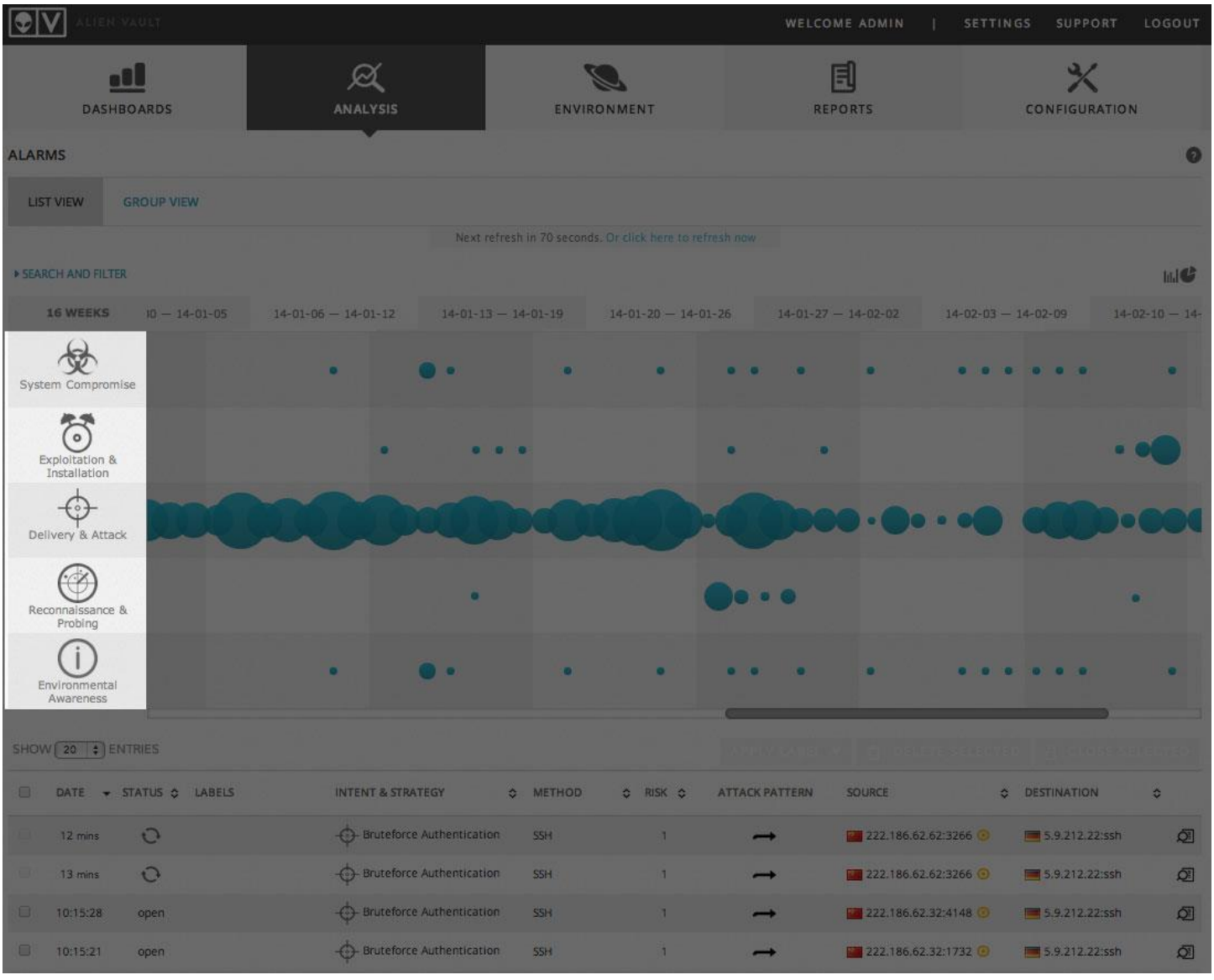

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Index

AT&T AlienVault Cyber Kill Chain

With unrivaled visibility of the AT&T IP backbone, global USM (Unified Security Management) sensor network, and the Open Threat Exchange (OTX), AT&T Alien Labs delivers continuous, tactical threat intelligence to the USM platform to keep your defense up to date.

AlienVault was specifically designed to avoid the rigidity of the Lockheed Martin cyber kill chain.



The cyber kill chain in AlienVault

The alarm prioritization taxonomy in AlienVault USM and OSSIM (Open Source Security Information Management) is a simplified version of the Lockheed Martin "Cyber Kill Chain" methodology. To help you quickly prioritize alarms, each alarm category in AlienVault provides the intent of the threat. The intent can be surmised based on attack activity and how they're interacting with your network and its assets. AlienVault Labs applies their extensive research into attacker profiles, tools and techniques to evaluate each threat to determine the appropriate category for each alarm.

Index

Alarm Type (Intent)	Description	Examples
Reconnaissance & Probing 	Behavior indicating an actor attempting to discover information about the organization	• Port Scans • Social Engineering
Delivery & Attack 	Behavior indicating an attempted delivery of an exploit	Network-based & analysis-based detection of known attacks and payloads
Exploitation & Installation 	Behavior indicating a successful exploit of a vulnerability or backdoor/RAT being installed on a system	• RAT installation • Bot installation
System Compromise 	Behavior indicating a compromised system	• Data exfiltration attempts • Outbound traffic to CnC host
Informational: Environmental Awareness 	Observed behavior and status about the environment being monitored	• Information about running services • User activity & behavior • System configuration

AlienVault has 1700+ event correlation rules in our threat intelligence subscription – each alarm is triggered by an event correlation rule. In terms of security exposure, the most critical events will be in the System Compromise category. Once a system has been compromised, an attacker has gained a foothold into your network. This may be a contained incident to one system, however, in most cases this is just the tip of the iceberg.

So when viewing all of your alarms, you may want to begin with those that are the most critical, and typically, this would be signaled by the System Compromised intent.

In general, keep these tips in mind:

- For each incident, ask yourself these questions: "*How close to a successful breach is this*?" and "*How close are the attackers to their goal*?"
- Move away from "a first-in-first-out" pipe model. Look at each event in the context of other events as well as the context of what an attacker's goal or intent might be.
- Use the context of your environment and business model to surmise what the intent of the attacker is, and use the reporting source of the event to further refine prioritization efforts. Establish the reliability of the data source based on the full context of what it is reporting.

Index

MITRE ATT&CK Framework

"The MITRE ATT&CK framework provides explicit pseudo-code examples for detecting or mitigating a given threat within a network and ties specific behaviors back to individual actors."

The **Adversarial Tactics, Techniques, and Common Knowledge or MITRE ATT&CK** is a guideline for classifying and describing cyberattacks and intrusions. It was created by the Mitre Corporation and released in 2013.

The framework consists of 14 tactics categories consisting of "technical objectives" of an adversary. Examples include privilege escalation and command and control. These categories are then broken down further into specific techniques and sub-techniques

The framework is an alternative to the Cyber Kill Chain developed by Lockheed Martin.

The Mitre Corporation (stylized as The MITRE Corporation and MITRE) is an American not-for-profit organization with dual headquarters in Bedford, Massachusetts, and McLean, Virginia. It manages federally funded research and development centers (FFRDCs) supporting various U.S. government agencies in the aviation, defense, healthcare, homeland security, and cybersecurity fields, among others

The latest (v12) and past revisions to the MITRE ATT&CK Matrix for Enterprise can be found at this link

Q: Which analysis framework provides the most explicit detail regarding how to mitigate or detect a given threat?

A: MITRE ATT&CK Framework

Index

Diamond Model of Intrusion Analysis

"The Diamond Model provides an excellent methodology for communicating cyber events and allowing analysts to derive mitigation strategies implicitly. The Diamond Model is constructed around a graphical representation of an attacker's behavior."

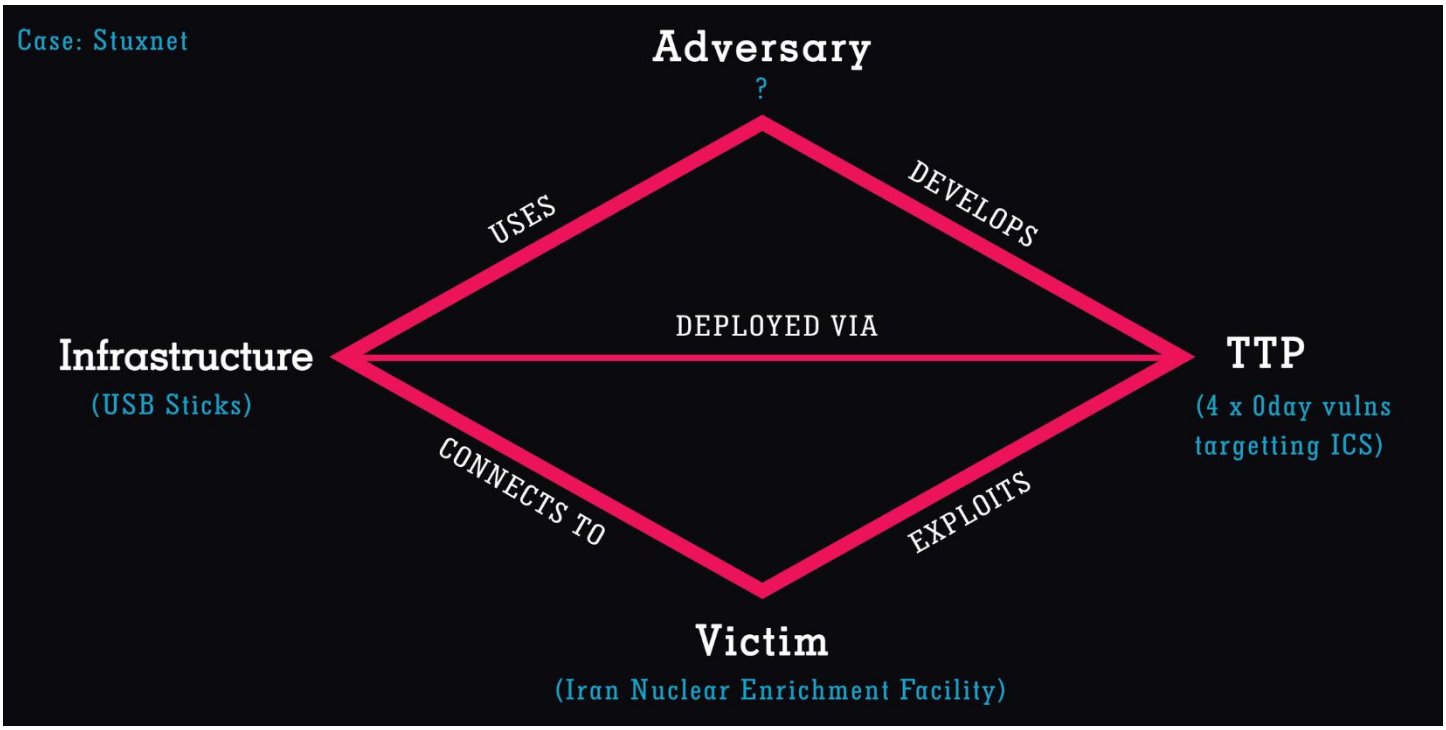
The Diamond Model of Intrusion Analysis is a model to describe cyber-attacks. It contains 4 parts - adversary, infrastructure, capability, and target. It gives analysts a comprehensive view of cyber-attacks.

Adversary: Where are attackers from? Who are the attackers? Who is the sponsor? Why attack? What is the activity timeline and planning?

Infrastructure: Infected computer(s), C2 domain names, location of C2 servers, C2 server types, mechanism, and structure of C2, data management & control, and data leakage paths

Capability / Techniques, Tactics & Procedures (TTP): What skills do the attackers have to do reconnaissance, deliver their attacks, attack exploits and vulnerabilities, deploy their remote-controlled malwares and backdoors, and develop their tools?

Target: Who is their target country/region, industry sector, individual, or data?



Index

Open Indicators of Compromise (OpenIOC) Framework

"OpenIOC contains a depth of research on APTs but does not integrate the detection and mitigation strategy."

OpenIOC is an open framework, meant for sharing threat intelligence information in a machine-readable format. It was developed by the American cybersecurity firm MANDIANT in November 2011. It is written in eXtensible Markup Language (XML) and can be easily customized for additional intelligence so that incident responders can translate their knowledge into a standard format. Organizations can leverage this format to share threat-related latest Indicators of Compromise (IoCs) with other organizations, enabling real-time protection against the latest threats.

What is the schema of OpenIOC?

The base schema of OpenIOC is a simple framework that is written in XML, which can be used to document and classify forensic artifacts of an intrusion occurring across any network or host. The framework comes with a 500 pre-defined base set of indicators, as provided by MANDIANT. These pre-defined sets of environments can be used to track down advanced threats. The base schema can be extended further to include additional indicators from multiple sources. The users of OpenIOC are free to create and add their own sets of indicators and extend it as they see fit.

Why should organizations use OpenIOC?

Conventional methods of detecting security breaches are no longer adequate, as simple signatures have become very easy for an intruder to overcome. Various organizations across the same or even different sectors need to be able to communicate on how to spot intruders in their hosts and networks using a machine digestible format that can get rid of a human delay from intelligence sharing. OpenIOC provides a common platform to enable this communication.

Why are the benefits of OpenIOC?

By using the OpenIOC framework, the organizations will have access to the latest IOCs shared by other organizations. These IOCs can be readily leveraged by multiple threat detection tools, enabling real-time threat detection capabilities. With this, organizations can benefit from the collaborative effect of shared threat intelligence within their industry.

Index

Cryptography - Hashing Algorithms – MD5, SHA, etcetera.

Cryptography, or cryptology (from Ancient Greek: κρυπτός, romanized: kryptós "hidden, secret") is the practice and study of techniques for secure communication in the presence of adversarial behavior.

In this regard, cryptographic hashing algorithms aid communicating parties by allowing them to determine that the contents of their messages and files are unaltered in transit, or not corrupted from the source. By themselves, they do not hide the contents nor secure the communications though!

MD-5 creates a 128-bit fixed output. The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value, and replaces the earlier MD4. MD5 can be used as a checksum to verify data integrity against unintentional corruption. Historically it was widely used as a cryptographic hash function; **however it has been found to suffer from extensive vulnerabilities**. It remains suitable for other non-cryptographic purposes, such as for determining the partition for a particular key in a partitioned database, and may be preferred due to lower computational requirements than more recent Secure Hash Algorithms.

The **Secure Hash Algorithms (SHA)** are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS), including:

- SHA-0: A retronym applied to the original version of the 160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to **an undisclosed "significant flaw"** and replaced by the slightly revised version SHA-1.
- SHA-1: A 160-bit hash function (creates a 160-bit fixed output) which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. **Cryptographic weaknesses were discovered in SHA-1, and the standard was no longer approved for most cryptographic uses after 2010.**
- SHA-2: A family of two similar hash functions, with different block sizes, known as SHA-256 (creates a 256-bit fixed output) and SHA-512. They differ in the word size; SHA-256 uses 32-bit words where SHA-512 uses 64-bit words. There are also **truncated versions** of each standard, known as SHA-224, SHA-384, SHA-512/224 and SHA-512/256. These were also designed by the NSA.
- SHA-3: A hash function formerly called Keccak, chosen in 2012 after a public competition among non-NSA designers. It supports the same hash lengths as SHA-2, and its internal structure **differs significantly from the rest of the SHA family**.

The corresponding standards are FIPS PUB 180 (original SHA), FIPS PUB 180-1 (SHA-1), FIPS PUB 180-2 (SHA-1, SHA-256, SHA-384, and SHA-512). NIST has updated Draft FIPS Publication 202, SHA-3 Standard separate from the Secure Hash Standard (SHS).

Index

RIPEMD (RIPE Message Digest) is a family of cryptographic hash functions developed in 1992 (the original RIPEMD) and 1996 (other variants). There are five functions in the family: RIPEMD, RIPEMD-128, RIPEMD-160, RIPEMD-256, and RIPEMD-320, of which RIPEMD-160 (creates a 160-bit fixed output) is the most common.

The original RIPEMD, as well as RIPEMD-128, is not considered secure because 128-bit result is too small and also (for the original RIPEMD) because of design weaknesses. The 256- and 320-bit versions of RIPEMD provide the same level of security as RIPEMD-128 and RIPEMD-160, respectively**; they are designed for applications where the security level is sufficient but longer hash result is necessary.**

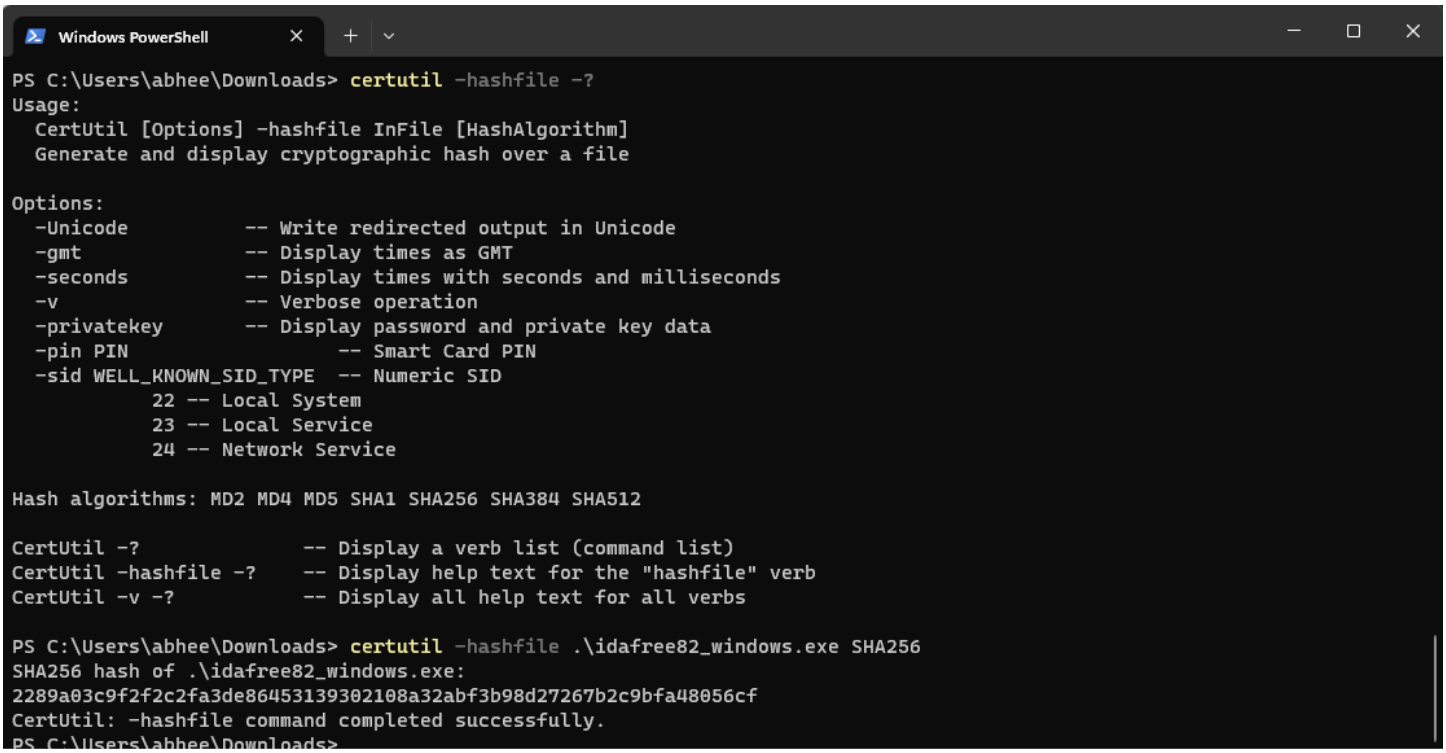
While RIPEMD functions are less popular than SHA-1 and SHA-2, **they are used, among others, in Bitcoin and other cryptocurrencies** based on Bitcoin.

NTLM creates a 128-bit fixed output.

Compute File Hashes in Windows

Certutil.exe is a command-line program, installed as part of Certificate Services. You can use certutil.exe to dump and display certification authority (CA) configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains.

Additionally, it may be used to generate file hashes via the *certutil* ***-hashfile <filename> <hash_algorithm>****:*



Index

Q: Dion Training has just suffered a website defacement of its public-facing webserver. The CEO believes the company's biggest competitor may have done this act of vandalism. The decision has been made to contact law enforcement so that evidence can be collected properly for use in a potential court case. Laura is a digital forensics investigator assigned to collect the evidence. She creates a bit-by-bit disk image of the web server's hard drive as part of her evidence collection. What technology should Laura use after creating the disk image to verify the copy's data integrity matches that of the original web server's hard disk?

A: SHA-256

SHA-256 is the Secure Hash Algorithm with a 256-bit length output. This is one of the most common hash algorithms in use and is employed in many applications and protocols.

SHA-256 and other hashing algorithms are used to ensure the data integrity of a file has not been altered. RSA, 3DES, and AES are all encryption algorithms which can ensure confidentiality but not integrity.

Index

Cryptography: Encryption Algorithms – Symmetric & PKI Systems

In cryptography, encryption is the process of encoding information, i.e. converting the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is possible to decrypt the message without possessing the key but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message, though.

Modern encryption schemes use the concepts of public-key and symmetric-key. Modern encryption techniques ensure security because modern computers are inefficient at cracking the encryption.

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both the encryption of plaintext and the decryption of ciphertext. **The keys may be identical, or there may be a simple transformation to go between the two keys.** The keys, in practice, represent a **shared secret** between two or more parties that can be used to maintain a private information link. The requirement that both parties have access to the secret key is one of the main drawbacks of symmetric-key encryption. However, symmetric-key encryption algorithms are **usually better for bulk encryption**. With the exception of the one-time pad they have a smaller key size, which means less storage space and faster transmission. **Due to this, asymmetric-key encryption is often used to exchange the secret key for symmetric-key encryption.**

AES, DES, RC4, Twofish and Blowfish are all symmetric algorithms.

Public-key cryptography or asymmetric cryptography is the system of using **pairs of related keys**, typically a public key and a private key. Security of public-key cryptography depends on keeping the private key secret; the public key can be openly distributed without compromising security.

Two of the best-known uses of public key cryptography are:

- ***Public key encryption***: A sender obtains the intended receiver's public key and uses it to encrypt a message. On receiving this message, the receiver decrypts it with their private key. Thus, PKI encryption is asymmetric in nature: different keys are used for the encryption and decryption of the plaintext!
- ***Digital signatures*****,** in which a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key. This verification proves that the sender had access to the private key, and therefore is very likely to be the person associated with the public key. It also proves that the signature was prepared for that exact message, since verification will fail for any other message one could devise without using the private key.

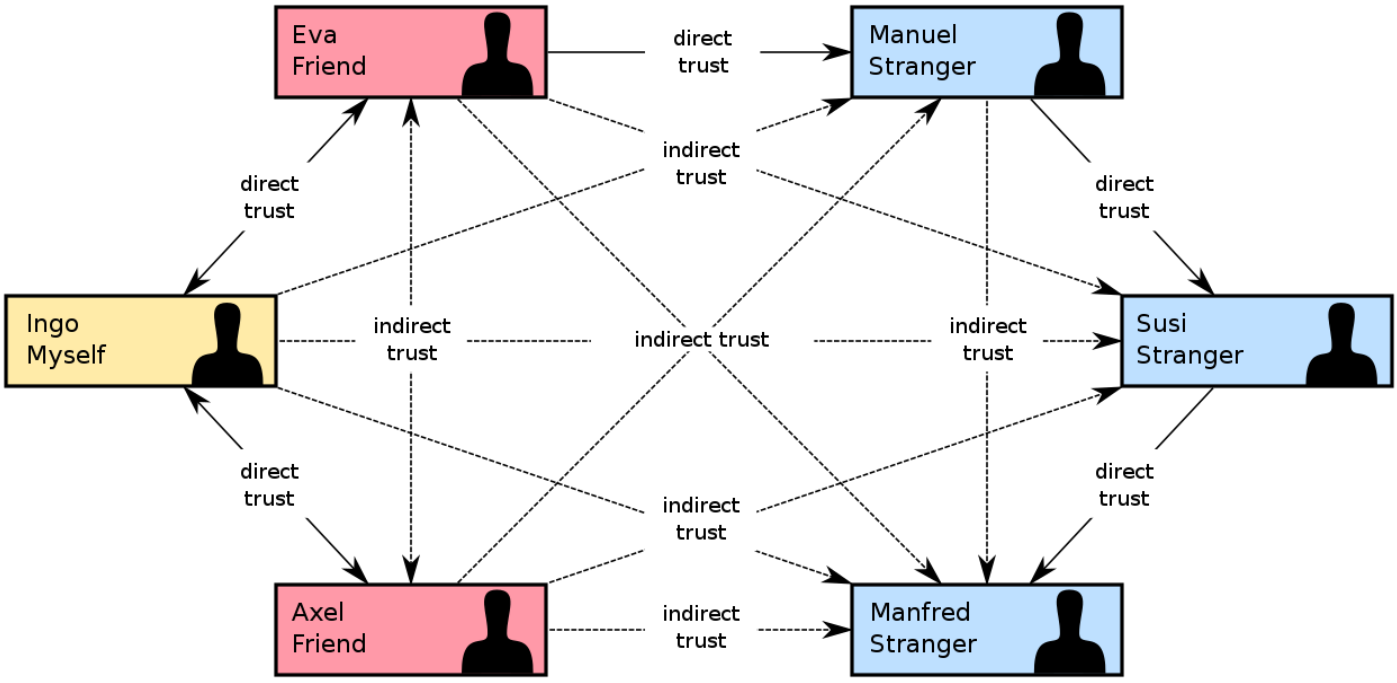
ECC, PGP, GPG, Diffie-Hellman, DSA, and RSA are all asymmetric algorithms.

Index

One important issue is confidence/proof that a particular public key is authentic, i.e. that it is correct and belongs to the person or entity claimed, and has not been tampered with or replaced by some (perhaps malicious) third party. There are several possible approaches, including:

A Public Key Infrastructure (PKI), in which one or more third parties – known as certificate authorities – certify ownership of key pairs. TLS relies upon this. This implies that the PKI system (software, hardware, and management) is trust-able by all involved.

A "Web of Trust" which decentralizes authentication by using individual endorsements of links between a user and the public key belonging to that user. **Pretty Good Privacy (PGP) uses this approach, as does domain name system (DNS) lookups. The DKIM system for digitally signing emails also uses this approach.**



The Web of Trust's decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such). As with computer networks, there are many independent webs of trust, and any user (through their public key certificate) can be a part of, and a link between, multiple webs.

The web of trust concept was first put forth by PGP creator Phil Zimmermann in 1992 in the manual for PGP version 2.0:

"As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys."

Note the use of the word **emergence** in this context. The web of trust makes use of the concept of emergence.

Index

Q: Which of the following cryptographic algorithms is classified as asymmetric?

A: Diffie-Hellman

Diffie-Hellman (DH) is used to exchange cryptographic keys over a public channel securely and was one of the first public-key protocols. As a public-key protocol, it relies on an asymmetric algorithm. AES, DES, RC4, Twofish and Blowfish are all symmetric algorithms.

Advanced Encryption Standard (AES) is a symmetric-key algorithm for encrypting digital data. It was established as an electronic data encryption standard by NIST in 2001. AES can use a 128-bit, 192-bit, or 256-bit key, and uses a 128-bit block size.

DES and AES both rely on a single shared secret key, making it vulnerable to attack. DES has already been broken, while AES remains unbroken (today).

Q: Which of the following cryptographic algorithms is classified as symmetric?

A: Blowfish

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products. ECC, PGP, Diffie-Hellman, DSA, and RSA are all asymmetric algorithms.

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. The algorithm uses a key pair consisting of a public key and a private key.

RSA (Rivest–Shamir–Adleman) was one of the first public-key cryptosystems and is widely used for secure data transmission. As a public-key cryptosystem, it relies on an asymmetric algorithm. RSA is vulnerable to attack with enough time and computing power.

Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. As a public-key cryptosystem, it relies on an asymmetric algorithm.

Q: Frank and John have started a secret club together. They want to ensure that when they send messages to each other, they are truly unbreakable. What encryption key would provide the STRONGEST and MOST secure encryption?

A: Randomized one-time use pad

NOT AES/ECC with 256-bit keys or DES with a 56-bit key.

The only truly unbreakable encryption is one that uses a one-time use pad. This ensures that every message is encrypted with a different shared key that only the two owners of the one-time use pad would know. This technique ensures that there is no pattern in the key for an attacker to guess or find. Even if one of the messages could be broken, all of the other messages would remain secure since they use different keys to encrypt them. Unfortunately, one-time use pads require that two identical copies of the pad are produced and distributed securely before they can be used.

Index

Block Ciphers & Cipher Block Chaining (CBC) Mode

In cryptography, a block cipher mode of operation is an algorithm that uses a block cipher to provide information security such as confidentiality or authenticity.

In cryptography, a block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks. Block ciphers are specified elementary components in the design of many cryptographic protocols and are widely used to encrypt large amounts of data, including in data exchange protocols. A block cipher uses blocks as an unvarying transformation.

Even a secure block cipher is suitable for the encryption of only a single block of data at a time, using a fixed key. A multitude of modes of operation has been designed to allow their repeated use in a secure way to achieve the security goals of confidentiality and authenticity. However, block ciphers may also feature as building blocks in other cryptographic protocols, such as universal hash functions and pseudorandom number generators.

A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block. A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block.

Most modes require a unique binary sequence, often called an initialization vector (IV), for each encryption operation. The IV has to be non-repeating and, for some modes, random as well. The initialization vector is used to ensure distinct ciphertexts are produced even when the same plaintext is encrypted multiple times independently with the same key. Block ciphers may be capable of operating on more than one block size, but during transformation the block size is always fixed. Block cipher modes operate on whole blocks and require that the last part of the data be padded to a full block if it is smaller than the current block size. There are, however, modes that do not require padding because they effectively use a block cipher as a stream cipher.

The earliest modes of operation, ECB, CBC, OFB, and CFB, date back to 1981 and were specified in FIPS 81, DES Modes of Operation. In 2001, the US National Institute of Standards and Technology (NIST) revised its list of approved modes of operation by including AES as a block cipher and adding CTR mode

The block cipher modes ECB, CBC, OFB, CFB, CTR, and XTS provide confidentiality, but they do not protect against accidental modification or malicious tampering. Modification or tampering can be detected with a separate message authentication code such as CBC-MAC, or a digital signature. The cryptographic community recognized the need for dedicated integrity assurances and NIST responded with HMAC, CMAC, and GMAC.

Q: Dion Training has contracted a software development firm to create a bulk file upload utility for its website. During a requirements planning meeting, the developers asked what type of encryption is required for the project. After some discussion, Jason decides that the file upload tool should use a cipher capable of encrypting 64 bits of data at a time before transmitting the files from the web developer's workstation to the webserver. What of the following should be selected to meet this security requirement?

A: Block Cipher

A block cipher is used to encrypt multiple bits at a time before moving to the next set of data. Block ciphers generally have a fixed-length block (8-bit, 16-bit, 32-bit, 64-bit, etc.).

Stream ciphers encrypt a single bit (or byte) at a time during their encryption process.

Index

HTTPS – Encrypted HTTP

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It **uses encryption for secure communication over a computer network**, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

The principal motivations for HTTPS are **authentication** of the accessed website and protection of the **privacy** and **integrity** of the exchanged data while it is in transit. **It protects against man-in-the-middle attacks, and the bidirectional block cipher encryption of communications between a client and server protects the communications against eavesdropping and tampering**.

The authentication aspect of HTTPS requires a trusted third party to sign server-side digital certificates. This was historically an expensive operation, which meant fully authenticated HTTPS connections were usually found only on secured payment transaction services and other secured corporate information systems on the World Wide Web. In 2016, a campaign by the Electronic Frontier Foundation with the support of web browser developers led to the protocol becoming more prevalent.

HTTPS is now used more often by web users than the original, non-secure HTTP, primarily to protect page authenticity on all types of websites, secure accounts, and keep user communications, identity, and web browsing private.

Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. **The protocol is widely used in applications such as email, instant messaging, and voice over IP, but its use in securing HTTPS remains the most publicly visible.**

The TLS protocol aims primarily to provide security, including privacy (confidentiality), integrity, and authenticity through the use of cryptography, **such as the use of certificates**, between two or more communicating computer applications. It **runs in the presentation layer** and is itself composed of two layers: the TLS record and the TLS handshake protocols.

The closely related Datagram Transport Layer Security (DTLS) is a communications protocol that provides security to datagram-based applications. In technical writing, references to "(D)TLS" are often seen when it applies to both versions.

TLS is a proposed **Internet Engineering Task Force (IETF) standard**, first defined in 1999, and the current version is TLS 1.3, defined in August 2018. TLS builds on the **now-deprecated SSL (Secure Sockets Layer)** specifications (1994, 1995, 1996) **developed by Netscape** Communications for adding the HTTPS protocol to their Navigator web browser.

Q: What technology is NOT PKI x.509 compliant and cannot be used in various secure functions?

A: Blowfish

AES, Public-Key Cryptography Standards (PKCS), and SSL/TLS are all compatible with x.509 and can be used in a wide variety of functions and purposes. AES is used for symmetric encryption. PKCS is used as a digital signature algorithm. SSL/TLS is used for secure key exchange.

Index

Q: You have run a vulnerability scan and received the following output:

```
                                    ©2022 Dion Training

CVE-2011-3389
QID 42366 - SSLv3.0/TLSv1.0 Protocol weak CBC mode Server side
            vulnerability
Check with: openssl s_client -connect login.diontraining.com:443 - tls
            -cipher "AES:CAMELLISA:SEED:3DES:DES"
```

Which of the following categories should this be classified as?

A: Web Application Cryptography Vulnerability

This vulnerability should be categories as a web application cryptographic vulnerability. This is shown by the weak SSLv3.0/TLSv1.0 protocol being used in cipher block chaining (CBC) mode. Specifically, the use of the 3DES and DES algorithms during negotiation is a significant vulnerability. A stronger protocol should be used, such as forcing the use of AES.

Index

Cryptography: Key Stretching Techniques

In cryptography, key stretching techniques are used to make a possibly weak key, typically a password or passphrase, more secure against a brute-force attack by increasing the resources (time and possibly space) it takes to test each possible key.

There are **several ways** to perform key stretching: One way is to apply a cryptographic hash function or a block cipher repeatedly in a loop. Another way is to use cryptographic hash functions that have large memory requirements – these can be effective in frustrating attacks by memory-bound adversaries.

Q: Dion Training has added a salt and cryptographic hash to their passwords to increase the security before storing them. To further increase security, they run this process many times before storing the passwords. What is this technique called?

A: Key Stretching (NOT Salting!)

Code Analysis: Static vs Dynamic Approaches

Static Code Analysis examines code to identify issues within the logic and techniques. Static Application Security Testing (SAST) is a testing process that looks at the application from the inside out without executing the program, but rather by examining the source code, byte code or application binaries for signs of security vulnerabilities. **DeepScan** is an example of a static code analysis tool: it inspects the code for possible errors and issues without actually running the code.

Dynamic Code Analysis adopts the opposite approach and involves running code and examining the outcome, which also entails testing possible execution paths of the code. Dynamic Application Security Testing (DAST) looks at the application from the outside in — by examining it in its running state and trying to manipulate it in order to discover security vulnerabilities. **A fuzzer, decompiler, and fault injector are all dynamic analysis tools because they require the program to be run during testing and analysis.**

Q: A software assurance laboratory performs a dynamic assessment on an application by automatically generating random data sets and inputting them to cause an error or failure condition. Which of the following is the laboratory performing?

A: Fuzzing (NOT Stress Testing!)

Fuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, failing built-in code assertions, or potential memory leaks.

Index

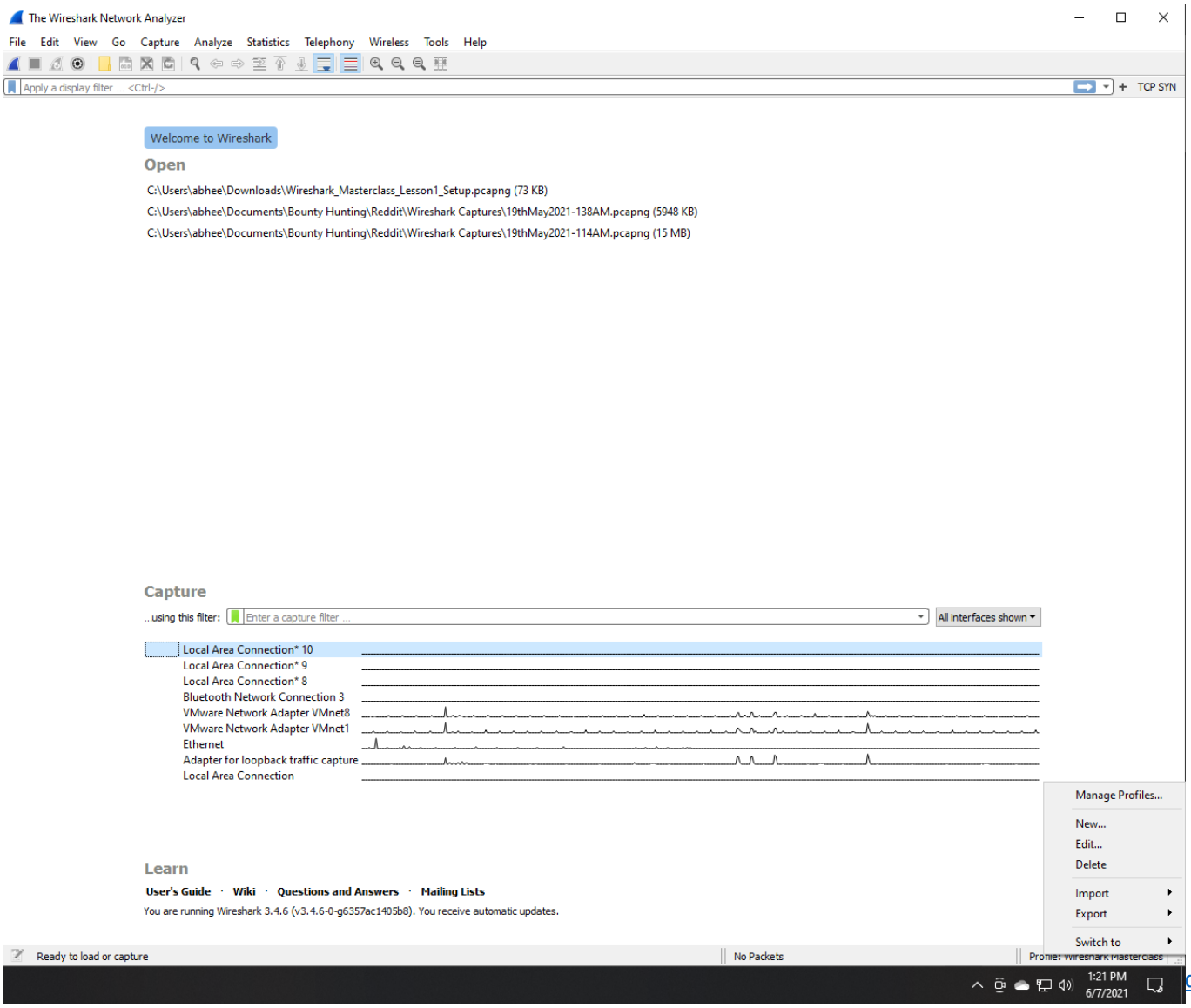
Tools of the Trade

Protocol Analyzers

→ Check packets to & from web app
→ Check ports being used
→ Check IPs
→ Check encryption
→ Analyze web traffic

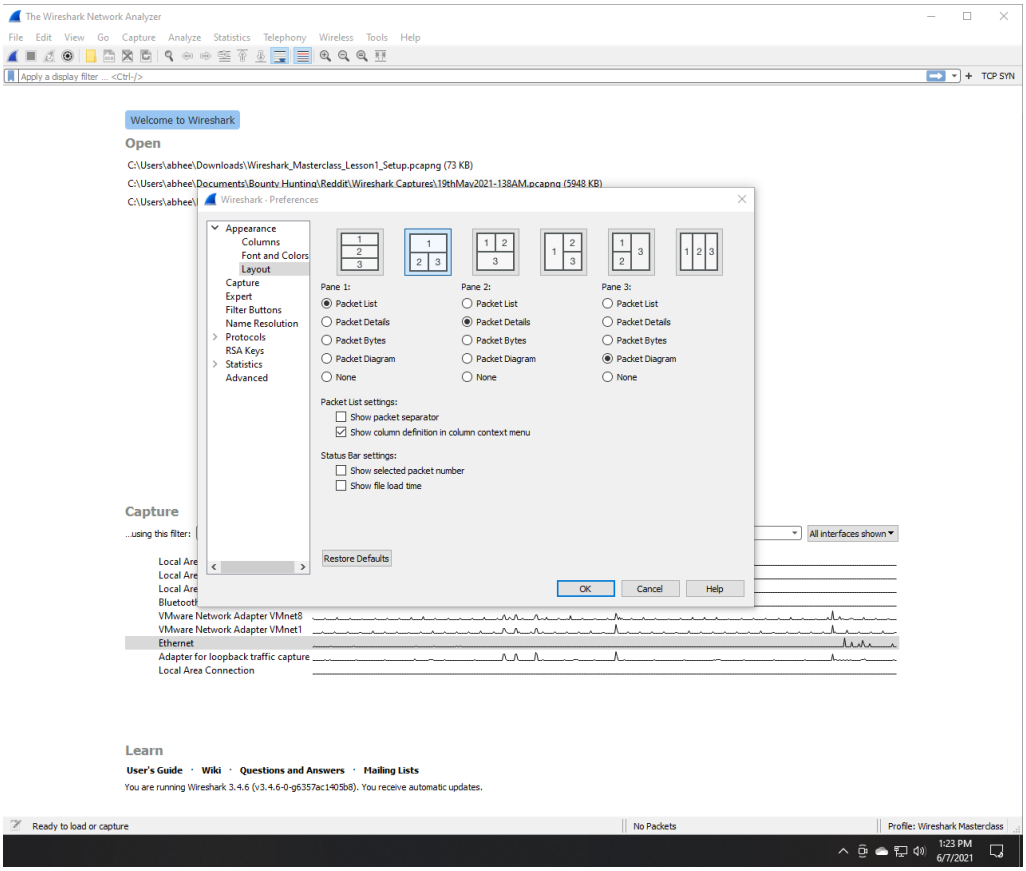
WIRESHARK

- **Profiles: Create a New Profile by Right Clicking the Bottom Right of the Screen:**

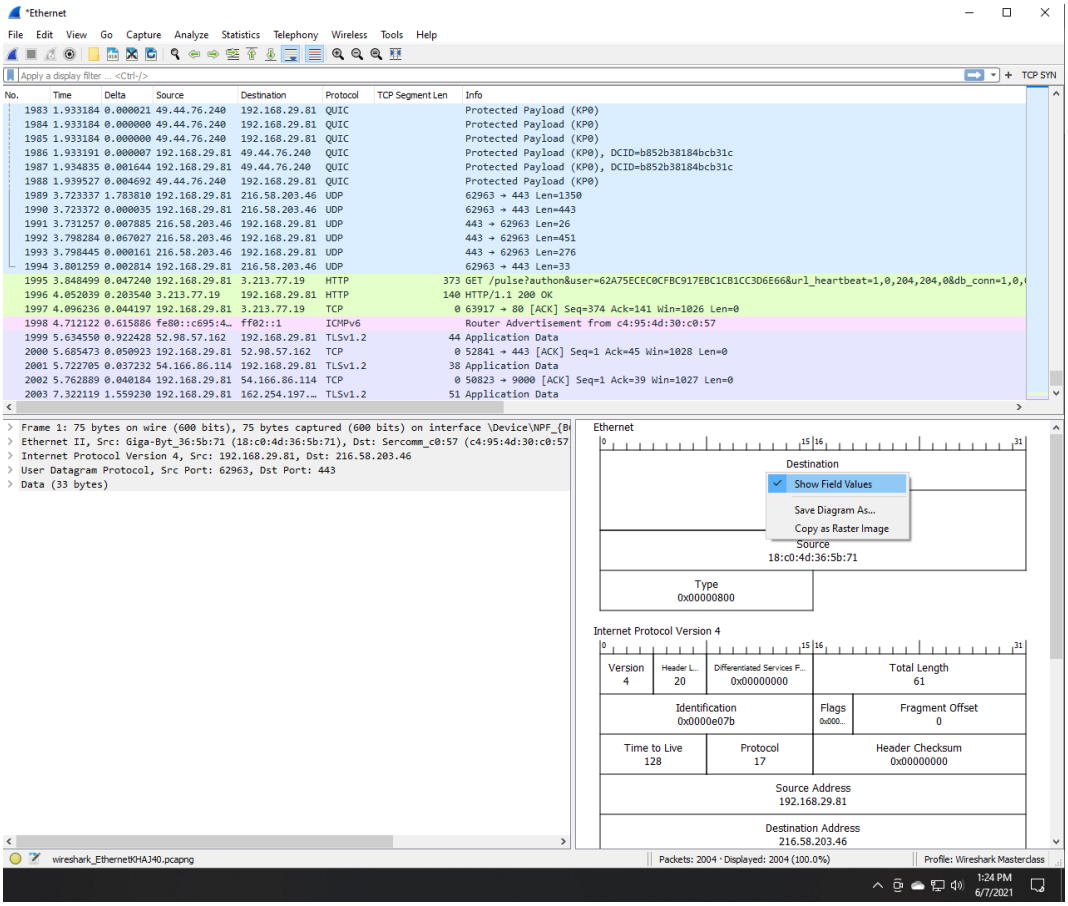


dex

- **Layouts: Adjust Layout by Heading to Edit -> Preferences:**

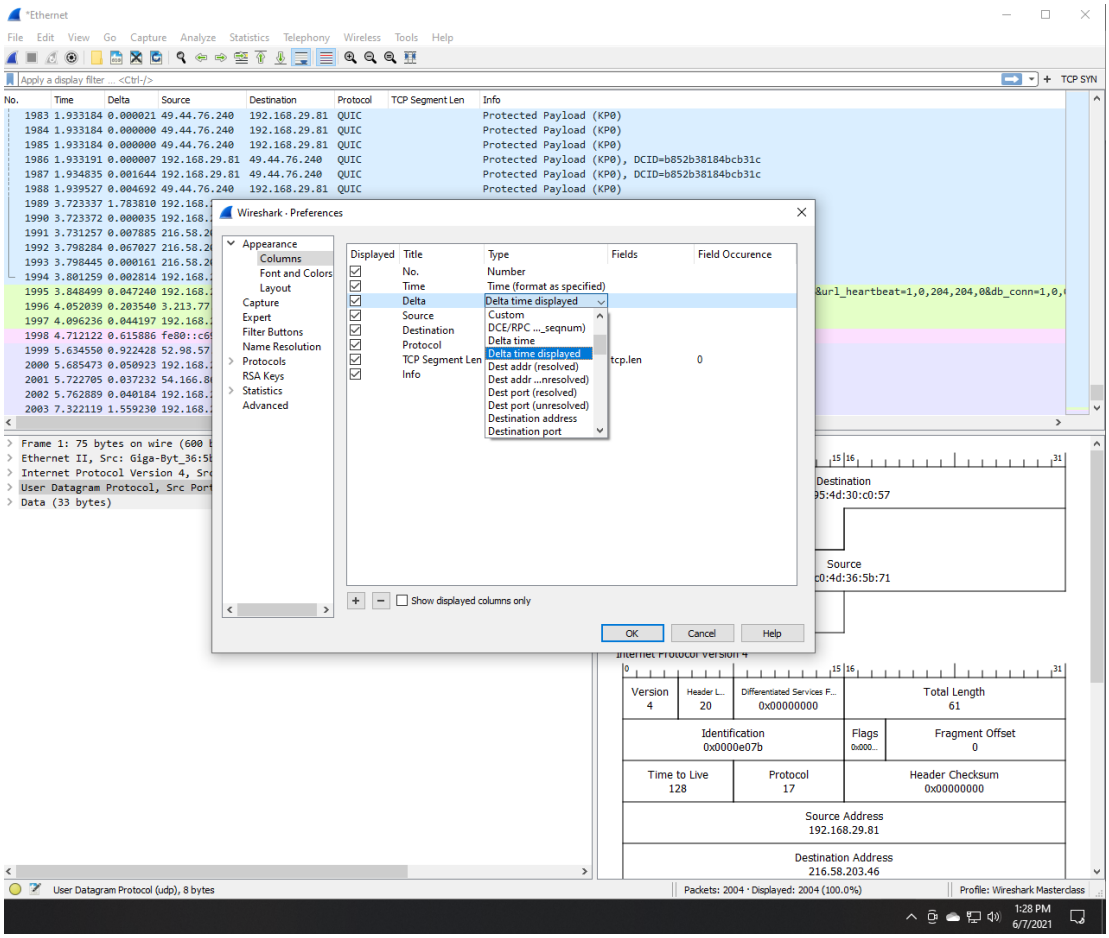


- **Network Diagram Field Values: Show actual field values transmitted in the captured packet by right clicking the network diagram and selecting the relevant option:**

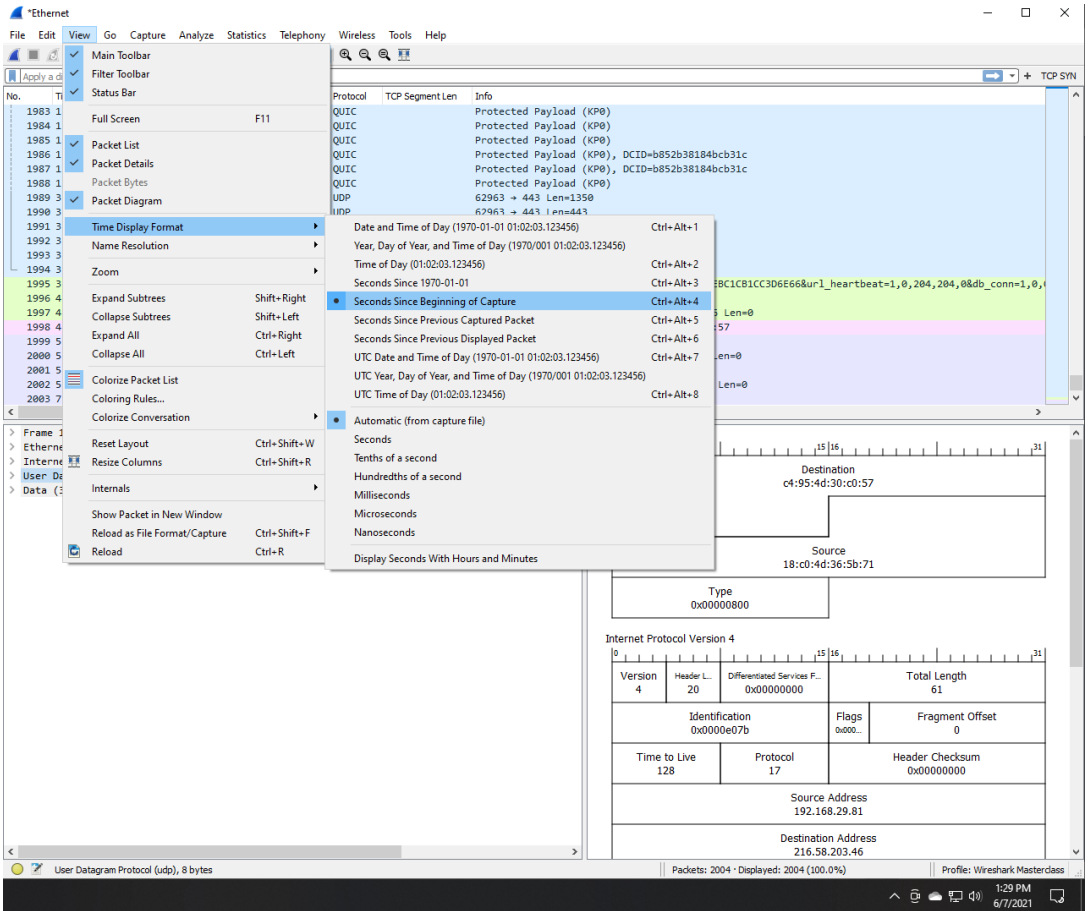


Index

- **Columns: Add a New Column, such as a Delta Time Column, by Heading to Edit -> Preferences:**

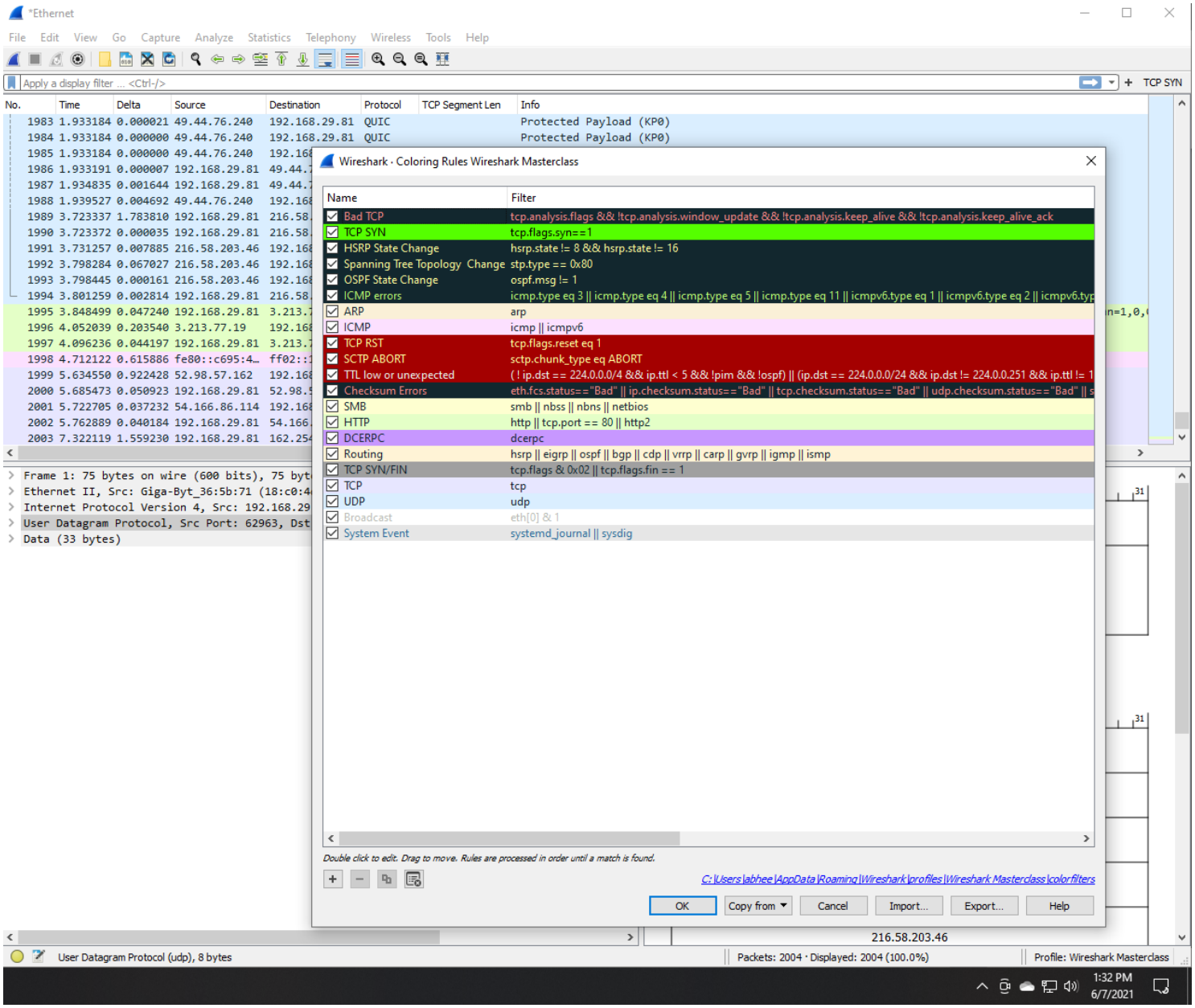


- **Time Format: Adjust Time Format by Heading to View -> Time Display Format:**



Index

- **Coloring Rules & Filters: Add and Edit Filters and Coloring Rules by Heading to View -> Coloring Rules… Add a New Rule by Hitting + and typing it in. Hit Foreground & Background Buttons to Adjust the Color:**

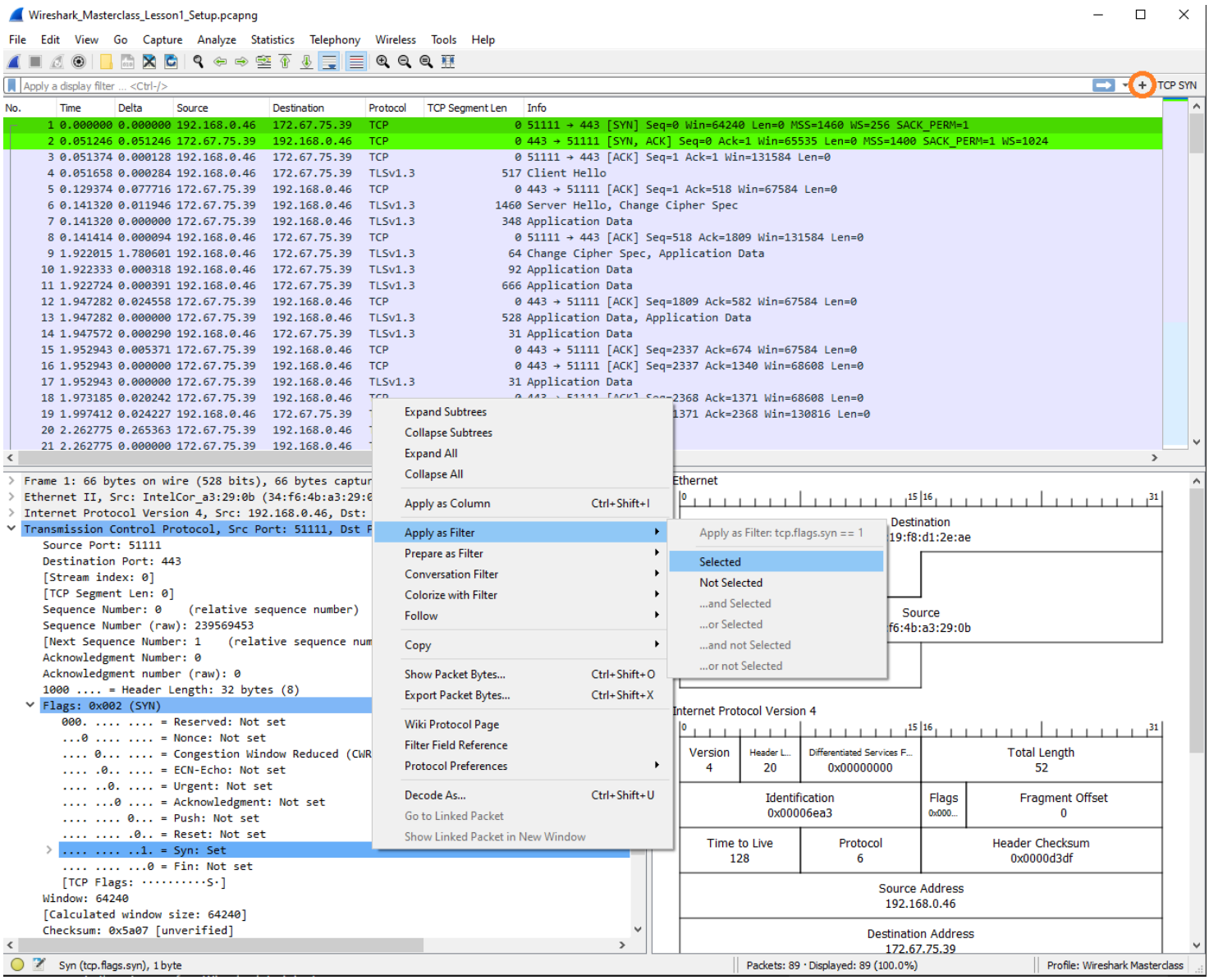


Note that color rules are applied in order they're present! Drag and move them around. With the above setup, only the first TCP SYN packet will be highlighted in green, any retransmissions will be marked black & red as per rule 1.

Lastly, refresh the captured packets list after adding new rules!

Index

- **Filters: Apply a filter from a Captured Packet's Field Value Directly:**



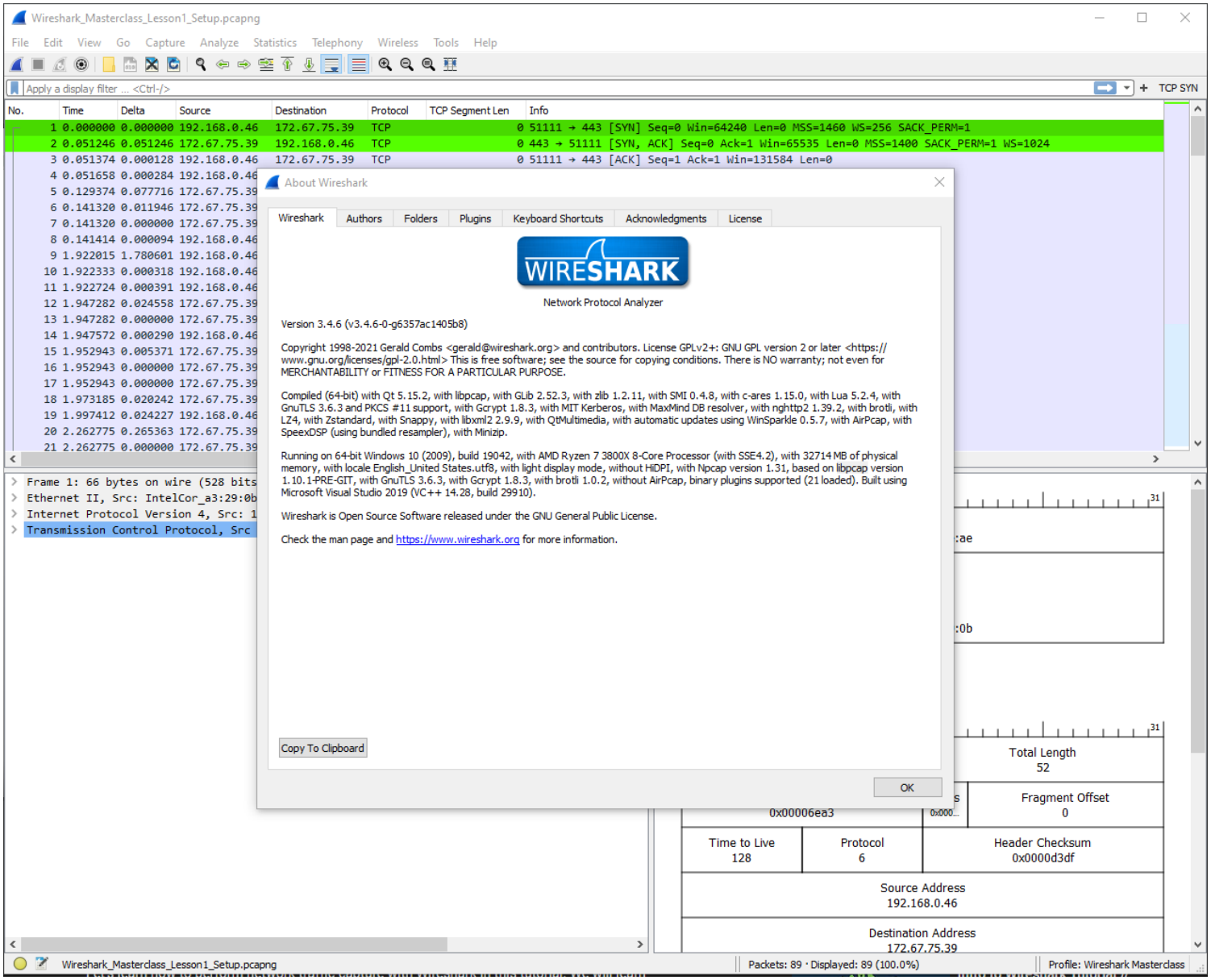
Hit the plus on the top-right of the search/filter bar to add the currently selected filter as a dedicated, separate button. Give it a label as preferred. Now you can simply hit this to filter out packets instead of having to type it every time.

Adding a New Column, the Short & Easy Way: Simply hit the "Apply as Column" option you see in the menu in the screenshot above to add any field of a captured packet as a column!

TCP Segment Length, a field visible above, reveals the amount of actual data encompassed in the payload of this specific packet. This shows us how much data this packet is actually carrying in terms of bytes of data. The overall length then can even be ignored, and you'll notice that we've removed the Length column all together in favor of TCP Segment Length, which has been added by right clicking on that specific field in the screenshot above and selecting "Apply as column".

Index

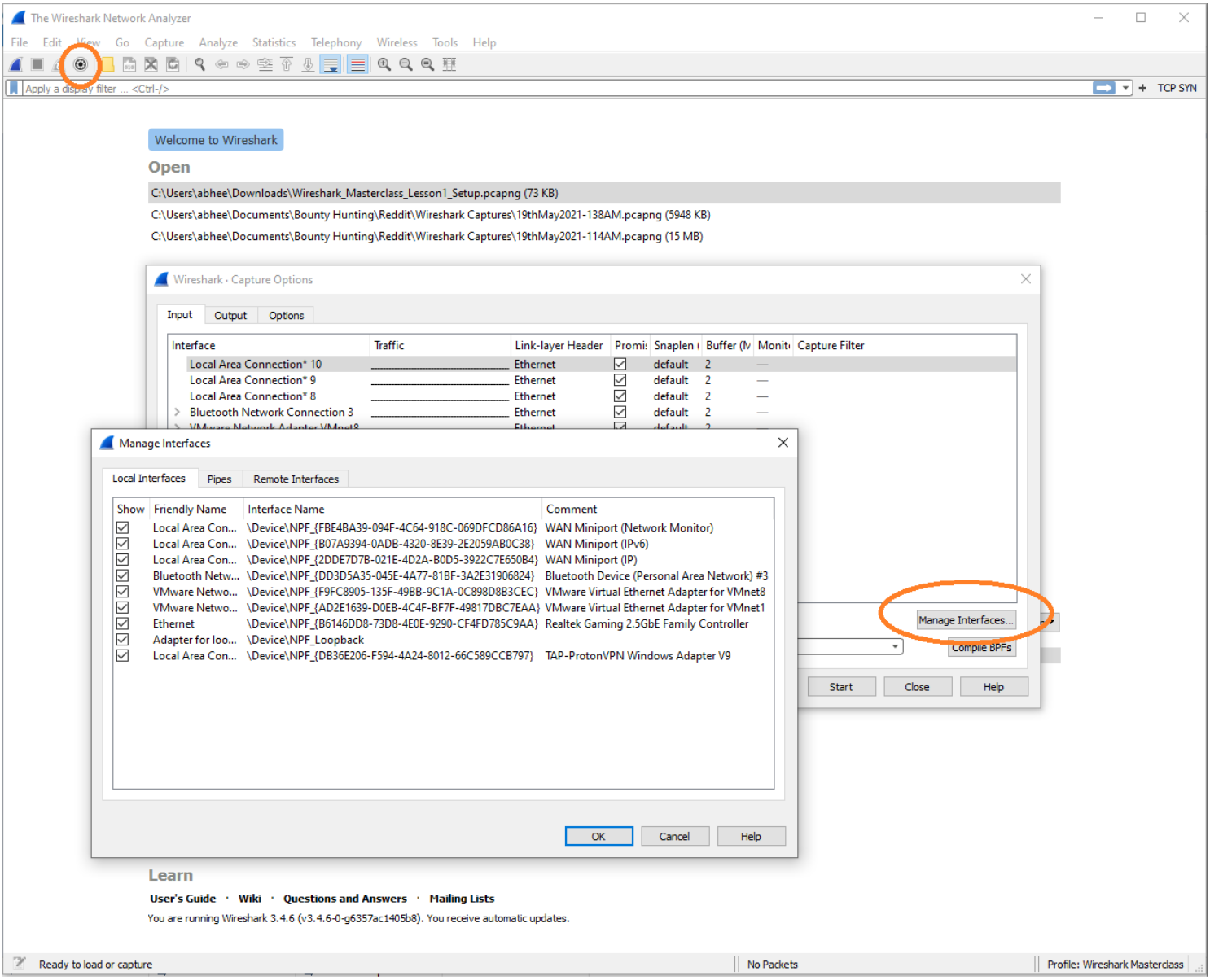
- **Identifying Wireshark's Packet Capture Driver:**



Go to Help -> About Wireshark

Index

- **Adjust Interfaces:**



Click the gear icon at the top left and hit Manage Interfaces

→ Promiscuous mode is explained below

→ Use Snaplength to stop the capture automatically after a certain amount of data has been captured. Don't capture too less accidently, though!

→ Buffer specifies the kernel buffer in MB and the default 2MB is fine and can be left as is unless you're in a very high throughput environment like a data center

→ Use the Output tab to setup save options, including a permanent save file that's overwritten, the format of this output file, the creation of a new file every time a certain condition is met such as size or number of packets etc. and even a ring buffer to limit the number of files created

Index

Promiscuous Mode:

Promiscuous: Uninhibited, unrestrained

As per Wikipedia*: In computer networking,* ***promiscuous mode*** *is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is specifically programmed to receive. This mode is normally used for packet sniffing that takes place on a router or on a computer connected to a wired network or one being part of a wireless LAN. Interfaces are placed into promiscuous mode by software bridges often used with hardware virtualization.*

In IEEE 802 networks such as Ethernet or IEEE 802.11, each frame includes a destination MAC address. In non-promiscuous mode, when a NIC receives a frame, it drops it unless the frame is addressed to that NIC's MAC address or is a broadcast or multicast addressed frame. In promiscuous mode, however, the NIC allows all frames through, thus allowing the computer to read frames intended for other machines or network devices.

Many operating systems require superuser privileges to enable promiscuous mode. A non-routing node in promiscuous mode can generally only monitor traffic to and from other nodes within the same broadcast domain (for Ethernet and IEEE 802.11) or ring (for Token Ring). Computers attached to the same Ethernet hub satisfy this requirement, which is why network switches are used to combat malicious use of promiscuous mode. A router may monitor all traffic that it routes.

Promiscuous mode is often used to diagnose network connectivity issues. There are programs that make use of this feature to show the user all the data being transferred over the network. Some protocols like FTP and Telnet transfer data and passwords in clear text, without encryption, and network scanners can see this data. Therefore, computer users are encouraged to stay away from insecure protocols like telnet and use more secure ones such as SSH.

Detection

As promiscuous mode can be used in a malicious way to capture private data in transit on a network, computer security professionals might be interested in detecting network devices that are in promiscuous mode. In promiscuous mode, some software might send responses to frames even though they were addressed to another machine. However, experienced sniffers can prevent this (e.g., using carefully designed firewall settings). An example is sending a ping (ICMP echo request) with the wrong MAC address but the right IP address. If an adapter is operating in normal mode, it will drop this frame, and the IP stack never sees or responds to it. If the adapter is in promiscuous mode, the frame will be passed on, and the IP stack on the machine (to which a MAC address has no meaning) will respond as it would to any other ping. The sniffer can prevent this by configuring a firewall to block ICMP traffic.

Find the page here: https://en.wikipedia.org/wiki/Promiscuous_mode

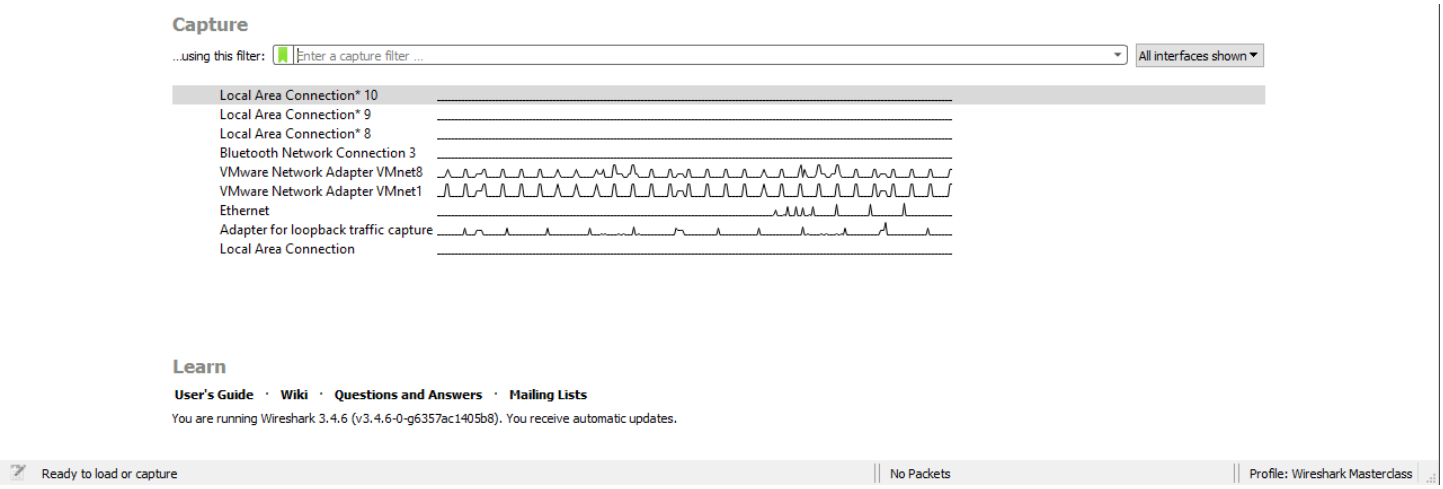
Index

- **Filtering**

→ “Pre-filtering” is the capture of only a specific type of traffic, such as DNS requests.
→ “Display filtering” is filtering on already captured traffic for specific requests, such as DNS again.

A. Pre-Capture Filtering:

→ Set a pre-capture filter in Wireshark by specifying the filter along with the interface when you begin capturing:

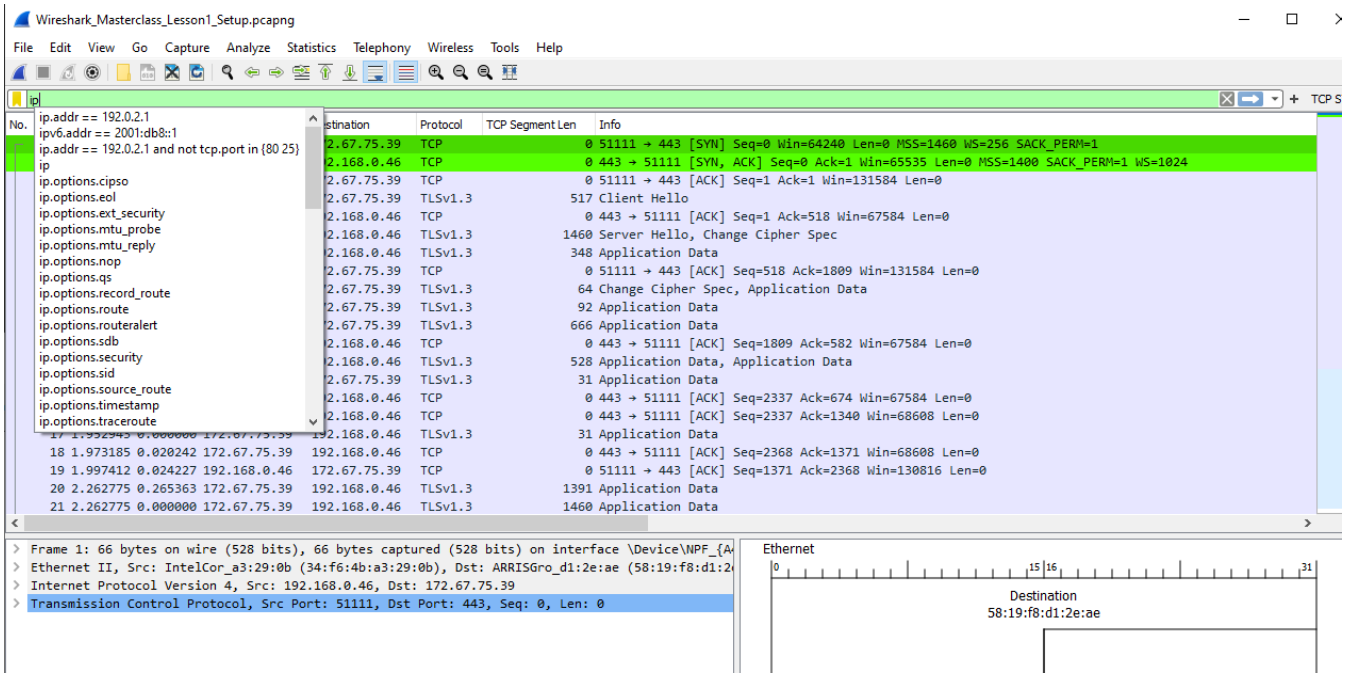


→ Be careful of the syntax you put into the filter bar as typing some values such as “DNS” won’t work, and the bar will turn red
→ The language for capture filters is different than that for display filters: “DNS” would work just fine as a display filter!
→ Here are some valid capture filter values you can feed in:
  - IP
  - ARP
  - port <>
    - port 53: this would be a DNS filter on UDP port 53
  - TCP
  - host <>
    - Wireshark will give you suggestions here
→ Do not set too fine a capture filter! Because say you were only capturing for TCP but there were ICMP messages trying to inform you of packet loss over the connection, you wouldn’t see those at all as you’d set Wireshark to only capture TCP!

Index

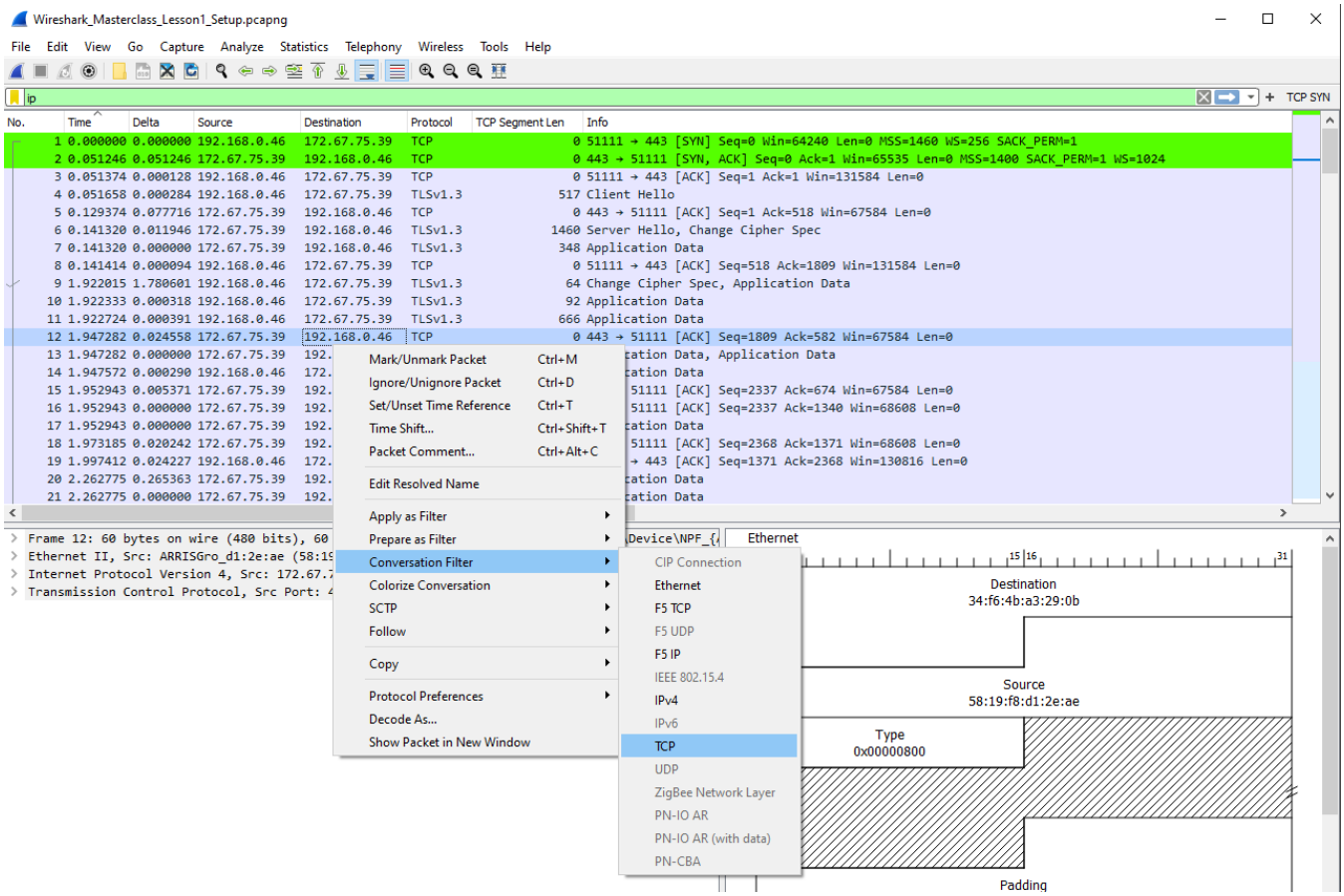
B. Display Filtering:

→ The filter bar will again provide suggestions; for example, typing “ip” will produce the following drop-down:



Typing in a specific filter can be cumbersome due to both the length and specific syntax of the filter so anytime you can, use Wireshark’s right-click filtering mechanism described in point 7

→ This can also be used for setting a **conversation filter**, filtering for all or specific traffic communications to and from a specific server or destination:



Index

→ In the above filter we're filtering for all TCP traffic to and from the specific destination address 192.168.0.46 and will also include the port numbers on both ends

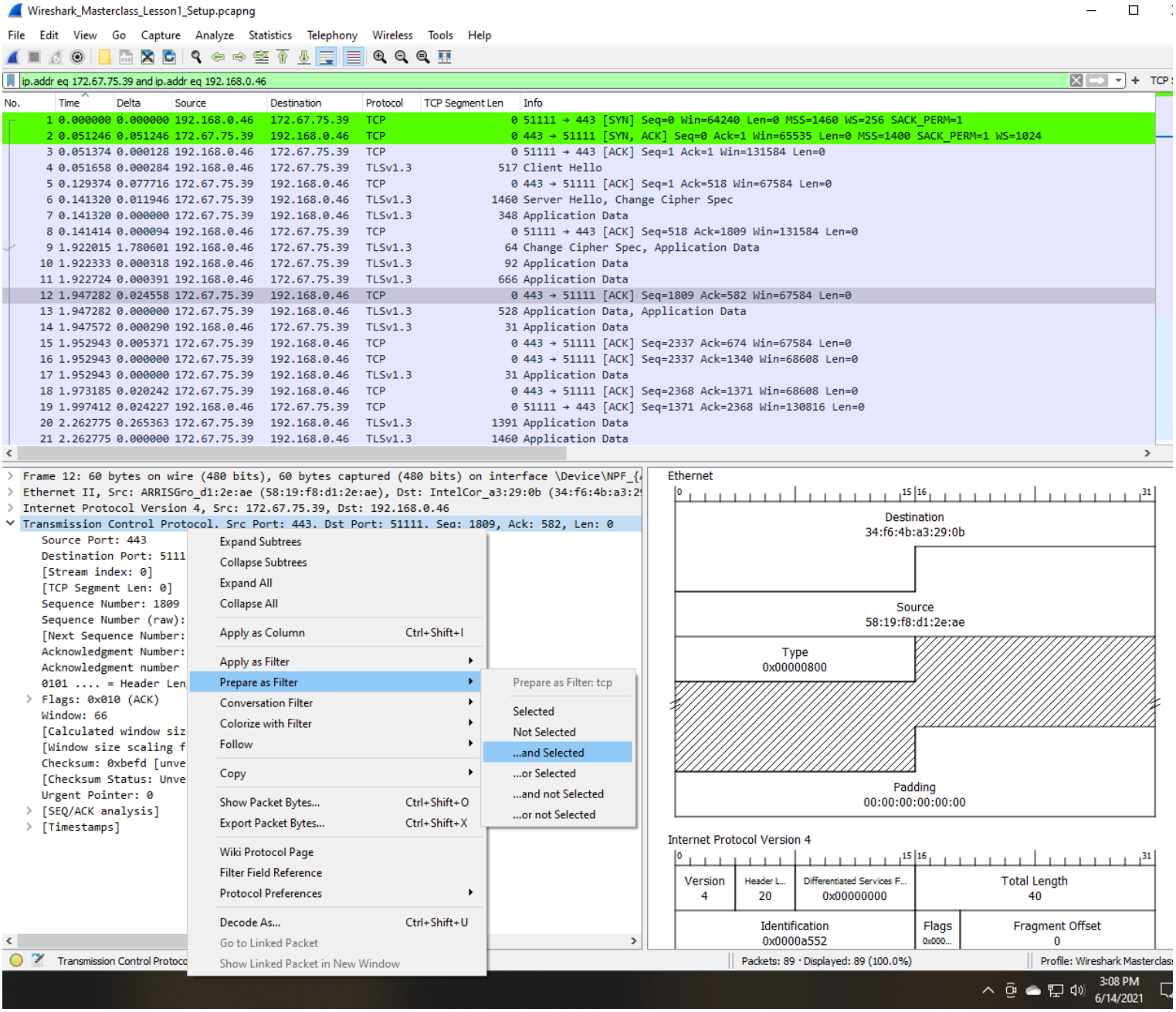
→ Applying the TCP filter above will result in the following filter being auto set in the filter bar:

(ip.addr eq 172.67.75.39 and ip.addr eq 192.168.0.46) and (tcp.port eq 443 and tcp.port eq 51111)

→ Now, once we have set a filter, we can further add to this filter via "and" clauses & parentheses as above

→ These additional clauses need not be manually written: say you carried out only IP filtering and now wish to add TCP: ***ip.addr eq 172.67.75.39 and ip.addr eq 192.168.0.46***

→ Simply right-click on any of the captured packets and head down to the TCP header and proceed to use right-click filtering:

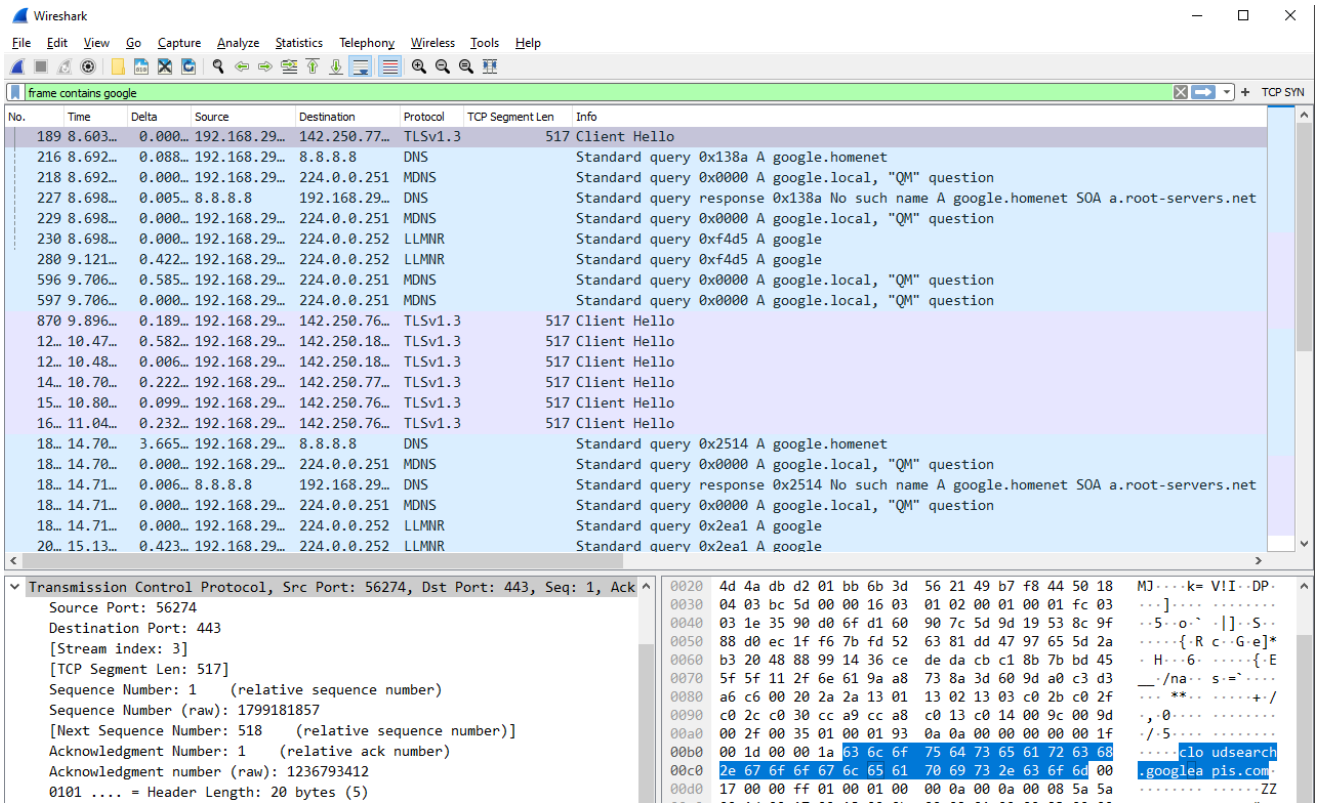


Index

→ Some notes on the above:
    - "Prepare as Filter" tells Wireshark to word out the filter in the bar but not apply it yet, essentially allowing you to review the filter instead of applying it directly
    - "…and Selected" tells Wireshark to add to any currently applied display filters instead of simply overwriting them
→ *This is the typical way to build out filters: start with an endpoint, then proceed to add its conversation, then add its port number or application/protocol values and continue building out your filters that way*

→ Another great use of filters is to hide captured traffic that you're not using for your troubleshooting, say for example if you do not wish to see the ARP traffic: typing in ***not arp*** or simply "***! arp"*** will do the trick
→ Expand this further: ***not (arp or ipv6 or ssdp)***
→ Moving further, what if you'd want to filter for a TCP conversation that's spread across several different ports? For example, you may be using an application that could be TCP port 80 or 443, how would you set a filter for something like this? Via this filter: ***tcp.port in {80 443 8080}***

→ We can also carry out **"string filtering"** when looking for specific words
→ Be careful though because now-a-days packets are often encrypted so a lot times the specific string will be encrypted!
→ Some packets such as DNS requests or TLS handshakes still contain cleartext in Wireshark and are thus still available for troubleshooting via string filtering
→ When setting a string filter, we start off with specifying what protocol or what layer would you like to begin this filtering and simply stating "frame" is a good safe bet as it scans all captured packets
→ So based on the above, say we're looking for frames containing "google": ***frame contains google***
→ This will look through all captured packets for the word "google"
→ This "contains" filter is case-sensitive! For a case-insensitive search use "matches", which is a regex type search: ***frame matches google***



Index

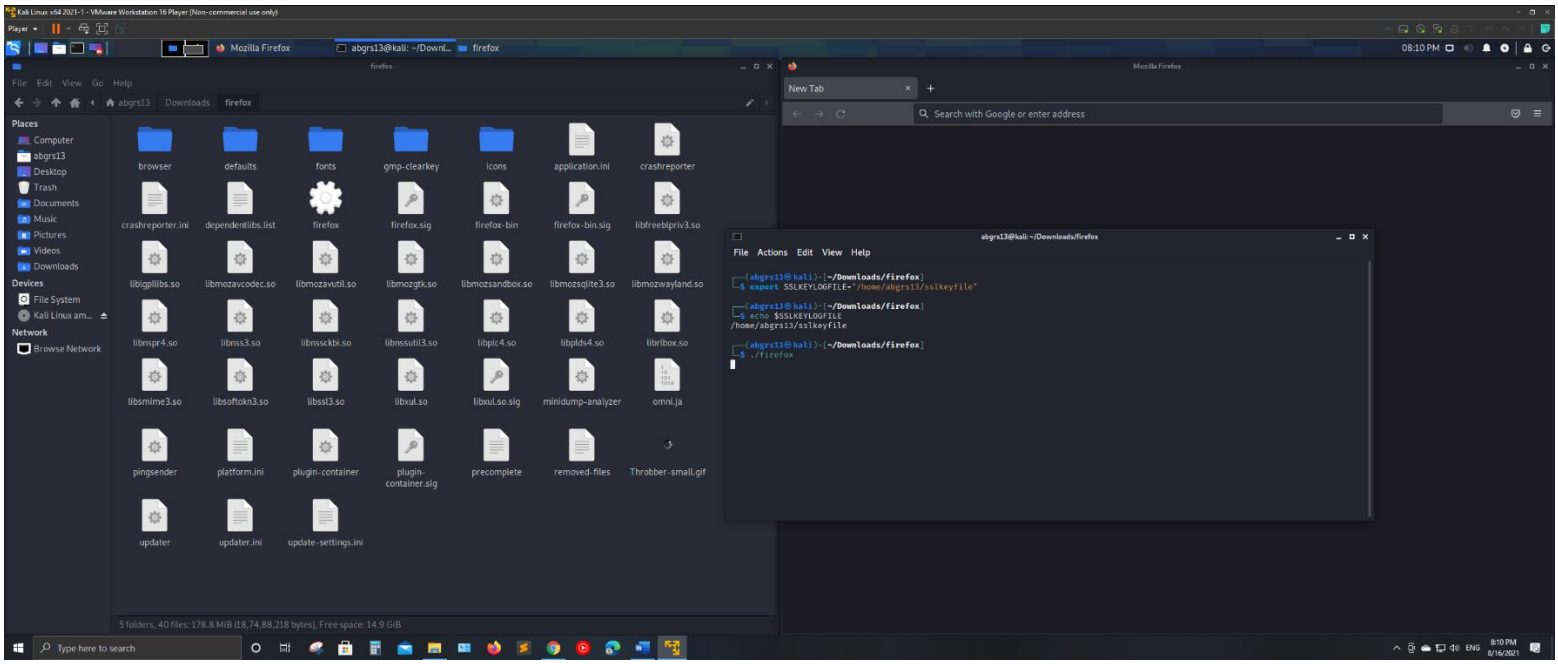
- **Decrypting HTTPS Traffic in Wireshark**

A. Kali Linux:

→ Decrypting traffic involves capturing the SSL key in a keystore file and directing Wireshark to use that file in regard to the captured traffic
→ To do this, we create an SSL keystore file which our browser subsequently uses to store the keys for the session
→ In Kali Linux, this file is created on a per-session basis
→ Kali Linux comes with Firefox ESR preinstalled, for some reason this browser refuses to cooperate in this process
→ So, head over to the Firefox site and simply download the latest non-ESR build for Linux
→ Then, use the *tar xjfv <firefox.tar>* to unpack the tarball archive
- X – Extract an archive
- J – Filter through bzip2, which is a free and open-source file compression program using the Burrows-Wheeler algorithm
- F – Filename of the archive
- V – Verbose output

→ CD into the extracted Firefox directory
→ Set the SSL key-log environment variable for the session:
- *export SSLKEYLOGFILE="/home/abgrs13/sslkeyfile"*
- Check that it's set properly with: *echo $SSLKEYLOGFILE*

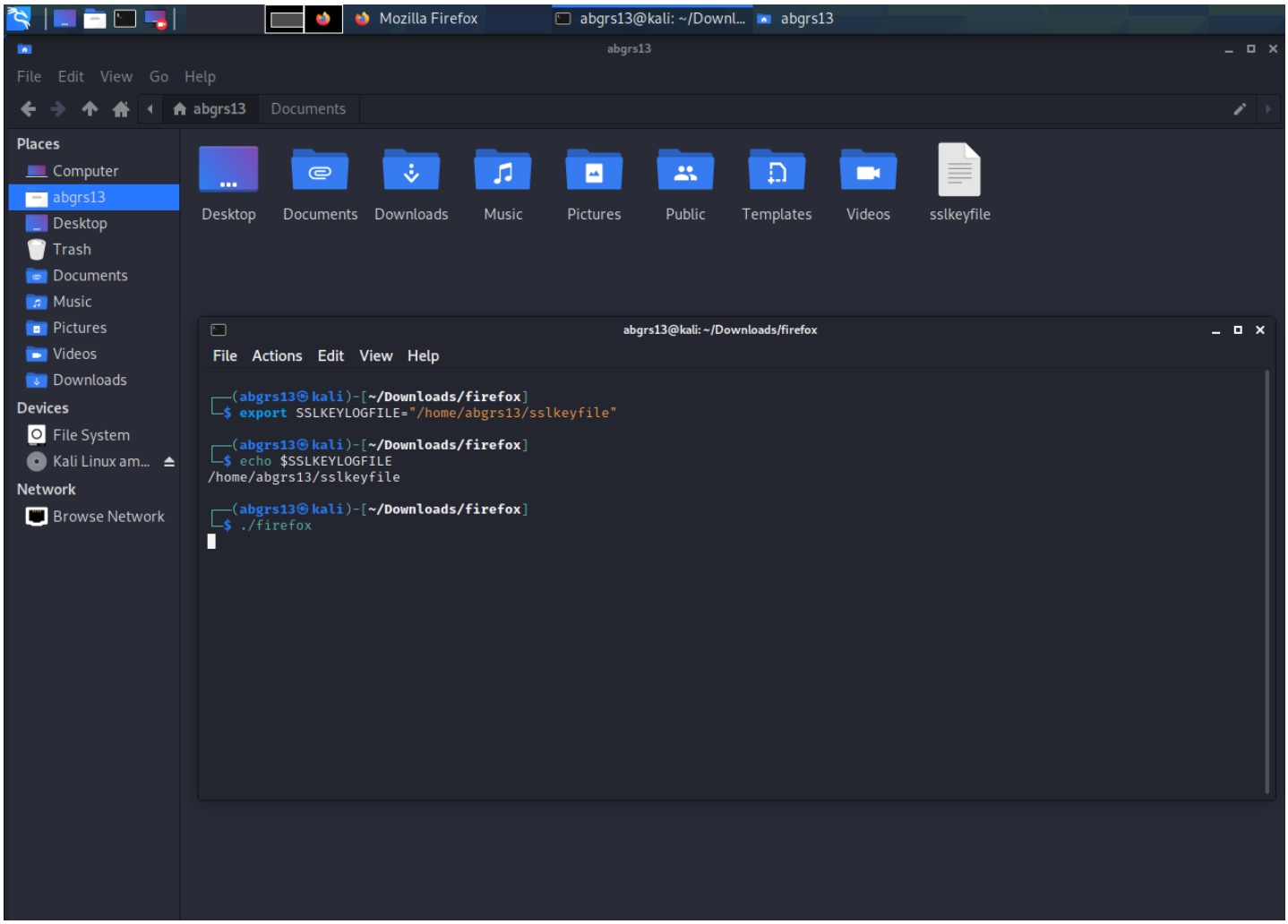
→ Run Firefox: *./firefox*



Index

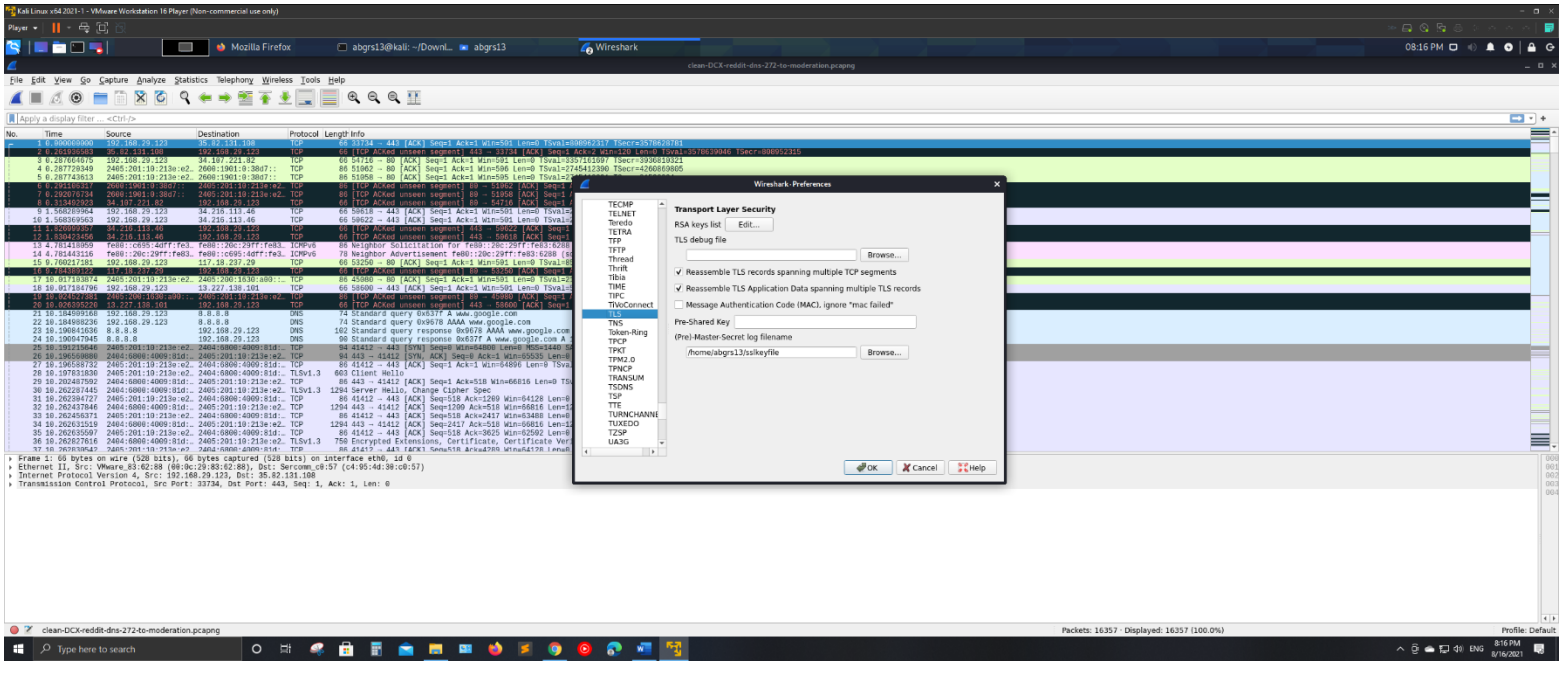
→ Open Wireshark and begin capturing traffic (TURN OFF PROMISCIOUS MODE TO CAPTURE CLEAN TRAFFIC IN THE KALI VM WHEN USING BRIDGED NETWORKING!!)

→ Visit any HTTPS site and the browser will store the keys captured in that file!



→ Set Wireshark to use this file to decrypt the captured traffic:

- *Edit -> Preferences -> Protocols -> TLS -> (Pre)-Master-Secret log filename*

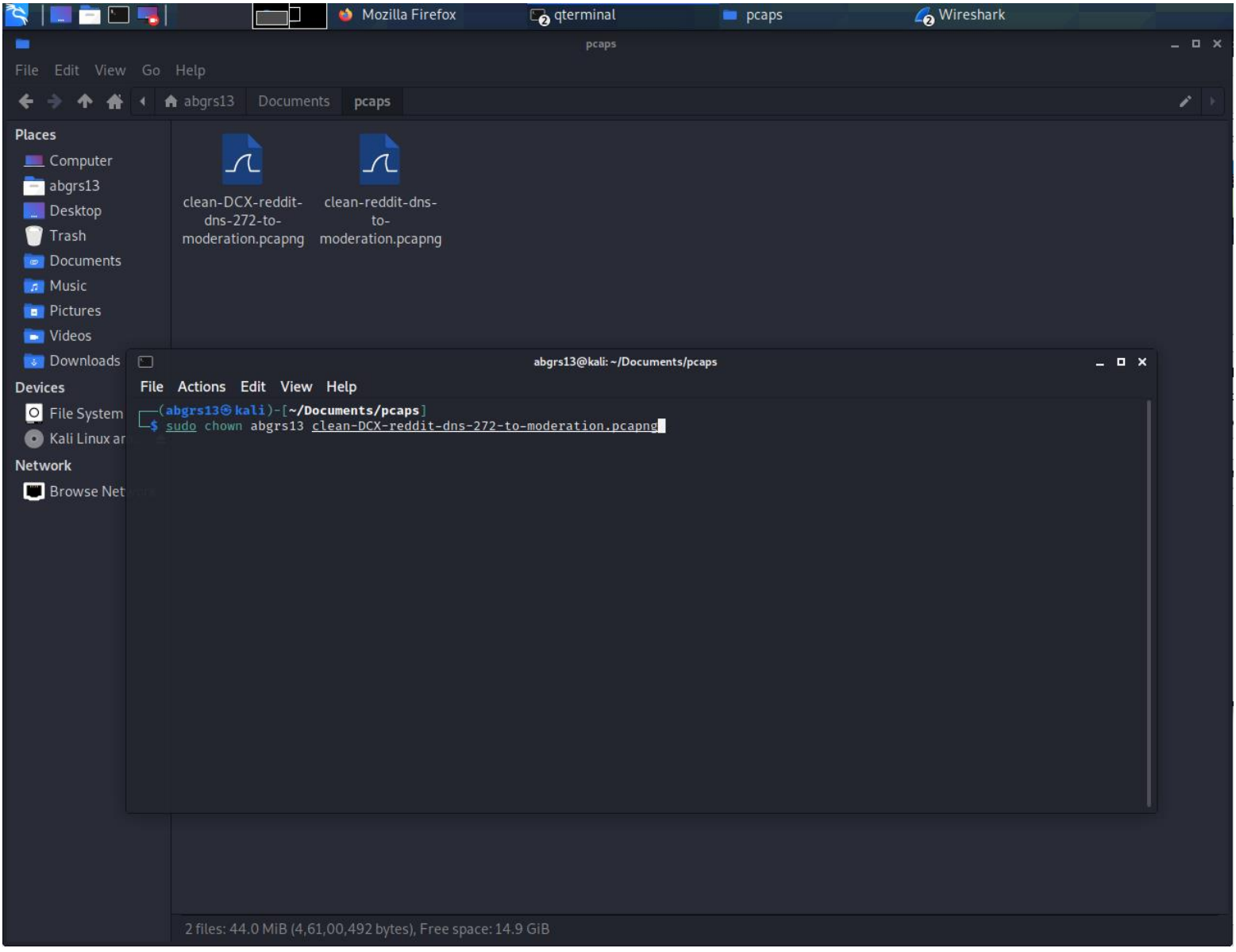


→ The now decrypted packets will be displayed, with some additional lines that weren't even visible before showing up in green!

→ Wireshark and its files belong to Root on Kali Linux, so to copy these files elsewhere, such as to Windows for further analysis will require one to transfer the ownership of these files to oneself

→ The *chown* command must be used for this, i.e., *change owner:*

- *sudo chown <new_owner_username> <filename>*

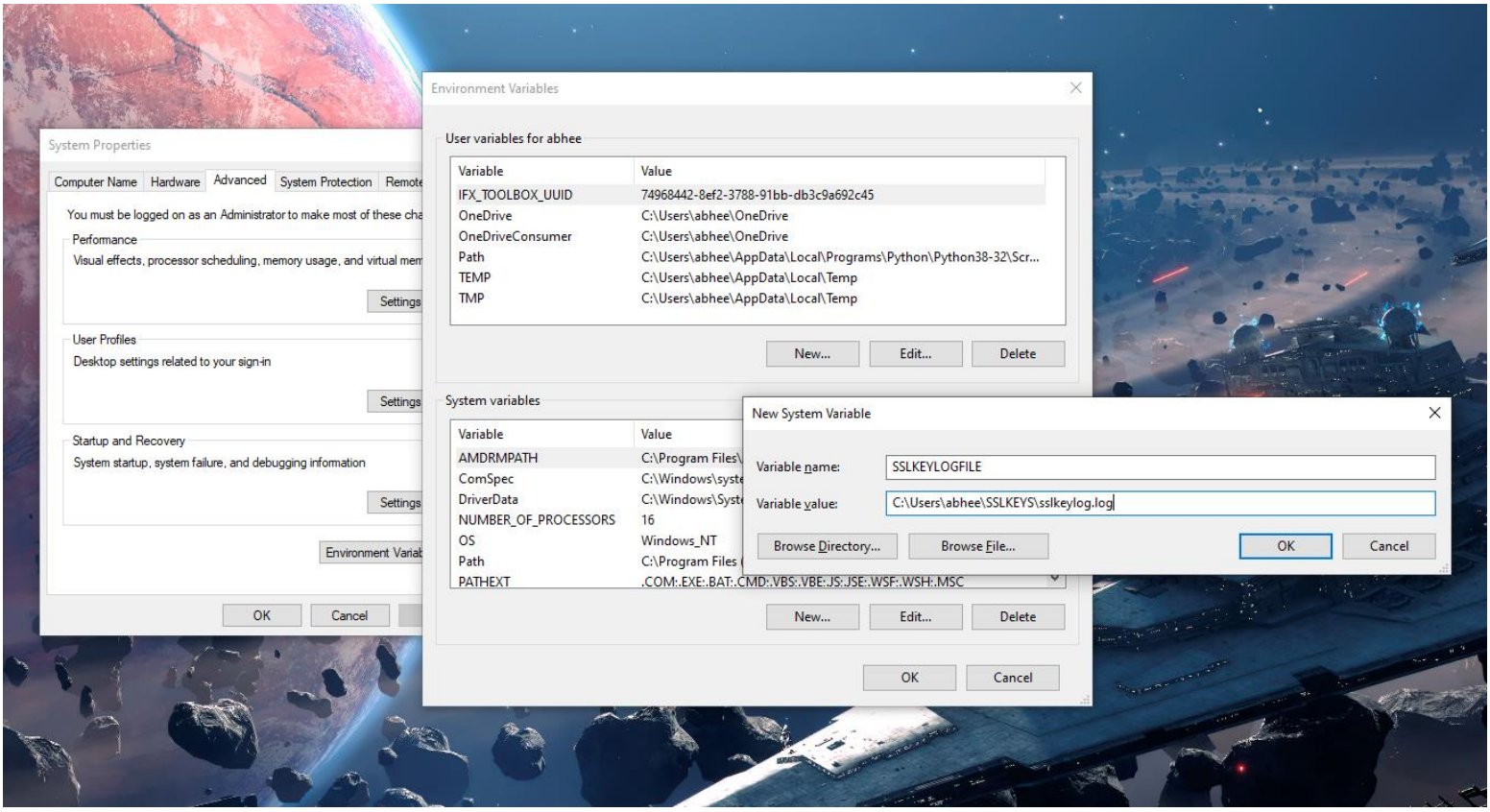


→ If desired, these pcaps and the keylog file can now be transferred to Windows to be analyzed there

Index

B. Windows

→ The process remains largely the same, but the good thing is here we can set a permanent environment variable to capture the keys in:



→ The rest of the process remains the same: restart browser (works with either Firefox/Chrome), start Wireshark, capture traffic, and set Wireshark to use this file as the keystore to decrypt traffic

Index

DUMPCAP

→ This is a command line tool that's installed by Wireshark
→ To run this and the many other tools that Wireshark installs, you need to add Wireshark's installed directory to your systems Path
→ This tool captures network packets and stores them into a file for later analysis
→ This is a large part of what Wireshark itself does, but a CMD tool may be preferrable in some environments as it's lighter to run than a GUI

1. Dumpcap Help - View All the Flags and Associated Options:
   dumpcap -h

   Note the last few lines of the output!

   Example: dumpcap -i eth0 -a duration:60 -w output.pcapng
   "Capture packets from interface eth0 until 60s passed into output.pcapng"

   Use Ctrl-C to stop capturing at any time.

2. Interfaces: View All Available Network Interfaces:
   dumpcap -D

   Use the index numbers from the output to easily specify the interface to capture from:

   Output:

   C:\Users\abhee>dumpcap -D
   1. \Device\NPF_{FBE4BA39-094F-4C64-918C-069DFCD86A16} (Local Area Connection 10)*
   2. \Device\NPF_{B07A9394-0ADB-4320-8E39-2E2059AB0C38} (Local Area Connection 9)*
   3. \Device\NPF_{2DDE7D7B-021E-4D2A-B0D5-3922C7E650B4} (Local Area Connection 8)*
   4. \Device\NPF_{DD3D5A35-045E-4A77-81BF-3A2E31906824} (Bluetooth Network Connection 3)
   5. \Device\NPF_{F9FC8905-135F-49BB-9C1A-0C898D8B3CEC} (VMware Network Adapter VMnet8)
   6. \Device\NPF_{AD2E1639-D0EB-4C4F-BF7F-49817DBC7EAA} (VMware Network Adapter VMnet1)
   7. \Device\NPF_{B6146DD8-73D8-4E0E-9290-CF4FD785C9AA} (Ethernet)
   8. \Device\NPF_Loopback (Adapter for loopback traffic capture)
   9. \Device\NPF_{DB36E206-F594-4A24-8012-66C589CCB797} (Local Area Connection)

3. Capture from a Specific Interface:
   dumpcap -i 7

Index

Output:

C:\Users\abhee>dumpcap -i 7
Capturing on 'Ethernet'
File: C:\Users\abhee\AppData\Local\Temp\wireshark_EthernetVMCO40.pcapng
Packets captured: 53
Packets received/dropped on interface 'Ethernet': 53/0 (pcap:0/dumpcap:0/flushed:0/ps_ifdrop:0) (100.0%)

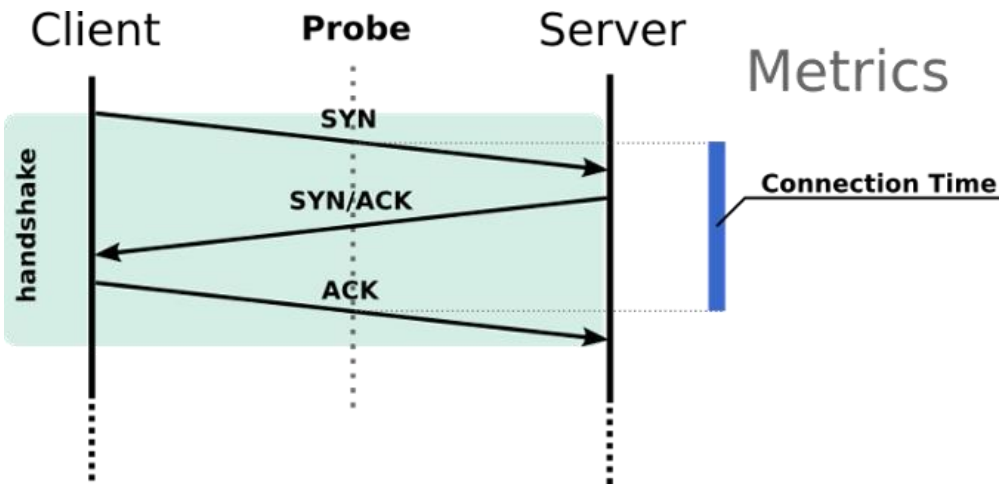
4. Specify both Interface and File Name of the Output File:
   dumpcap -i 7 -w dumpcapHelloWorldRun.pcapng

5. Specify a Ring Buffer; Example: 10 files of 500MB each:
   dumpcap -i 7 -w dumpcapHelloWorldRun-RingBuffer.pcapng -b filesize:500000 -b files:10

   - File size is specified in Kilobytes so the 500000KB equates to MB
   - This is obviously a long command so feel free to refer to Dumpcap's help to figure out the specific flags and options to specify

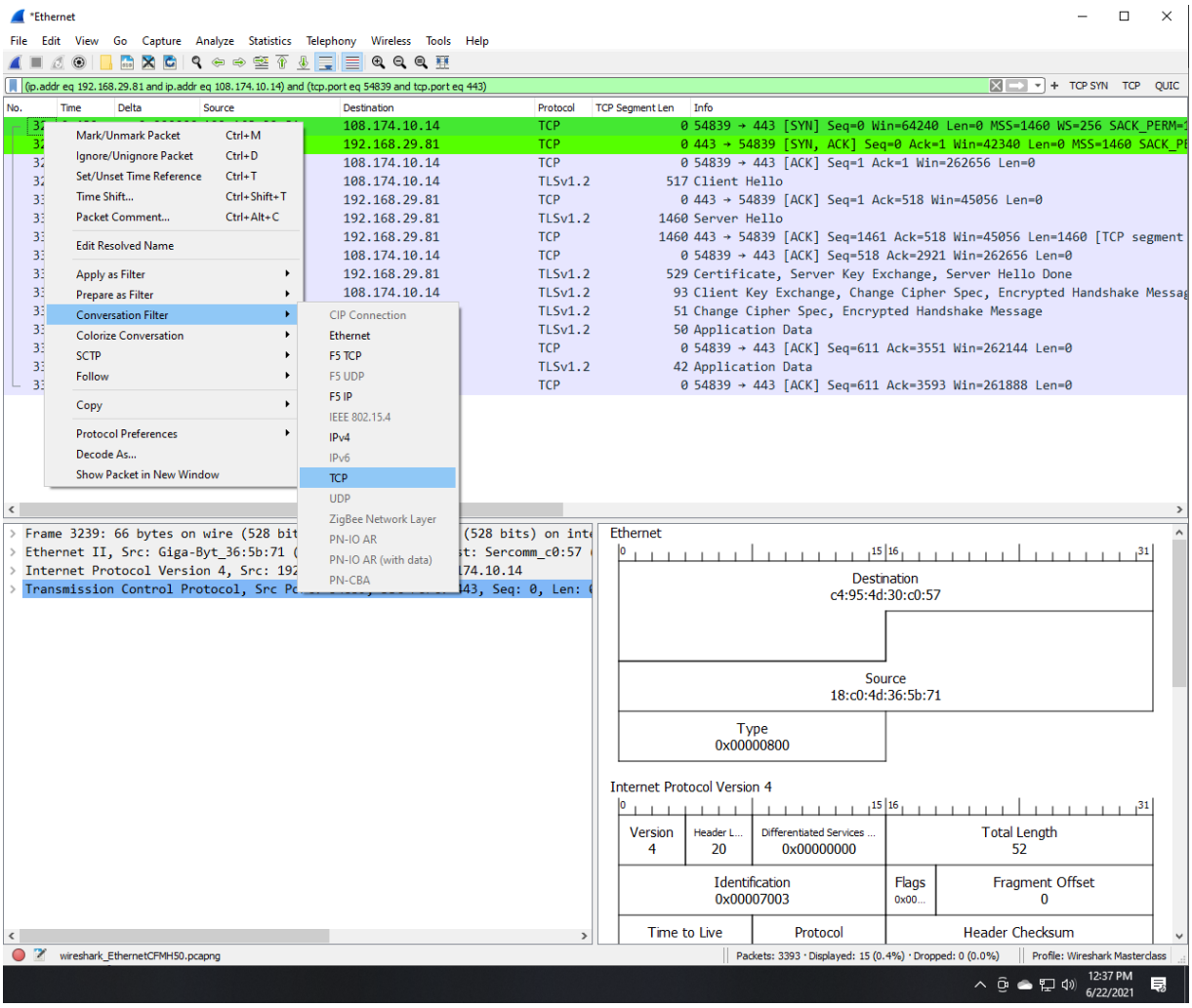
Index

1. The Handshake



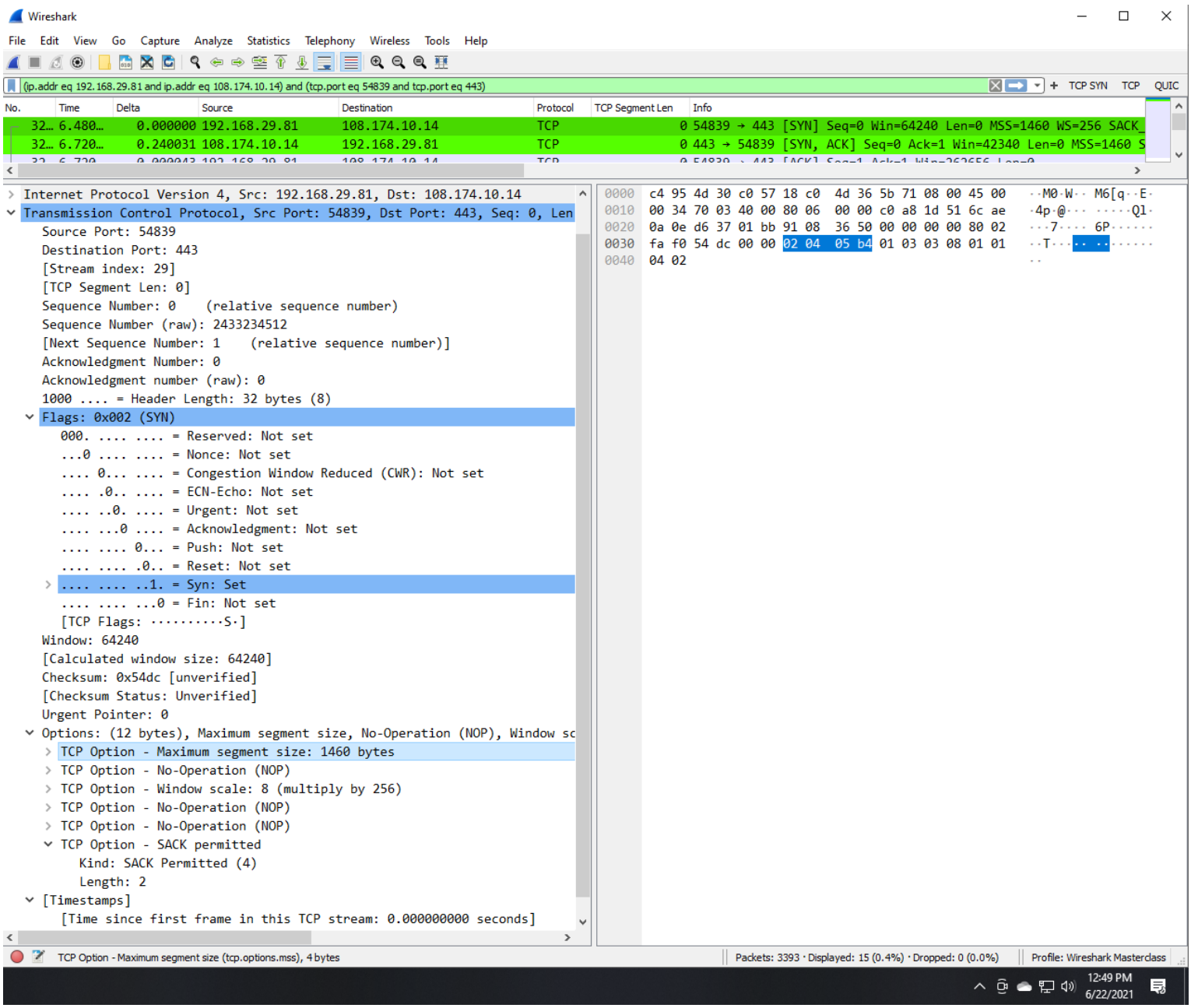
Three-way handshake wherein the client starts by sending a SYN (Synchronize) packet following which a series of acknowledgments are exchanged.

Filter out this handshake in Wireshark via a conversation filter:



Index

2. TCP SYN Packet Analysis in Wireshark:

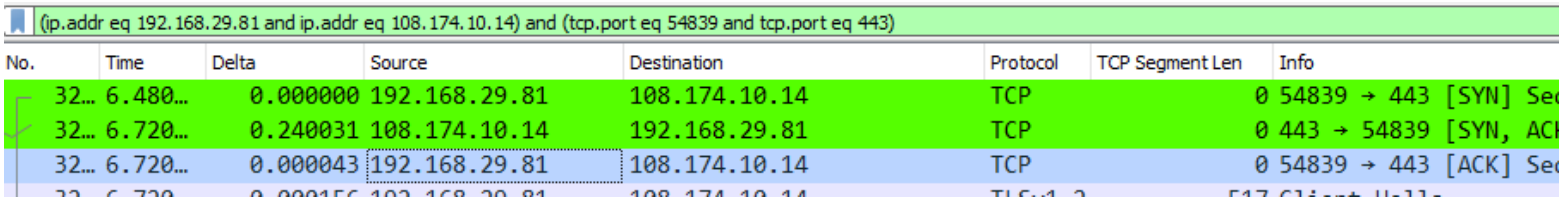


Highlight a SYN packet and expand its TCP segment in Wireshark to view the information exchanged in that packet:

1. Firstly, notice that the sequence number is 0. If you highlight this, you'll see that it's actually a large 4-byte number, but Wireshark is just setting it to 0 for this conversation to make it easy on us, the human observers. So, it's not actually 0, rather it's a complicated 4-byte number.
2. Next, notice that the packet length for this SYN packet is shown as 0, meaning there is no data sent. But the response SYN, ACK will act as if the set ACK flag is actually a byte, and the subsequent ACK from the client will acknowledge that so to speak. So, the SYN, ACK is a packet with no data either, but the ACK byte will be treated as a byte. This is therefore called a "ghost byte"! This allows the sequence number to get going with the client response ACK set to no. 1.

Index

3. Expand Flags to see what flags have been set:
    a. Only SYN is set to 1
    b. For the subsequent SYN, ACK both Acknowledgement and Syn flags will be set
    c. While the last ACK will have only Acknowledgement set
4. Click on a field to see its length. Notice it's mentioned below in the lower bar at the bottom-left of the page and the four hexadecimal digits are highlighted in the right pane, indicating four bytes for the Maximum Segment Size (MSS) fields
5. Window size:
    a. Controls the flow of data
    b. The field length is limited to 2 bytes, or a window size of 65,535 bytes. This is because:
        i. A byte has 8 bits
        ii. The max value for a byte is thus when all bits are set: 11111111
        iii. Since we're referring to Binary notation, this is evaluated as powers of 2:
        = 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0
        = 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1
        = 255
        iv. So, a single byte can represent values ranging from 0 – 255, for a total of 256 values
        v. Two bytes can therefore represent: 256x256 = 65,536 values
    c. Since the field size cannot be expanded, a window scaling factor was later introduced into the TCP protocol
    d. The scale value represents the number of bits to left-shift the 16-bit window size field and can be set from 0 (no shift) to 14.
    e. To calculate the true window size, multiply the size by 2^S where S is the scale value. For example, for a scale value of 3: 65535*2^3 = a true window size of 524280.
    f. In the Wireshark screenshot above, we see that the window size is 64240 and a scale factor of 8 is applied. This implies a scaling factor of 2^8 = 256 and Wireshark is even nice enough to directly tell us to multiply by 256! The true window size is thus: 16,445,440.
6. It's very important to capture the TCP handshake due to the above, as otherwise you wouldn't know what the scaling factor and thus what the window size actually is!
7. Expand TCP Options to see: Maximum Segment Size (MSS): You're telling the destination that this is the maximum number of bytes you can put in a TCP segment. Network infrastructure devices such as routers etc. could change this along the way!
8. TCP Segment vs TCP Packet: We say TCP segment is the protocol data unit which consists of a TCP header and an application data piece (packet) which comes from the (upper) Application Layer. Transport layer data is generally named as segment and network layer data unit is named as datagram but when we use UDP as transport layer protocol we don't say UDP segment, instead, we say UDP datagram.
9. Also within TCP Options is TCP SACK Permitted Option. This is basically telling your link partner whether you allow for Selective Acknowledgement (SACK) or not. More on this below.
10. The final handshake ACK from client to server will not contain TCP options.
11. Another great reason to capture the TCP handshake is that the Delta Time column will tell you the initial roundtrip time as the first SYN is set to Delta time 0:



Index

3. Selective Acknowledgements (SACK)

1. SACK is a refinement of TCP's traditional "cumulative" acknowledgements: In TCP's sliding-window scheme, the receiver *acknowledges* the data it receives, so that the sender can advance the window and send new data
2. As originally specified, these acknowledgements ("ACKs") are *cumulative*: the receiver tells the sender how much *consecutive* data it has received.
3. Multiple packet losses from a window of data can thus have a catastrophic effect on TCP throughput as this cumulative ACK strategy forces the sender to either wait for a roundtrip time to find out about each lost packet, or to unnecessarily retransmit segments which have already been correctly received
4. This in turn causes TCP to lose its ACK-based clock, reducing overall throughput
5. Selective Acknowledgment (SACK) is a strategy which corrects this behavior in the face of multiple dropped segments
6. With selective acknowledgments, the data receiver can inform the sender about all segments that have arrived successfully, so the sender need retransmit only the segments that have actually been lost
7. SACKs also allow a receiver to acknowledge non-consecutive data, so that the sender can retransmit only what is missing at the receiver's end

Wireless Scanners/Crackers

→ Analyzing the wireless side of your networks: Who is connected? What are they accessing? Is everything in conformance with your security plan?
→ Need to answer the above on a regular basis
→ Many tools available for this task:

Scanners:

- ♠ **Kismet**
- ♠ **NetStumbler**
- ♠ **MiniStumbler**

Scanners + Crackers:

- ♠ **AirSnort**
- ♠ **AirCrack**
- ♠ **CoWPAtty**

AirCrack-ng is a complete suite of wireless security assessment and exploitation tools that includes monitoring, attacking, testing, and cracking of wireless networks. This includes packet capture and export of the data collected as a text file or pcap file.

Index

Network Mapping and Flow Analysis

NetFlow

As defined in a NIST (National Institute of Standards and Technology) Special Publication: "A network flow is a particular communication session between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts."

Flow analysis is a very powerful technique to analyze network traffic, and one of the most ubiquitous examples of a flow analysis tool is **Cisco's NetFlow**, which groups traffic into flows.

Other standards include sFlow ("sampled Flow": conducts random packet sampling instead of separating traffic into flows to achieve scalability), echo and IPFIX (IP Flow Information Export), which has superseded NetFlow. IPFIX is based on NetFlow v9 and like NetFlow, groups traffic into flows and sends them to a centralized collection point.

Q: A company's NetFlow collection system can handle up to 2 Gbps. Due to excessive load, this has begun to approach full utilization at various times of the day. If the security team does not have additional money in their budget to purchase a more capable collector, which of the following options could they use to collect useful data?

A: Enable sampling of the data (NOT compression! It would save disk space but not aid with the bottleneck.)

The organization should enable sampling of the data collected. Sampling can help them capture network flows that could be useful without collecting everything passing through the sensor. This reduces the bottleneck of 2 Gbps and still provides useful information.

Quality of Service (QoS) is a set of technologies that work on a network to guarantee its ability to run high-priority applications and traffic dependably, but that does not help in this situation.

Index

Nmap: Network/Port Scanner

- These tools probe for open, filtered, and closed ports on networks & systems and hence detect machines & services on networks
- Can work on any network with any type of device (mobile, desktop, etc.) with any OS
- Very beneficial to have this tool in your toolbox and know how to use it well
- Can do the following:
  - ∑ ***Search for live hosts using ICMP, UDP or TCP packets:*** ICMPv4 is very popular but is blocked by default on many modern OSes so UDP & TCP are now more popular for this.
  - ∑ ***Search for any open ports, identifying them on a host, group of hosts or network:*** Scanning many ports over many systems can give you a very good idea of the services running on hosts. Scans can be done using default set of popular ports, many ports, or every possible port from 1 to 65535.
  - ∑ ***Search for specific ports such as mail servers etc.***
  - ∑ ***Identify/guess the services running on those ports.*** Example a service on port 80 is likely to be a HTTP web server (if standards have been followed).
  - ∑ ***Look for misc. TCP/UDP services.***
- As a cybersec professional, you will use this tool like an attacker: looking for open ports running services and decide if these open services should be running at all and if so, can their functionality be reduced in any way? Example: scan a network for systems accepting TCP traffic/connections over TCP port 1443 (MS SQL Server) to detect if someone installed something they shouldn't have!
- **PORT SCANNING IS LIKELY TO TRIGGER AN INCIDENT RESPONSE:** Ensure cyber-ops team is aware in advance on the timing and scope to prevent this.

∇ Workings:
- ∑ Depends heavily on the options selected
- ∑ Example: running a standard TCP scan against 192.168.1.20 for ports 1-1000
  - Scanner will attempt to establish a TCP connection to each port in that range on that IP
  - The scanner sends a SYN packet to each port and awaits the SYN/ACK response. The responses may be:
    - → If received, it'll attempt to complete the three-way handshake & mark the port as "Open"
    - → If the response times out or an RST packet is received, the port is marked as "Closed"
    - → If an "administratively prohibited" message or something similar is returned, that port is marked as "Filtered"
  - When the scan is complete, the scanner will present results in a summary format – listing the open, closed, and filtered ports and so on.
- ∑ Based on the scan results above, you can deduce some information about the scanned system(s):
  - **Open:** Ports accepting connections. You may be able to connect to these with a network scanner, in which case they're unfiltered, but they may also immediately drop your connections if you attempt to connect to them in some other manner. Example: SSH port

22 will appear open to a network scanner but will drop SSH connections. If this is the case, the service/port is likely filtered by a host-based firewall, or a firewall capability within the service.

- **Closed:** returns an RST packet.
- **Filtered:** Typically seen when an ICMP unreachable error is returned. Indicates filtering by a firewall or other device.
- **Additional types:** Some scanners will attempt to further classify responses such as dropped, blocked, denied, timeout, etc. Tool specific, refer to the tool's docs.

∇ Strategy:

∑ In general, you should run multiple scans with different options to ensure a better picture is obtained: A SYN scan may return a different result than a NULL scan or FIN scan.

∑ You'll want to run both TCP & UDP scans too.

∑ You may want to alter your scanning approach to use multiple techniques at different times of the day/night to ensure complete coverage.

∑ Port scans are also very useful for testing firewall configurations as the results highlight all open ports, all services etc.

∇ Defense against port scanners:

∑ Not easy! These scans are pretty much part of the internet traffic landscape now.

∑ You can block IP addresses that scan you, but most organizations don't as it runs the risk of an attacker spoofing source addresses as decoys for other scanning activity.

∑ The best defense is to carefully control what traffic you let in and out of your network via the use of firewalls, network filters and host filters and then carefully monitor the traffic that you do allow in!

♠ **Nmap aka Network Mapper**

Book Note:

"The previous two sections have described two of the most widely used and versatile tools, Wireshark and Nmap. Understanding what these tools can do and when and how they can be employed on your network covers a lot of testable areas of this objective."

Index

∇ Nmap Usage Notes:

OS Fingerprinting:

→ Nmap is pretty much the main tool for OS fingerprinting; most of the other tools actually use Nmap in the background!
→ Active vs Passive fingerprinting is a thing depending on whether packets are sent by the fingerprinting tool to illicit a response or is it simply listening for packets on the wire
→ The following techniques are used for OS fingerprinting:
- **IP TTL values**
  - The Time-To-Live value determines the max number of network hops before a packet dies; every OS will set a slightly different TTL value
- **IP ID values**
- **TCP window size**
- **TCP options** (typically TCP SYN & SYN/ACK packets)
- **DHCP requests**
  - Devices coming online broadcasts a DHCP request to every device requesting an IP address unless the appropriate device responds
  - These request broadcasts can contain a lot of valuable info
- **ICMP requests**
  - These are pings: Windows pings a little differently than other OSes
- **HTTP packets** (generally User-Agent field)
- **Running services**
  - Different devices/OSes may have different services running
- **Open port patterns**
  - Open ports can sometimes have banners, for example if you have an email system running and the banner says "Microsoft Exchange Server 2016" you can be pretty sure it's a Windows OS as that server is available only on Windows!
- **Many other techniques**
  - How many packets are sent, frequency and spacing between packets
  - How packets are retransmitted when errors occur
  - Actively sending packets and analyzing responses
  - Etcetera!

Rogue System Detection:

→ These are unauthorized systems falling outside an enterprise's umbrella, adding risk to a system
→ This is why the first elements of the top 20 sec controls consists of knowing the authorized software & hardware in your environment
→ Rogue system detection should be done on a regular basis
→ Can be done via a network scanner in two ways:
  ∇ Active network scans in order to detect unauthorized devices
  ∇ Passive scans via packet inspection to check for unauthorized communications

Index

Network Mapping Tools:

→ AKA network scanners
→ These tools create network diagrams of how machines are connected
→ Mapping tools stop there, but scanners further identify systems, services, and open ports etc.
→ By the above, network analyzers are also mappers but with more capabilities
→ Mapping tools can identify nodes on a network & sort them to OS, purpose, systems etc.

Q: Consider the following snippet from a log file collected on the host with the IP address of 10.10.3.6:

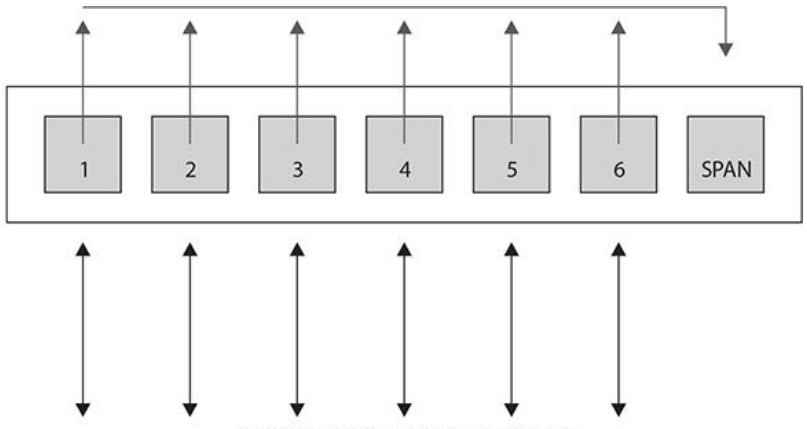
```
                                                    ©2022 Dion Training
  BEGIN LOG
 -------------
Time: Jun 12, 2020 09:24:12 Port:20 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Jun 12, 2020 09:24:14 Port:21 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Jun 12, 2020 09:24:16 Port:22 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Jun 12, 2020 09:24:18 Port:23 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Jun 12, 2020 09:24:20 Port:25 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Jun 12, 2020 09:24:22 Port:80 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Jun 12, 2020 09:24:24 Port:135 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Jun 12, 2020 09:24:26 Port:443 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Jun 12, 2020 09:24:26 Port:445 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP
-------------
  END LOG
```

What type of activity occurred based on the output above?

A: Port scan targeting 10.10.3.6

Switched Port Analyzer *(SPAN)*

→ AKA “Port Mirroring” or “Port Monitoring”
→ Usually specific to CISCO networks
→ Copy network traffic from one or more ports on a switch on one or more VLANs and forward it to a port designated for traffic capture & analysis



Traffic to and from Ports on a Switch

Index

Netcat

This simple utility reads and writes data across TCP or UDP network connections. It is designed to be a reliable back-end tool to use directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need, including port binding to accept incoming connections.

Its list of features includes port scanning, transferring files, and port listening: as with any server, it can be used as a backdoor.

The original Netcat's features include:

- Outbound or inbound connections, TCP or UDP, to or from any ports
- Full DNS forward/reverse checking, with appropriate warnings
- Ability to use any local source port
- Ability to use any locally configured network source address
- Built-in port-scanning capabilities, with randomization
- Built-in loose source-routing capability
- Can read command line arguments from standard input
- Slow-send mode, one line every N seconds
- Hex dump of transmitted and received data
- Optional ability to let another program service establish connections
- Optional telnet-options responder

Q: A penetration tester has issued the following command on a victimized host: nc -l -p 8080 | nc 192.168.1.76 443. What will occur based on this command?

A: Netcat will listen on port 8080 & output anything received to a remote connection on 192.168.1.76 port 443

Ncat

Though the original Netcat was released by Hobbit in 1995, but it hasn't been maintained despite its popularity. It can sometimes even be hard to find a copy of the v1.10 source code! The flexibility and usefulness of this tool prompted the Nmap Project to produce Ncat, a modern reimplementation which supports SSL, IPv6, SOCKS and http proxies, connection brokering, and more. Other takes on this classic tool include the amazingly versatile Socat, OpenBSD's nc, Cryptcat, Netcat6, pnetcat, SBD, & so-called GNU Netcat.

Ncat is a feature-packed networking utility which reads and writes data across networks from the command line. Ncat was written as a much-improved reimplementation of the venerable Netcat. It uses both TCP and UDP for communication and is designed to be a reliable back-end tool to instantly provide network connectivity to other applications and users. Ncat will not only work with IPv4 and IPv6 but provides the user with a virtually limitless number of potential uses.

Index

Password Crackers

→ Used by hackers to find weak passwords, so a sys admin should use one for the same reason!
→ Run your system's passwords through a cracker to verify their security level
→ They work using dictionary lists and brute force
→ With dictionary lists, they make passwords by combining words with each other, with numbers, special symbols, and test those against the system
→ They can also do brute force attacks
→ While they can be run online against a live system, they run the risk of being timed or locked out after several incorrect attempts
→ But if they can steal the password file, they can operate at maximum speed until a match is found: a modern (?) Corei7 will take about a month for a ten-character password

Cain and Abel

Cain and Abel (often abbreviated to Cain) is a popular password cracking tool. It can recover many password types using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force, and cryptanalysis attacks. It also includes a module to conduct Cisco VPN Client Password Decoding too.

Q: An attacker is searching in Google for Cisco VPN configuration files by using the filetype:pcf modifier. The attacker located several of these configuration files and now wants to decode any connectivity passwords that they might contain. What tool should the attacker use?

A: Cain and Abel

John the Ripper

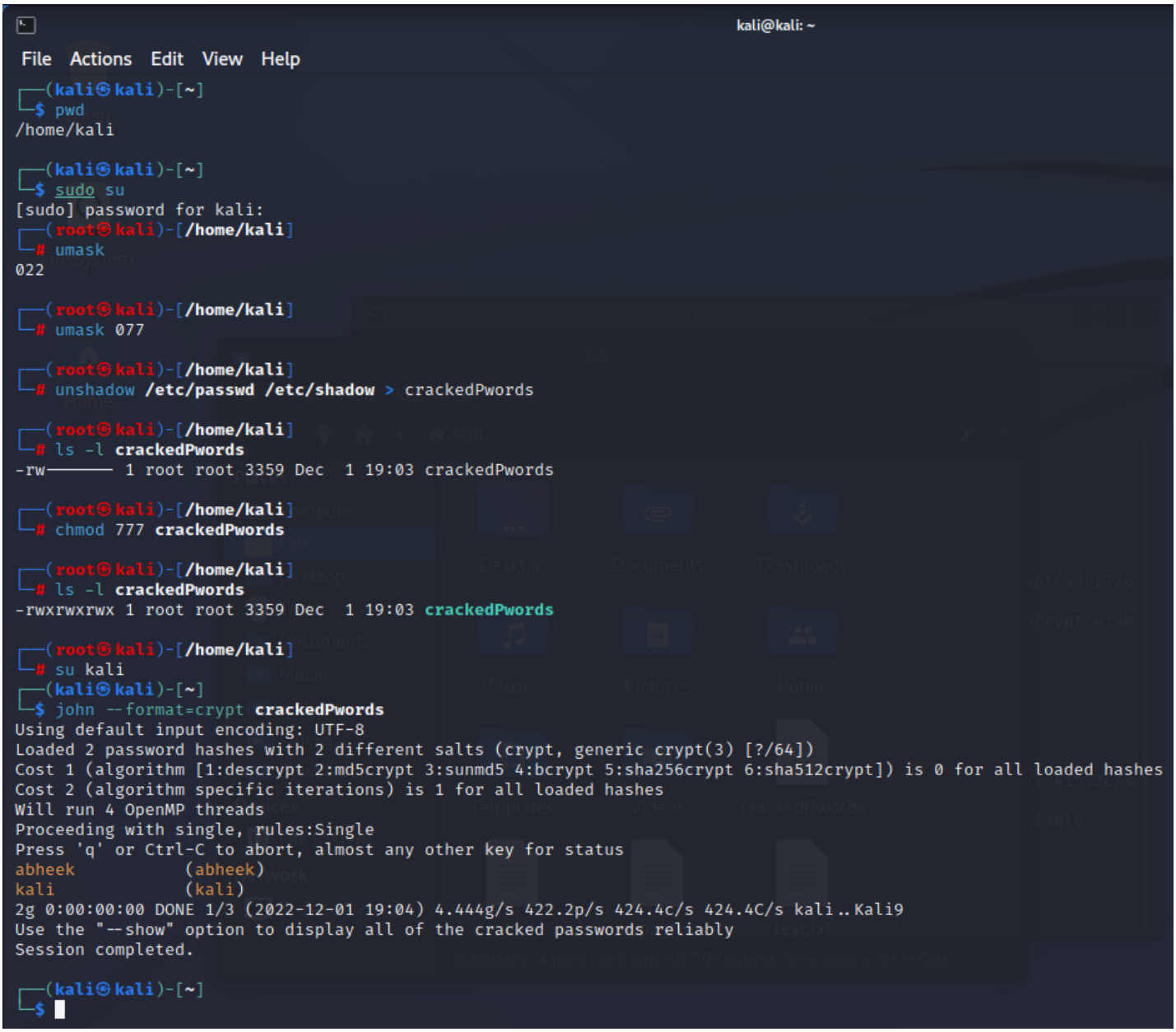
Quoting from https://www.openwall.com/john/:

"*John the Ripper is an Open-Source password security auditing and password recovery tool available for many operating systems. John the Ripper jumbo supports hundreds of hash and cipher types, including for: user passwords of Unix flavors (Linux, *BSD, Solaris, AIX, QNX, etc.), macOS, Windows, "web apps" (e.g., WordPress), groupware (e.g., Notes/Domino), and database servers (SQL, LDAP, etc.); network traffic captures (Windows network authentication, Wi-Fi WPA-PSK, etc.); encrypted private keys (SSH, GnuPG, cryptocurrency wallets, etc.), filesystems and disks (macOS .dmg files and "sparse bundles", Windows BitLocker, etc.), archives (ZIP, RAR, 7z), and document files (PDF, Microsoft Office's, etc.) These are just some of the examples - there are many more.*"

An easy way to start getting acquainted with this utility is to try and compromise your own Linux account credentials, stored in the /etc/passwd & /etc/shadow files (both these files are covered in detail later in these notes).

→ User credentials within these files in Kali are encrypted using yescrypt, as indicated by the y in /etc/shadow
→ Cracking this using JTR requires you to specify **--format=crypt** during executing the 'john' command
→ Prior to this, the unshadow utility (shipped with JTR) must be leveraged to generate a file that's a combination of information in the /etc/passwd & /etc/shadow files
→ As the above is done as root, make the generated file accessible to other users via **chmod**
→ To force JTR to crack the same hashes again, delete the **~/.john/john.pot** file

Index



Example: Cracking User Credentials in Kali

*Delete the **~/.john/john.pot** file to force JTR to crack the same hashes again:*

Index

Vulnerability Scanners

→ These are programs that probe a system for weaknesses, misconfigurations, old versions of software and so on

→ Essentially three main categories of vulnerability scanners: Network, Host & Application

∇ **Network Vulnerability Scanners:**

- ∑ They probe a host or hosts for issues across their network connections
- ∑ Typically, these tools will also contain or use a port scanner to perform an initial assessment of the network to determine which hosts are alive and present, and which services are open on them
- ∑ It then probes each service
- ∑ They are very broad tools and can potentially run thousands of checks, depending on the OS & services being examined
- ∑ This makes them a very good "broad sweep" for network-visible vulnerabilities
- ∑ They can generate a large amount of traffic and connections to the systems being probed due to the number of checks they perform
- ∑ Hence, you should take care to minimize the impact on production systems & networks
- ∑ These tools are essentially the **equivalent of a Swiss army knife for assessments**: they do a lot of tasks and are extremely useful to have around, but they may not be as good as a tool dedicated to examining one specific service type
- ∑ **However, if you can only run one tool to examine your network for vulnerabilities, you'll want that tool to be a network vulnerability scanner!**
- ∑ Bottom line: If you need to perform a broad sweep for vulnerabilities on one or more hosts across your network, a network vulnerability scanner is the right tool for the job

♠ **Nessus from Tenable Network Security:** Nessus is a very popular vulnerability scanner. It can be used to check how vulnerable your network is by using various plugins to test for vulnerabilities. Also, Nessus can perform compliance auditing, like internal and external PCI-DSS audit scans.

∇ **Host Vulnerability Scanners**

- ∑ These tools are designed to run on a specific host and look for vulnerabilities & misconfigurations on that host
- ∑ They're more specialized than network vulnerability scanners as they're looking for issues associated with a specific OS or set of operating systems

♠ **Microsoft Baseline Security Analyzer (MSBA):**

- ∑ MSBA is designed to examine the security state of a Windows host & offer guidance to address any vulnerabilities, misconfigurations, or missing patches
- ∑ It can be run against remote systems across the network

Index

- ∑ But is typically meant to run on the host being examined and requires local, administrator access to that host
- ∑ If you want to scan a specific host for vulnerabilities, weak password policies, or unchanged passwords and have direct access to that host, a host vulnerability scanner is often the right tool for the job

♠ Tools such as Nessus blur the line between network and host vulnerability scanners: if you supply Nessus with host, login & domain credentials, it can perform many checks that would be considered "host based"

→ ***It's worth noting that to do a thorough job, you'll likely need both network-based & host-based scanners – particularly for critical assets***

→ ***Both types of scanners perform different tests and provide visibility into different types of vulnerabilities so if you want to ensure the best possible coverage, you'll need to run both!***

∇ **Application Vulnerability Scanners**

- ∑ These tools are designed to look for vulnerabilities in applications or certain types of applications
- ∑ As a result, these are some of the most specialized scanners
- ∑ Even though they contain hundreds, even thousands, of checks, they only look for misconfigurations or vulnerabilities in a specific type of application
- ∑ Some may even be scanners for web-based applications, and these are arguably the most popular type of application vulnerability scanners
- ∑ This is because the very nature of web applications makes them very lucrative targets for attackers – they're designed to be visible, interact with users and accept and process user input
- ∑ As a result of this, a relatively large number of web application scanners are available, ranging from open source to subscription based
- ∑ Tools effective in this domain must be able to perform thousands of checks for vulnerabilities, misconfigurations, default content, settings, issues, etc.
- ∑ They must be able to do this with a wide variety of web technologies from IIS to Apache to PHP to ASP to everything else in between
- ∑ They are usually capable of performing advanced checks, such as for SQL or JavaScript injection attacks, that require interacting with the web application being examined & modifying requests & responses based on feedback from the application
- ∑ If you want to examine a specific application or multiple instances of the application (such as a website), then an application vulnerability scanner is the tool of choice

♠ **Acunetix WVS (Web Vulnerability Scanner) - for Web Tech**

→ ***Selecting the right type of vulnerability scanner isn't that difficult: just focus on what types of vulnerabilities you need to scan for and how you will be accessing the host, services or applications being scanned.***

Index

Configuration Compliance Scanners

- → The need to automate configuration checks has existed for years and has become important enough that a standard format has been developed: SCAP - Security Content Automation Protocol
- → This is a protocol to manage information related to security configurations and their automated validation
- → There are in turn a wide variety of configuration compliance scanners that can perform this task
- → Some of these are SCAP compliant while some are not, but they all have the same intended purpose: informing sys admins whether or not their systems align with their defined requirements
- → The use of these tools requires that a baseline set of defined configurations is established and then these tools can track changes as this defined baseline itself changes
- → In most cases, these tools themselves can be used to set a baseline upon first operation and set to measure any deviations from this baseline

Exploitation Frameworks

- → Toolsets designed to assist hackers in the tasks associated with exploiting vulnerabilities in a system
- → There frameworks are important as the exploitation path typically consists of multiple steps, all carried out in a precise order against a system

    - ♠ **Metasploit**
    - ♠ **Browser Exploitation Framework (BeEF)** is a pentesting tool that focuses on the web browser

- → Metasploit is the most popular framework here: It's a set of tools designed to assist a pentester in carrying out the steps needed to exploit a vulnerability in a system
- → These frameworks can be used by security personnel as well, specifically to test the exploitability of a system based on existing vulnerabilities and employed security controls

Data Sanitization Tools

- → These tools are used to destroy, purge, or otherwise identify for destruction specific types of data on systems
- → You need to do the above before a system is retired or disposed-off
- → Several approaches:
    - ∇ Whole disk approach: you can use data sanitization tools to erase or wipe the entire storage, making any information on it inaccessible. One method of doing this is to use self-encrypting disks, with the destruction of the key rendering the disk unrecoverable
    - ∇ Targeted approach: identify sensitive data & deal with it specifically

    - ♠ **Identity Finder**

- → Tools such as Identity Finder excel at all aspects of data sanitization
- → However, as with any & all tools, it's not just the tool itself that provides value, but rather the processes & procedures that ensure work is done & done correctly when required

Index

Steganography Tools

→ Steganography is the science of hidden writing, more specifically the hiding of messages in other content
→ Historically, this has been done by painting over messages, and later removing the cover paint, and by other methods as well
→ Because of the nature of digital images, video and audio files and sufficient encoding capacity in streams, it's possible to embed additional content in files
→ If such hidden content is invisible to the typical user, then it's considered to be steganography
→ The same techniques are used to add watermarks, visible or otherwise, to files so that their lineage can be traced
→ Such watermarks are used to trace documents or serialize copies so a firm can tell who's leaked critical information

Honeypot

→ A honeypot is a server that's designed to act like the real server on a corporate network, but possesses fake data
→ Such servers serve to attract attackers, thus serving as a trap as any traffic to the honeypot can be assumed to be malicious
→ A honeynet is a network designed to look like a corporate network, and is thus a collection of honeypots
→ It looks like the corporate network, but is a false copy and all traffic within it is assumed to be illegitimate
→ This makes it easy to characterize the attacker's traffic and identify where the attacks are coming from

Forensic Disk Imaging

→ Disk Imaging is **the process of copying a hard drive as a backup copy or an archive**. The process entails copying all the data stored on the source drive, including data like the master boot record and table allocation information
→ Generally, there are three primary types of forensic image collection techniques: 1) creating a physical forensic image i.e. a bit-by-bit copy of the device, capturing deleted and encrypted files & data 2) collecting a logical image capturing all user-visible data; or 3) doing a targeted collection of device data for specific files or folders relevant to a legal matter
→ The first thing that must be done after acquiring a forensic disk image is to create a hash digest of the source drive and destination image file to ensure they match. A critical step in the presentation of evidence will be to prove that analysis has been performed on an identical image to the data present

Index

on the physical media and that neither data set has been tampered with. When comparing hash values, you need to use the same algorithm used to create the reference value.

→ Digitally signing the image file could serve the function of non-repudiation, but it is an uncommon practice and not required to be performed.

- ♠ **FTK Imager**: can create perfect copies or forensic images of computer data without making changes to the original evidence. The forensic image is identical in every way to the original, including copying the slack, unallocated, and free space on a given drive
- ♠ The **dd tool** can also create forensic images, but it is not a proprietary tool since it is open-source
- ♠ **Autopsy** is a cross-platform, open-source forensic tool suite

Passive Vs Active Tools

→ Tools may be passive or active:

- ∇ *Passive tools* are those that do not interact with the system in a manner that would permit their detection, for example by sending packets or altering traffic. They instead use existing traffic to provide data for analysis.
  - ♠ **Tripwire – can detect changes to a file based on hash values**
  - ♠ **Wireshark – performs passive activities such as packet inspection and even OS mapping by analyzing TCP/IP traces**
- ∇ *Active tools* interact with the system in a manner that their use can be detected
  - ♠ **Nmap – maybe not the tool itself but it's use, which results in the sending of packets, can be detected**

→ When determining whether to use an active or a passive tool, attackers may consider how much time they have on hand to carry out the attack

→ Given plenty of time, they'll likely choose a passive toolset to sneak around undetected

→ But passive tools do have some limitation: they can only detect systems based on their behavior in a network, and their collection point must be on the path between the source & destination for conversations being examined

→ An active tool on the other hand can use the network to carry its interrogatory packets to a host & back, eliminating the location issue to a large degree, at the cost of alerting the system being interrogated!

→ In summary, passive tools only receive traffic and do nothing to the traffic flow that would permit their detection. Active tools modify and/or send traffic & are thus discoverable by their traffic patterns

Banner Grabbing

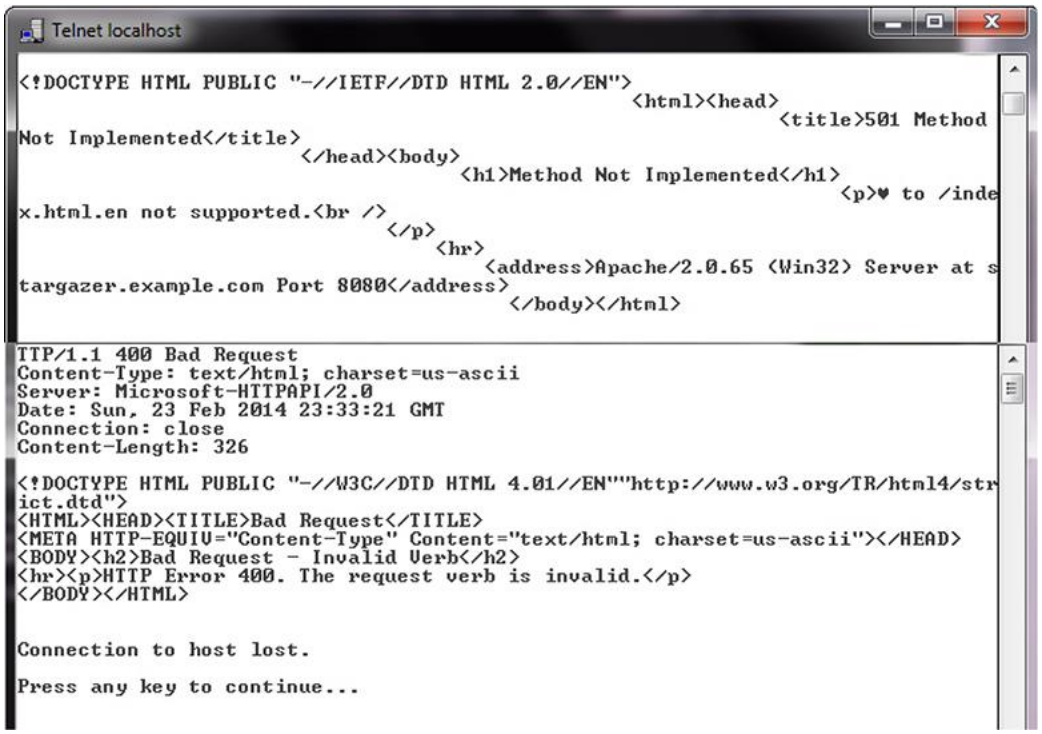
→ A technique used to gather information from a service that publicizes information via a banner

→ Banners are used for many things: they can be used to identify services by type, version, etc. & they enable administrators to post information, including warnings, to users when they log-in

Index

→ Such banners can be used to determine what services are running
→ Typically used against common banner-issuing services such as HTTP, FTP, SMTP, and Telnet

♠ ***The figure below shows a couple of banner grabs being performed from a Telnet client against a web server. In this example, Telnet sends information to two different web servers and displays the responses (the banners). The top response is from an Apache instance (Apache/2.0.65) and the bottom is from Microsoft IIS (Microsoft-HTTPAPI/2.0):***



→ An organization, wishing to raise the bar for attackers, can change the information in the banners to be less specific, masking the true revision etc. and in some cases, even the actual type of service
→ This will only serve to slow down an adversary, but each element that forces more attempts is in the defenders' interests as it provides additional time to catch an attacker!

Q: You have been asked to determine if Dion Training's web server is vulnerable to a recently discovered attack on an older version of SSH. Which technique should you use to determine the current version of SSH running on their web server?

A: Banner Grabbing

Banner grabbing is conducted by actively connecting to the server using telnet or netcat and collecting the web server's response. This banner usually contains the server's operating system and the version number of the service (SSH) being run. This is the fastest and easiest way to determine the SSH version being run on this web server. While it is possible to use a vulnerability scanner, protocol analyzer, or to conduct a passive scan to determine the SSH version, these are more time-consuming and not fully accurate methods to determine the version being run.

Index

Command Line Tools

Tracert (Traceroute) is a command-line utility used to **trace an IP packet's path** as it moves from its source to its destination. While using ping will tell you if the remote website is reachable or not, it will not tell you where the connection is broken. Tracert performs a **series of ICMP echo requests** to determine which device in the connection path is not responding appropriately. This will help to identify if the connectivity issue lies within your intranet or is a problem with the ISP's connection. It's thus a diagnostic utility that determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. **While 'tracert' is the Windows command, 'Traceroute' is used for Unix, Linux, and OS X.**

route: The route command is used to create, view, or modify manual entries in the network routing tables of a computer or server. **Think Static Routing.**

nslookup: The nslookup tool is used for DNS queries & troubleshooting. To lookup a specific type of DNS server, use the "***set type=<>***" command. Ex: ***set type=ns*** for name servers, or ***set type=mx*** for mail servers.

netstat: The netstat tool is used to display **network statistics** & active connections (NO DIAGNOSTIC). It's used to monitor incoming & outgoing connections, routing tables, port states & usage statistics on an interface.

nbtstat: Displays NetBIOS over TCP/IP **(NBT) protocol statistics**, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. This command also allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Used without parameters, this command displays Help information. This command is available only if the Internet Protocol (TCP/IP) stack is installed as a component in the properties of a network adapter in Network Connections.

ping: The ping tool is used to test an end-to-end connection, but will not provide any data on the hops found in the connection.

Hping is a handy little utility that assembles and sends custom ICMP, UDP, or TCP packets and then displays any replies. It was inspired by the ping command but offered far more control over the probes sent. It also has a handy traceroute mode and supports IP fragmentation. Hping is particularly useful when trying to traceroute/ping/probe hosts behind a firewall that blocks attempts using the standard utilities. Hping also allows you to map out firewall rule sets. It is also great for learning more about TCP/IP and experimenting with IP protocols. Hping does not support IPv6, though, so the NMAP creators have created Nping to fill this gap and serve as an updated variant of Hping.

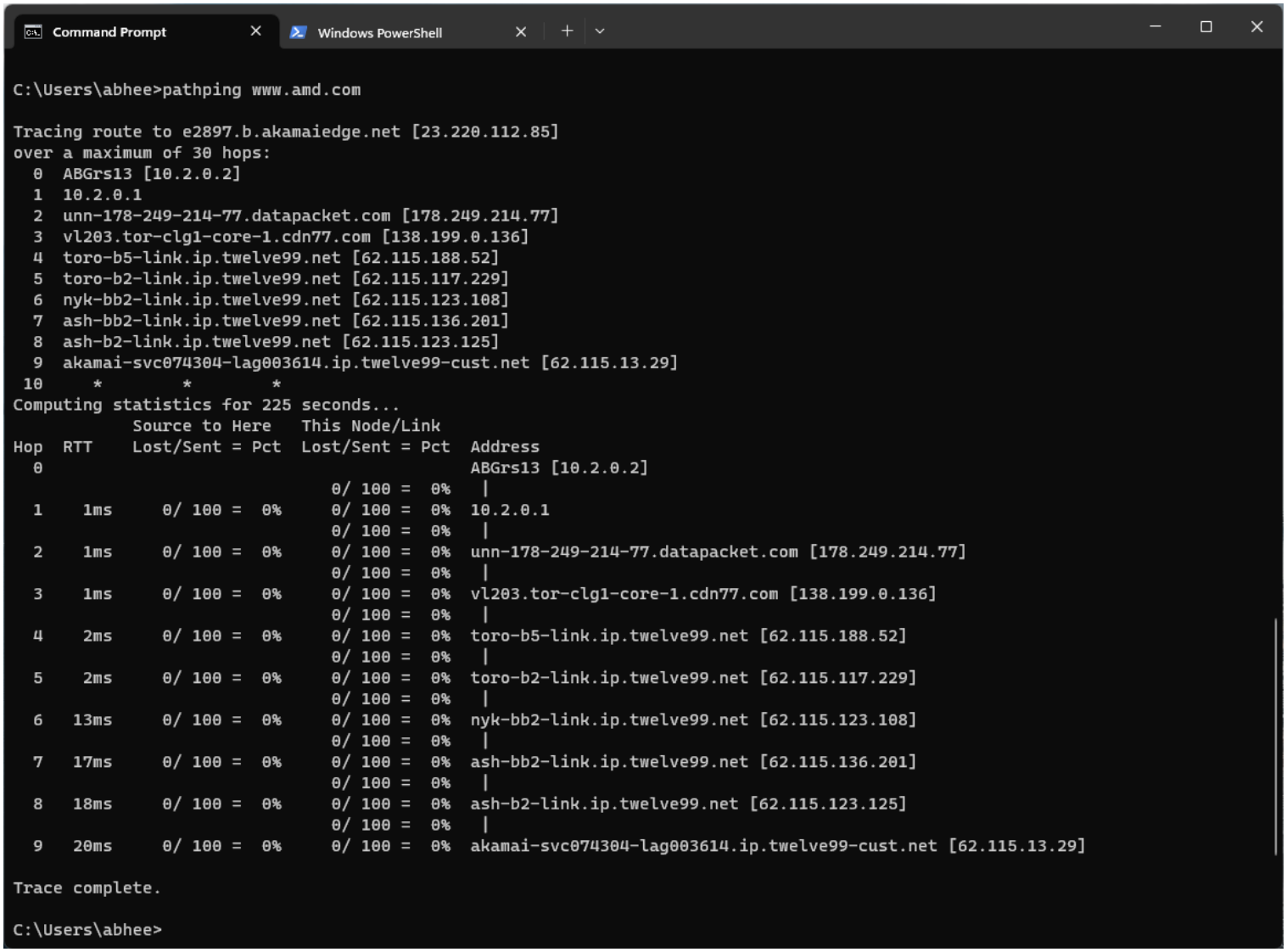
Ptunnel is an application that allows you to reliably tunnel TCP connections to a remote host using ICMP echo request & response packets, commonly known as ping requests and replies. Ptunnel is used as a covert channel, not to elicit a response from a host using TCP.

The net use command is used to connect to, remove, and configure **connections to shared network resources** such as mapped drives and network printers. For example, "net use S: \\SERVER\DATA /persistent:yes" would map the DATA folder on the SERVER to your local S:\ drive on a Windows computer.

The tcpdump tool is a text-based packet capture and analysis tool that can capture packets and display the contents of a packet capture (pcap) file. While you may be able to identify the services, applications, or operating systems using tcpdump by analyzing the captured packets, tcpdump will not send specifically crafted packets to the devices as it is a passive reconnaissance tool.

Index

The PathPing command is a Windows command-line tool that is used to locate spots that have network latency & network loss between a client & destination. The advantages of PathPing over ping & traceroute are that each node is pinged via a single command & that the behavior of nodes is **studied over an extended period, rather than the default ping sample of four messages or default traceroute single route trace.**



PathPing Output on Windows 11

arp: The arp command is used to view and modify the local Address Resolution Protocol (ARP) cache of a device, which contains recently resolved MAC addresses of IP hosts on the network.

telnet: The telnet command is used to open a command-line interface on a remote computer or server. Telnet operates in plain text mode and should never be used over an untrusted or public network.

A NetFlow Analyzer is used to perform monitoring, troubleshooting, inspection, interpretation, and synthesis of network traffic flow data. A NetFlow analyzer can help you quickly identify traffic patterns and the different applications/protocols in use on the network.

A Spectrum Analyzer is used to measure the magnitude of an input signal's frequency.

Index

A Terminal Emulator is used by a network administrator to make a given computer appear like an actual terminal or client computer networked to a server or mainframe.

An IP Scanner is used to monitor a network's IP address space in real-time and identify any devices connected to the network. Essentially, the tool will send a ping to every IP on the network and then creates a report of which IP addresses sent a response.

A Port Scanner is used to determine which ports and services are open and available for communication on a **target system**.

A Protocol Analyzer is used to capture, monitor, and analyze data transmitted over a communication channel.

Nmap, or Network Mapper, is a cross-platform, open-source tool used to scan IP addresses and ports on a target network, and to detect running services, applications, or operating systems on that network's clients, servers, and devices.

The iPerf tool is used to create TCP and UDP data streams and measure the throughput of a given network. The iPerf tool is well suited to **testing the throughput of the new switches** and its results can be used to create the new network performance baseline.

Q: Dion Training's remote office is experiencing poor network performance. You have been asked to look at the traffic patterns for the remote office and compare them to the network performance baselines. Which of the following tools should you utilize?

A: NetFlow Analyzer

Q: You are currently troubleshooting a workstation in the office and determined that it is an issue with the cabling somewhere between the workstation and the switch. You have tested the patch cable from the workstation to the wall jack and it is not faulty. You want to check the port on the switch next. Which of the following would BEST help you identify which switch port is associated with the workstation's wall jack?

A: Proper labeling!

You should always use proper labeling of your cables, wall jacks, and patch panels to make it easy to locate which switchport is associated with each portion of the cable distribution plant. Ensuring everything is properly labeled will help when you need to troubleshoot a network connection in your interior cable distribution plant.

Q: Eduardo, a network technician, needs to protect IP-based servers in the network DMZ from an intruder trying to discover them. What should the network technician do to protect the DMZ from ping sweeps?

A: Block all ICMP Traffic to and from the DMZ

Ping sweeps are conducted using ICMP by default, not UDP, therefore disabling UDP on the servers will not stop a ping sweep.!

Index

Q: Which of the following tools allows you to view and modify the layer 2 to layer 3 address bindings?

A: arp

Q: Dion Training has configured a new web server and connected it to their screened subnet. A network technician wants to ensure the server is properly hardened and that it only allows inbound HTTPS requests while blocking any HTTP requests. Which of the following tools should the technician utilize?

A: Port Scanner

A port scanner is used to determine which ports and services are open and available for communication on a target system. The port scanner will scan the server and display any open ports. If the technician finds that port 443 (HTTPS) is open and all other ports are closed, then they know the server has been properly hardened.

Index

Legal Lemming

A legal hold is a process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated. If a legal hold notice has been given to the backup service, **they will not destroy the old backup tapes until the hold is lifted.**

The process of discovery is the formal process of exchanging information between the parties about the witnesses and evidence they will present at trial.

The chain of custody is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. It documents all changes in the control, handling, possession, ownership, or custody of a piece of evidence. The chain of custody is an important part of documenting the evidence collected during an incident response and should include any individual who worked with evidence during an investigation.

A data transport request is a formalized request to initiate a data transfer by establishing a circuit or connection between two networks.

eDiscovery is the term that refers to the process of evidence collection through digital forensics. eDiscovery is conducted during an incident response.

Q: When a criminal or government investigation is underway, what describes the identification, recovery, or exchange of electronic information relevant to that investigation?

A: eDiscovery

Separation of Duties is the concept of having more than one person required to complete a particular task to prevent fraud and error.

Dual Control, instead, requires both people to act together. For example, a nuclear missile system uses dual control & requires two people to each turn a different key simultaneously to launch a missile.

Mandatory Vacation Policies require employees to take time away from their job and help to detect fraud or malicious activities. Even if other controls such as separation of duties, least privilege & dual control are used, an employee could collude with others to conduct fraud. By utilizing mandatory vacation policies, this fraud can often be discovered since a new person will be conducting the duties assigned to the person on vacation.

A Background Check is a process a person or company uses to verify that a person is who they claim to be and provides an opportunity to check a person's criminal record, education, employment history, and other past activities to confirm their validity.

Index

Forensic Investigation

As a forensic investigator, **you should always 'secure the area' before taking any other actions**. This includes ensuring that no other people are in the area to disrupt your forensic collection (such as the suspect or their accomplices), ensuring the workstation isn't unplugged from the network or the power, and other actions to prevent the evidence from being tampered with. **Once the area is secure, then you should document the scene, begin your evidence collection, and implement the chain of custody.**

Data Classification

Protected Health Information (PHI) refers to medical and insurance records, plus associated hospital & laboratory test results. Data collected by genetic mapping and heredity companies include the subject's DNA, making it PHI.

Personally Identifiable Information (PII) is data that can be used to identify, contact, or locate an individual. Information such as social security number (SSN), name, date of birth, email address, telephone number, street address, and biometric data is considered PII.

Sensitive Personal Information (SPI) is information about a subject's opinions, beliefs, and nature afforded specially protected status by privacy legislation. As it cannot be used to identify somebody or make any relevant assertions about health uniquely, it is neither PII nor PHI. According to the GDPR, information about an individual's race or ethnic origin is classified as SPI.

Intellectual Property (IP) or Proprietary Information is information created and owned by the company, typically about the products or services that they make or perform.

Controlled Unclassified Information (CUI) is federal non-classified information that must be safeguarded by implementing a uniform set of requirements and information security controls to secure sensitive government information.

Digital Rights Management (DRM) is a copyright protection technology for digital media and usually tries to restrict the number of devices allowed for playback of a licensed digital file, such as a music track or eBook.

The Digital Millennium Copyright Act (DMCA) is a 1998 United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization that criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works.

The General Data Protection Regulation (GDPR) is a regulation created in the European Union that creates provisions and requirements to **protect the personal data of European Union (EU) citizens**. Transfers of personal data outside the EU Single Market are restricted unless protected by like-for-like regulations, such as the US's Privacy Shield requirements. Further, personal data collected can only be used for the exact purpose in which explicit consent was obtained. For example, to use email addresses for marketing purposes.

The Payment Card Industry Data Security Standard (PCI-DSS) applies to companies of any size that accept credit card payments. If your company intends to accept card payment and store, process, and transmit cardholder data, you need to securely host your data and follow PCI compliance requirements.

Index

Q: Your organization is updating its incident response communications plan. A business analyst in the working group recommends that if the company discovers they are the victims of a data breach, they should only notify the affected parties to minimize media attention and bad publicity. Which of the following recommendations do you provide in response to the business analyst's statement?

A: Guidance from laws and regulations should be considered when deciding who must be notified to avoid fines and judgments from non-compliance

The requirements for different types of data breaches are set out in laws/regulations. The requirements indicate who must be notified. Other than the regulator itself, this could include law enforcement, individuals and third-party companies affected by the breach, and public notification through the press or social media channels. For example, the Health Insurance Portability and Accountability Act (HIPAA) sets out reporting requirements in legislation, requiring breach notification to the affected individuals, the Secretary of the US Department of Health & Human Services, and, if more than 500 individuals are affected, to the media.

Q: Your company is required to remain compliant with PCI-DSS due to the type of information processed by your systems. If there was a breach of this data, which type of disclosure would you be required to provide during your incident response efforts?

A: Notification to Visa and Mastercard!!

Very weird because you'd think this would be wrong on the simple basis that it does not include all the credit card providers such as Discover, Diners Club etc! However, apparently, it would seem, as per the exam, that "Any organization that processes a credit card is required to work with Visa and Mastercard to report a data breach. After a data breach, you should notify payment card brands (Visa and Mastercard), acquirers (merchant banks), and any other entities that may require notification, whether by contract or law. Conducting notification to your payment card brand and merchant banks is one of the first steps in the incident response process for this type of data breach" and typically, law enforcement does not have to be notified of a data breach at a commercial organization! However laws do generally require that customers be notified of data breaches within 72 hours!

Q: During an assessment of the POS terminals that accept credit cards, a cybersecurity analyst notices a recent Windows operating system vulnerability exists on every terminal. Since these systems are all embedded and require a manufacturer update, the analyst cannot install Microsoft's regular patch. Which of the following options would be best to ensure the system remains protected and are compliant with the rules outlined by the PCI DSS?

A: Identify, implement & document compensating controls (NOT remove the POS terminals!)

The analyst will likely not remove the terminals from the network without affecting business operations, so this is a bad option!

Index

Data Protection: Tokenization, Masking, Minimization & Anonymization

Tokenization means that all or part of data in a field is replaced with a randomly generated token or number that's used to reference the original value stored in another vault or database. The token is stored with the original value on a token server or token vault, separate from the production database. An authorized query or app can retrieve the original value from the vault, if necessary, so **tokenization is a reversible technique.**

Data Masking can mean that all or part of a field's contents are redacted, by substituting all character strings with x, for example.

Data Minimization involves limiting data collection to only what is required to fulfill a specific purpose. Reducing what information is collected reduces the amount and type of information that must be protected.

Data Anonymization is the process of removing personally identifiable information from data sets so that the people whom the data describe remain anonymous.

Q: A cybersecurity analyst is working for a university that is conducting a big data medical research project. The analyst is concerned about the possibility of an inadvertent release of PHI data. Which of the following strategies should be used to prevent this?

A: Conduct tokenization of the PHI data before ingesting it into the big data application

In a tokenization approach, all, or part of the data in a field is replaced with a randomly generated token. That token is then stored with the original value on a token server or token vault, separate from the production database. This is an example of a deidentification control and should be used since the personally identifiable medical data does not need to be retained after ingesting it for the research project; only the medical data itself is needed.

While using DevSecOps can improve the overall security posture of the applications being developed in this project, it does not explicitly define a solution to prevent this specific issue making it a less ideal answer choice for the exam.

Formal verification methods can be used to prove that none of the AI/ML techniques that process the PHI data could inadvertently leak. Still, the cost and time associated with using these methods make them inappropriate for a system used to conduct research. A formal method uses a mathematical model of a system's inputs and outputs to prove that the system works as specified in all cases. It is difficult for manual analysis and testing to capture every possible use case scenario in a sufficiently complex system. Formal methods are mostly used with critical systems such as aircraft flight control systems, self-driving car software, and nuclear reactors, not big data research projects.

The option provided that recommends utilizing a SaaS model is not realistic. There is unlikely to be a SaaS provider with a product suited to the big data research being done. SaaS products tend to be commoditized software products that are hosted in the cloud. The idea of migrating to a SaaS is a distractor on this exam, which is trying to get you to think about shifting the responsibility for the PHI to the service provider and away from the university, but due to the research nature of the project, this is unlikely to be a valid option in the real world and may not be legally allowed due to the PHI being processed.

Index

Regulations & Acts

The Family Educational Rights and Privacy Act (FERPA) requires that **educational** institutions implement security and privacy controls for student educational records.

The Gramm-Leach-Bliley Act (GLBA) institutes requirements that help protect the **privacy of an individual's financial information held by financial institutions & others,** such as tax preparation companies. The privacy standards & rules created as part of GLBA safeguard private information & set penalties in the event of a violation.

The Sarbanes-Oxley Act (SOX) dictates requirements for storing and retaining documents relating to an **organization's financial and business operations**, including the type of documents to be stored and their retention periods. It is relevant for any publicly-traded company with a market value of at least $75 million. SOX is thus a United States federal law that sets new or expanded requirements for all U.S. public company boards, management, and public accounting firms.

The Health Insurance Portability and Accountability Act (HIPAA) establishes several rules and regulations regarding **healthcare in the United States**. With the rise of electronic medical records, HIPAA standards have been implemented to protect patient medical information privacy through restricted access to medical records and regulations for sharing medical records. It's thus a United States federal law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers.

The Federal Information Security Management Act (FISMA) is a United States federal law that defines a **comprehensive framework to protect government information**, operations, and assets against natural or human-made threats. FISMA requires that government agencies and other organizations that operate systems on behalf of government agencies comply with security standards.

The Children's Online Privacy Protection Act (COPPA) is a United States federal law that imposes certain requirements on operators of websites or online services directed to **children under 13 years of age** and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

The Trusted Foundry Program, also called the trusted supplier's program, is a United States Department of Defense program designed to secure the manufacturing infrastructure for information technology vendors providing hardware to the military. Trusted Foundry was created to provide a chain of custody for classified/unclassified integrated circuits, ensure there is no reasonable threat related to supply disruption, prevent intentional/unintentional modification of integrated circuits, and protect integrated circuits from reverse engineering and vulnerability testing.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) guides governance-related topics, including fraud, controls, finance & ethics. COSO's ERM-integrated framework defines risk & related common terminology lists key components of risk management strategies and supplies direction and criteria for enhancing risk management practices.

Index

Heavy Lifting

Lift with your legs, not your back and if it's over 50 lbs., a coworker should be asked to assist with a team lift of the object!

Roles & Responsibilities

A Data Owner is **a senior role with the ultimate responsibility** for the confidentiality, integrity, availability, and privacy of information assets. A data owner is responsible for labeling the asset & ensuring that it's protected with appropriate controls. The data owner typically selects the data steward & data custodian and has the authority to direct their actions, budgets, and resource allocations.

The Data Steward is primarily **responsible for data quality**. This involves ensuring data are **labeled** and identified with appropriate **metadata**. That data is collected and stored in a format and with values that comply with applicable laws and regulations.

The Data Custodian is the role that handles **managing the system** on which the data assets are stored. This includes responsibility for **enforcing access control, encryption, and backup/recovery measures**.

The Privacy Officer is responsible for oversight of any PII/SPI/PHI assets managed by the company.

The primary role of the Data Protection Officer (DPO) is to ensure that her organization processes the personal **data of its staff, customers, providers, or any other individuals** (also referred to as data subjects) in compliance with the applicable data protection rules. They must understand how any privacy-related information is used within business operations. Therefore, they are the best person for the auditor to interview to get a complete picture of the data usage.

Digital Certificates: Key Terms

A Certificate Signing Request (CSR) is what is submitted to the CA (certificate authority) to request a digital certificate.

Key Escrow stores keys

Certificate Revocation List (CRL) is a list of revoked certificates

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It Provides the validity status of certificates such as good, revoked, or unknown. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI).

Q: The digital certificate on the Dion Training web server is about to expire. Which of the following should Jason submit to the CA to renew the server's certificate?

A: CSR

Index

Policies

A Bring Your Own Device (BYOD) Policy allows (and sometimes encourages) employees to access enterprise networks and systems using personal mobile devices such as smartphones, tablets, and laptops. It's also the strategy MOST likely to introduce vulnerabilities into a corporate network!

Company-Owned/Personally Enabled (COPE) means that the company provides the users with a smartphone primarily for work use, but basic functions such as voice calls, messaging, and personal applications are allowed, with some controls on usage and flexibility.

With Choose Your Own Device (CYOD), the user can choose which device they wish to use from a small selection of devices approved by the company.

Corporate Owned Business Only (COBO) is a mobile device deployment model that provides the employee with a corporate-owned device that may only be used for official work functions and purposes.

Containerization is the logical isolation of enterprise data from personal data while co-existing in the same device. The major benefit of containerization is that administrators can only control work profiles that are kept separate from the user's personal accounts, apps, and data. This technology creates a secure vault for your corporate information. Highly targeted remote wiping is supported with most container-based solutions.

A remote access policy is a document that outlines and defines acceptable methods of remotely connecting to the internal network.

A password policy is a set of rules created to improve computer security by motivating users to create dependable, secure passwords and then store and utilize them properly. This document promotes strong passwords by specifying a minimum password length, complexity requirements, requiring periodic password changes, and placing limits on the reuse of passwords.

An onboarding policy is a documented policy that describes all the requirements for integrating a new employee into the company and its cultures, as well as getting that new hire all the tools and information they need to begin their job successfully.

Account Management Policies describe the account life cycle from creation through decommissioning.

Data Ownership Policies describe how ownership information is created and used.

Data Classification Policies describe the classification structure of the data in use by an organization.

Retention Policies describe what data will be maintained and for how long it will be retained. This would include the minimum & maximum retention periods as well as a description of information that needs to be retained. It's MOST UNLIKELY to include the classification of information retained!

A security group is a collection of user accounts that can be assigned permissions in the same way as a single user object. Security groups are used when assigning permissions and rights, as it is more efficient to assign permissions to a group than to assign them individually to each user. You can assign permissions to a user simply by adding the user to the appropriate group. In most corporate environments, security groups control access to share drives, mailing lists, and other network resources.

Index

Service-Level Agreement Guarantees

The Recovery Point Objective (RPO) is the interval of time that might pass during a disruption before the **quantity of data lost** during that period exceeds the Business Continuity Plan's maximum allowable threshold or tolerance.

The Recovery Time Objective (RTO) is the **duration of time** and a service level **within which a business process must be restored** after a disaster to avoid unacceptable consequences associated with a break in continuity.

The Mean Time To Repair (MTTR) measures the **average time it takes to repair** a network device when it breaks.

The Mean Time Between Failures (MTBF) measures the **average time between when failures** occur on a device, or between system breakdowns. MTBF is a crucial maintenance metric to measure performance, safety, and equipment design, especially for critical or complex assets, like generators or airplanes. It is also used to determine the reliability of an asset.

Q: Which of the following terms represents the maximum amount of data, as measured in time, that an organization is willing to lose during an outage?

A: RPO. Do not confuse with RTO because it said time! RPO represents data loss, RTO refers to service recovery times.

Q: Dion Training has performed an assessment as part of their disaster recovery planning. The assessment found that their file server has crashed twice in the last two years. The most recent time was in August, and the time before that was 15 months before. Which of the following metrics would best represent this 15-month time period?

A: MTBF

Mission Essential Functions & Critical Systems

Mission essential functions are things that must be performed by an organization to meet its mission. For example, the Army being able to deploy its soldiers is a mission-essential function. If they couldn't do that because a network server is offline, then that system would be considered a **critical system** and should be prioritized for higher security and better defenses.

Q: Janet, a defense contractor for the military, performs an analysis of their enterprise network to identify what type of work the Army would be unable to perform if the network were down for more than a few days. Which of the following was Janet trying to identify?

A: Mission Essential Function

Index

Access Control Models & Types

There are five main access control systems or models defined under different terms. The type of model that will work best depends on many different factors, including the type of building, number of people who need access, permission-granularity capabilities of an access control software, and the level of security required:

In a **Role-Based Access Control (RBAC)** method or model, **a security professional determines** user permissions or user privileges **based on the role of the employee**. This could be their position or title within the company, or the type of employment status, such as differentiating between a temporary employee and full-time staff.

With **Rule-Based Access Control (RuBAC)**, a **security professional or system administrator sets access management rules** that can allow or deny user access to specific areas, regardless of an employee's other permissions.

With **Discretionary Access Control (DAC)**, the decisions on user permissions are **taken at the discretion of one person, who may or may not have security expertise**. While this limits the number of people who can edit user permissions, this model can also put an organization at risk because the decision maker may not be aware of the security implications of their decisions. **RBAC is a modification of DAC.**

In contrast, **Mandatory Access Control (MAC)** models give the responsibility of access decisions to a **security professional who is the only person with authority** to set and manage permissions and access rights. This model is often used for businesses who protect sensitive data or property, and therefore require **the highest levels of security**.

Attribute-Based Access Control (ABAC), also known as policy-based control**, evaluates the attributes or characteristics of employees, rather than roles**, to determine access. An employee that doesn't present attributes set by the security administrator is denied access.

Attribute-based access control (ABAC) provides the most detailed and explicit type of access control over a resource because it is capable of making access decisions based on a combination of subject and object attributes, as well as context-sensitive or system-wide attributes. Information such as the group membership, the OS being used by the user, and even the machine's IP address could be considered when granting or denying access.

The security professional must have a full understanding of the levels of risk & the risk areas, the organizational structure, business processes & the roles & responsibilities of all employees who require access.

Q: Which of the following access control models is the most flexible and allows the resource owner to control the access permissions?

A: DAC

Discretionary access control (DAC) stresses the importance of the owner: The original creator of the resource is considered the owner and can then assign permissions and ownership to others. The owner has full control over the resource and can modify its ACL to grant rights to others. This is the most flexible model and is currently implemented widely in Windows, Unix, Linux, and macOS systems.

Index

Assessments & Reports

Qualitative Risk Assessments categorize things based on the likelihood and impact of a given incident using non-numerical terms, such as high, medium, and low. It also utilizes red, yellow, and green colors based on the likelihood and impact of a given incident.

Quantitative Risk Assessments, on the other hand, provide exact numbers or percentages of risk.

A Privacy Impact Assessment (PIA) is a process used to determine how a program or service could affect the privacy of an individual. It can also help to avoid or lessen possible negative effects on privacy that might result from a program or service. It's a process which assists organizations in identifying and managing the privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, business relationships etc. It benefits various stakeholders, including the organization itself and the customers, in many ways. In the United States and Europe, policies have been issued to mandate and standardize privacy impact assessments.

The Lessons Learned Report provides you with the details of the incident, its severity, the remediation method, and, most importantly, how effective your response was. Additionally, it provides recommendations for improvements in the future.

A Forensic Analysis Report would not provide recommendations for future improvements, even though it provides many other details.

A Trend Analysis Report describes whether behaviors have increased, decreased, or stayed the same over time.

The Chain of Custody Report is the chronological documentation or paper trail that records the custody, control, transfer, analysis, and disposition of physical or electronic evidence.

Q: Vulnerability scans must be conducted continuously to meet regulatory compliance requirements for the storage of PHI. During the last vulnerability scan, a cybersecurity analyst received a report of 2,592 possible vulnerabilities and was asked by the Chief Information Security Officer (CISO) for a plan to remediate all the known issues. Which of the following should the analyst do next?

A: Filter the scan results to include only those items listed as critical in the asset inventory and remediate those vulnerabilities first

When attempting to remediate numerous vulnerabilities, it is crucial to prioritize them to determine which ones should be remediated first. In this case, there is a regulatory requirement to ensure the security of the PHI data. Therefore, those assets critical to the secure handling & storage of PHI should be prioritized for remediation. Besides, it's impractical to resolve all 2,592 vulnerabilities at once!

Q: During your review of the firewall logs, you notice that an IP address from within your company's server subnet had been transmitting between 125 to 375 megabytes of data to a foreign IP address overnight each day. You have determined this has been occurring for approximately 5 days, and the affected server has

since been taken offline for forensic review. Which of the following is MOST likely to increase the impact assessment of the incident?

A: PII of company employees and customers was exfiltrated

If the PII (Personally Identifiable Information) of the company's employees or customers were exfiltrated or stolen during the compromise, this would increase the incident's impact assessment. Loss of PII is a big issue for corporations and one that might garner media attention: <u>While all of the options presented here are bad things that could increase the impact of the assessment, loss of PII is considered the MOST likely to increase the impact dramatically.</u> Depending on the organization's size & type, there may also be mandatory reporting requirements, fines, or restitution that must be paid.

Annual Loss Expectancy (ALE) & Related Calculations

AV = Asset Value

EF / RF = Exposure / Risk Factor

SLE = Single Loss Expectancy

SLE = AV x EF

ARO = Annual Rate of Occurrence

ALE = Annual Loss Expectancy

ALE = SLE x ARO

Q: Jamie's organization is attempting to budget for the next fiscal year. Jamie has calculated that the asset value of a database server is $120,000. Based on her analysis, she believes that a data breach to this server will occur once every four years and has a risk factor is 30%. What is the ALE for a data breach within Jamie's organization?

A: $9,000

SLE = AV x RF = 120000 * 30% = $36,000

ALE = SLE x ARO = 36000 * 0.25 = $9,000

Remember it logically: the annual loss expectancy will be the SLE i.e. single loss expectancy times the annual rate of occurrence. So if the single loss expectancy is $100, and if it occurs twice a year, of course the annual loss expectancy is $200! Similarly, if it's once every four year, that's 0.25 a year times the SLE.

Similarly, the single loss expectancy will be the asset value time the risk factor, as in the asset-cost times the risk to it.

Index

Data: Clearing Hard Drives and Restoring Backups

For clearing hard drives of sensitive data, purging the drives, validating that the purge was effective, and documenting the sanitization is the best response.

Purging includes methods that eliminate information from being feasibly recovered even in a lab environment. For example, performing a Cryptographic Erasure (CE) would sanitize and purge the drives' data without harming the drives themselves. **Purging includes degaussing, encryption of the data with the destruction of its encryption key, and other non-destructive techniques.**

The Cryptographic Erase (CE) method sanitizes a self-encrypting drive by erasing the media encryption key **and then re-imaging the drive. It's the most efficient method of sanitizing a drive.**

A Secure Erase (SE) is used to perform the sanitization of flash-based devices (such as SSDs or USB devices) when cryptographic erase is not available.

The Zero-Fill Method relies on overwriting a storage device by setting all bits to the value of zero (0), but this is not effective on SSDs or hybrid drives.

Clearing them leaves the possibility that some tools would allow data recovery. Clearing data prevents data from being retrieved without the use of state-of-the-art laboratory techniques. Clearing often involves overwriting data one or more times with repetitive or randomized data.

Destroying data is designed not merely to render the information unrecoverable but also to hinder any reuse of the media itself. Destruction is a physical process that may involve shredding media to pieces, disintegrating it into parts, pulverizing it to powder, or incinerating it to ash.

Data Wiping or clearing occurs by using a software tool to overwrite the data on a hard drive to destroy all electronic data on a hard disk or other media. Data wiping may be performed with a 1x, 7x, or 35x overwriting, with a higher number of times being more secure. This allows the hard drive to remain functional and allows for hardware reuse.

Degaussing a hard drive involves demagnetizing a hard drive to erase its stored data. You cannot reuse a hard drive once it has been degaussed. Degaussing is classified as a form of purging: Some generic magnetic storage devices can be reused after the degaussing process has finished, such as VHS tapes and some older backup tapes. For this reason, though, the technique of **degaussing is classified as purging and not destruction**, even though hard drives are rendered unusable after being degaussed.

Shredding involves the physical destruction of the hard drive. This is a secure method of destruction but doesn't allow for device reuse. Destroy requires physical destruction of the media, such as pulverization, melting, incineration, and disintegration.

Hardware & Software Write Blockers are designed to ensure that forensic software and tools cannot change a drive inadvertently by accessing it. If a question indicates that you need to choose the BEST solution to protect the drive's contents from being changed during analysis, you should pick the hardware write blocker. A hardware write-blocker's primary purpose is to intercept and prevent (or 'block') any modifying command operation from ever reaching the storage device.

Index

Q: An attacker has compromised a virtualized server. You are conducting forensic analysis as part of the recovery effort but found that the attacker deleted a virtual machine image as part of their malicious activity. Which of the following challenges do you now have to overcome as part of the recovery and remediation efforts?

A: The attack widely fragmented the image across the host file system (NOT that you'll need to rollback to an early snapshot and then merge any checkpoints to the main image)

Due to the VM disk image's deletion, you will now have to conduct file carving or other data recovery techniques to recover and remediate the virtualized server. If the server's host uses a proprietary file system, such as VMFS on ESXi, this can further limit support by data recovery tools. The attacker may have widely fragmented the image across the host file system when they deleted the disk image.

VM instances are most useful when they are elastic (meaning they optimally spin up when needed) and then destroyed without preserving any local data when security has performed the task, but this can lead to the potential of lost system logs. To prevent this, most VMs also save their logs to an external Syslog server/file.

Virtual machine file formats are image-based and written to a mass storage device. Depending on the configuration and VM state, security must merge any checkpoints to the main image, using a hypervisor tool, not recovery from an old snapshot, and then roll forward. It is possible to load VM data into a memory analysis tool, such as Volatility. However, some hypervisors' file formats require conversion first, or they may not support the analysis tool.

Q: You have been hired as a consultant by Dion Training to review their current disaster recovery plans. The CEO has requested that the plans ensure that the company can limit downtime in the event of a disaster. Still, due to staffing concerns, he cannot approve the budget to implement or maintain a fully redundant offsite location to ensure 99.999% availability. Based on that limitation, what should you recommend to the CEO?

A: Redundant hardware be maintained at the offsite location and configured to be ready for the recovery of the company's backup data when needed (NOT collocation!)

A Warm Site provides some of a hot site's capabilities, but it requires the customer to do more work to become operational. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations. For most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement. By placing your redundant hardware at the offsite location and configuring it to be ready for recovery when needed, the company can have a higher availability level than a cold site but not have the full personnel costs involved with a hot site.

A Hot Site would ensure that the offsite location has all the hardware, equipment, personnel, and data installed and ready to provide services at all times, which is much more expensive than a warm site.

It is not recommended that your redundant servers are located within the same building since a fire, flood, or other disaster could destroy your primary and redundant capabilities.

Retaining the hardware at the office building but shipping the backups offsite is more in line with a Cold Site description. This would also not provide high availability levels since the systems would need to be set up, configured, and made ready for use.

Index

Documents, Agreements & Risks

A Service Level Agreement (SLA) is a documented commitment between a service provider and a client, where the quality, availability, and responsibilities are agreed upon by both parties.

A Non-Disclosure Agreement (NDA) is a documented agreement between two parties that define what data is considered confidential and cannot be shared outside of that relationship. An NDA is used to protect an organization's intellectual property.

An Acceptable Use Policy (AUP) is a set of rules applied by the owner, creator, or administrator of a network, website, or service, that restrict how the network, website, or system may be used and sets guidelines as to how it should be used.

A Memorandum of Understanding (MOU) is a non-binding agreement between two or more organizations to detail what common actions they intend to take.

The Business Continuity Plan (BCP) focuses on the tasks carried out by an organization to ensure that critical business functions continue to operate during and after a disaster. It outlines how a business will continue operating during an unplanned service disruption. A business continuity plan is more comprehensive than a disaster recovery plan and contains contingencies for business processes, assets, human capital, and business partners, and essentially every other aspect of the business that might be affected.

EULA is an End-User License Agreement and is used during the installation of a piece of software.

A Scope/Statement of Work (SOW) is a document that outlines all the work that is to be performed, as well as the agreed-upon deliverables and timelines.

Security Policy is a definition of what it means to be secure for a system, organization, or other entity.

A Disaster Recovery Plan is a documented, structured approach that documents how an organization can quickly resume work after an unplanned incident. These are **natural or man-made disasters**: unplanned incidents include things like natural disasters, power outages, cyber-attacks, and other disruptive events. The first step to developing an effective disaster recovery plan is to identify all assets. Once identified, you can then determine what assets and services are essential to business operations, what risks are facing them, and how best to recover in the event of a disaster.

An Incident Response Plan contains a set of instructions to help our network and system administrators detect, respond to, and recover from network **security** incidents. These types of plans address issues like cybercrime, data loss, and service outages that threaten daily work. It's a generic document for the overall steps of incident response and therefore does not apply to just a specific type of incident.

A Playbook is a checklist of actions to perform to detect and respond to a specific type of incident. Your organization will have playbooks for phishing attempts, privilege escalation, and other specific types of incidents.

A Runbook is an **automated version of a playbook used by a SOAR** to have the system conduct as many steps as possible.

The Interconnection Security Agreement (ISA) governs the relationship between any federal agency and a third party interconnecting their systems.

Index

System Lifecycle Plans, also known as life cycle planning, describe the approach to maintaining an asset from creation to disposal. In the information technology world, we normally have a 5-phase lifecycle that is used for all of our systems and networks: Planning, Design, Transition, Operations, and Retirement.

Change Management Documentation authorizes changes and upgrades and should include the specific details of what was changed and what things may have been affected by the change. Change Management is a systematic approach to dealing with the transition or transformation of an organization's goals, processes, or technologies.

A Master Service Agreement (MSA) is a contract reached between parties, in which the parties agree to most of the terms that will govern future transactions or future agreements. The MSA **is used when a pentester will be on retainer for a multi-year contract**, and an individual SOW will be issued for each assessment to define the individual scopes for each one.

Risk Appetite describes **how much risk an organization is willing to accept**. This is a crucial factor both in designing the assessment and determining the recommended mitigations.

Risk Mitigation is a strategy to **prepare for and lessen the effects of threats** faced by a data center. Risk mitigation refers to applying security controls to reduce the risk of a known vulnerability.

Risk Avoidance is the **elimination of hazards, activities, and exposures** that can negatively affect an organization's assets.

Risk Acceptance is the act of **accepting the identified risk and not taking additional actions to reduce the risk because the risk is low enough.** Risk acceptance should only be done once an organization’s risk tolerance is defined and communicated amongst the decision-makers.

Q: You are assisting the company with developing a new business continuity plan. What would be the BEST recommendation to add to the BCP?

A: Build redundant links between core devices (NOT backups!)

By keeping redundant links between core devices, critical business services can be kept running if one link is unavailable during a disaster. Some of the other options are good ideas, too, but this is the BEST choice to maintain a high availability network that can continue to operate during periods of business disruption.

Q: Last night, your company's system administrators conducted a server upgrade. This morning, several users are having issues accessing the company's shared drive on the network. You have been asked to troubleshoot the problem. What document should you look at first to create a probable theory for the cause of the issue?

A: Change management documentation (NOT release notes for the server software, however more logical that sounds)

Q: Jason wants to use his personal cell phone for work-related purposes. Because of his position, Jason has access to sensitive company data, which might be stored on his cell phone during its usage. The company is

Index

concerned about this but believes that it might be acceptable with the proper security controls in place. Which of the following should be done to protect both the company and Jason if they allow him to use his personal cell phone for work-related purposes?

A: Conduct real-time monitoring of the phone's activity and usage

While all four are good options (NDA, AUP & occasional-monitoring), the BEST solution (though the question did not ask for it and instead stated "acceptable security measures"! WTF man?) is to conduct real-time monitoring of the phone's activity since it is a technical control that could quickly identify an issue. The other options are all administrative controls (policies), which are useful but would not actually identify if the sensitive data was leaked from Jason's phone.

Q: Which type of agreement between companies and employees is used as a legal basis for protecting information assets?

Q: Which of the following agreements is used between companies and employees, between companies and contractors, and between two companies to protect information assets?

A: NDA (Note: Neither 'proprietary' nor 'confidential' were mentioned in the question!)

Q: Which of the following BEST describes when a third-party takes components produced by a legitimate manufacturer and assembles an unauthorized replica sold in the general marketplace?

A: Counterfeiting

Some of the more colorful options included 'Capitalism' and 'Entrepreneurship'!!!

Q: What is a legal contract outlining the confidential material or information that will be shared by the pentester and the organization during an assessment?

A: NDA

This is the definition of a Non-Disclosure Agreement (NDA). There may be two NDAs in use: One from the organization to the pentester and another from the pentester to the organization.

Q: Which of the following policies or plans would dictate how an organization would respond to a fire that left their office building unusable for the next 3 months?

A: Disaster Recovery Plan

Easy to confuse for Business Continuity Plan (and I did in the mock test!), but the question asks about RESPONDING to a fire, NOT how operations will continue! A good note to end on then: READ THE QUESTIONS CAREFULLY!!!

Index