Question 1.

PART A

Wireshark Traffic Analysis - Wireshark, a potent network protocol analyser, serves as a vital tool in detecting IP sniffing and spoofing activities within GlobalTech Solutions' network. By capturing live network traffic, Wireshark allows analysts to scrutinize packet contents for unauthorized interception. Analysts can identify anomalies in packet patterns, such as unexpected IP sources or mismatched MAC addresses, indicating potential IP spoofing. Wireshark's protocol analysis features highlight abnormal network behaviour, flagging unusual FTP commands or TCP handshake sequences that signify spoofed activities. Detection of ARP spoofing is facilitated through analysis of ARP request and reply packets. Additionally, Wireshark enables examination of traffic patterns and volumes, pinpointing sudden spikes or deviations from normal traffic flow. By leveraging Wireshark's capabilities, GlobalTech can swiftly detect, analyse, and respond to IP sniffing and spoofing threats, bolstering its cybersecurity defences

Intrusion Detection System

An Intrusion Detection System (IDS) at ABC's network would detect IP spoofing by analysing packet headers for inconsistencies, such as mismatched source IP addresses or abnormal TTL values. It employs signature-based detection, recognizing known spoofing patterns, and anomaly-based detection, identifying deviations from normal traffic behaviour. For instance, ARP spoofing or unusual data transfers could trigger alerts. The IDS logs events in real-time, providing immediate alerts to network administrators for swift response. Integration with firewalls allows for automated blocking of suspicious traffic sources. Historical analysis of logged events enables ABC to identify trends and strengthen network security against IP spoofing threats.

Analysing FTP Traffic –

Analysing FTP (File Transfer Protocol) traffic at ABC's network provides a crucial means of detecting IP spoofing attempts. By scrutinizing packet headers, FTP analysis verifies the legitimacy of source IP addresses. Any packets originating from unexpected or unauthorized IP ranges are flagged as potential IP spoofing indicators. Additionally, comparing MAC addresses within Ethernet frame headers against their associated IP addresses helps identify inconsistencies that suggest IP spoofing. Unusual traffic patterns, such as sudden spikes in FTP data transfers or abnormal protocol usage, serve as red flags for suspicious activity. Timestamp analysis further aids in pinpointing unauthorized access, especially during off-hours. This comprehensive approach, coupled with cross-referencing findings with IDS alerts, allows ABC to proactively identify and respond to potential IP spoofing incidents. FTP traffic analysis becomes a pivotal tool in securing the network, preventing unauthorized access, and safeguarding sensitive data from malicious IP spoofing activities.

PART B

Multi-Factor Authentication (MFA)-

Implementing Multi-Factor Authentication (MFA) serves as an immediate and potent strategy to counter the ongoing IP spoofing and packet sniffing attacks at ABC. MFA requires additional verification beyond passwords, such as OTPs or biometrics, making stolen credentials insufficient for access. Dynamic OTPs render intercepted codes useless after expiration, thwarting replay attacks from packet sniffing. MFA's device trust and contextual authentication factors, like geolocation, trigger extra verification for suspicious IPs or devices, preventing spoofed access attempts. For remote OpenVPN connections, MFA provides a robust layer of security, requiring attackers to bypass the second factor even with intercepted credentials. By swiftly deploying MFA, ABC fortifies its network against these threats, ensuring a resilient defence and safeguarding critical systems and sensitive data from unauthorized access.

IP Whitelisting and Blacklisting-

IP Whitelisting allows only trusted IP addresses to access the OpenVPN, bolstering security by restricting connections to known, authorized sources. Conversely, Blacklisting blocks known malicious IPs, preventing attackers from using spoofed IP addresses to gain unauthorized entry, fortifying the network against potential threats.

Update & Patching

Updating and patching network devices, operating systems, and applications plays a crucial role in mitigating the risk of IP spoofing. By addressing known vulnerabilities in network devices such as routers and switches, organizations reduce the likelihood of exploitation for malicious purposes. These updates often include security enhancements, strengthened authentication mechanisms, and protocol hardening measures, all of which contribute to a more secure network environment. Additionally, firmware updates for network devices ensure that any vulnerabilities in the device's firmware are remediated. Regular updates also enable intrusion prevention systems to have the latest threat intelligence, aiding in the detection and prevention of IP spoofing attempts. By adhering to compliance requirements and maintaining up-to-date software and firmware, organizations demonstrate their commitment to cybersecurity best practices. In essence, updating and patching create multiple layers of defence, collectively reducing the risk of successful IP spoofing attacks in the network

Network segmentation -

Introducing switches and bridges into GlobalTech's network infrastructure offers a strategic approach to bolstering security against IP spoofing and packet sniffing threats. While traditionally motivated by performance enhancements, these devices serve as crucial tools in limiting the flow of sensitive information and preventing unauthorized access. By segmenting network traffic, switches and bridges create boundaries that impede the spread of malicious activities. This segmentation ensures that sensitive data remains isolated and inaccessible to untrustworthy devices, enhancing overall network security. GlobalTech can leverage these benefits to fortify its cybersecurity posture, aligning with the company's goal of mitigating the current sophisticated attack vectors.

PART C

The table below defines each impact category description and its associated severity levels. Use the tables below to identify impact levels and incident details.

Impact Category	Category Severity Levels
Functional Impact – A measure of the impact to business functionality or ability to provide services	NO IMPACT – Event has no impact. DENIAL OF CRITICAL SERVICES/LOSS OF CONTROL – A critical system has been rendered unavailable. NO IMPACT TO SERVICES – Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers. MINIMAL IMPACT TO NON-CRITICAL SERVICES – Some small level of impact to noncritical systems and services. MINIMAL IMPACT TO CRITICAL SERVICES – Minimal impact but to a critical system or service, such as email or active directory. SIGNIFICANT IMPACT TO NON-CRITICAL SERVICES – A non-critical service or system has a significant impact SERVICES – A non-critical system is denied or destroyed. SIGNIFICANT IMPACT TO CRITICAL SERVICES – A critical system has a significant impact, such as local administrative account compromise
Information Impact – Describes the type of information lost, compromised, or corrupted.	NO IMPACT – No known data impact. SUSPECTED BUT NOT IDENTIFIED – A data loss or impact to availability is suspected, but no direct confirmation exists. PRIVACY DATA BREACH – The confidentiality of personally identifiable information (PII6) or personal health information (PHI) was compromised PROPRIETARY INFORMATION BREACH – The confidentiality of unclassified proprietary information7 , such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.

	DESTRUCTION OF NON-CRITICAL SYSTEMS – Destructive techniques, such as master boot record (MBR) overwrite; have been used against a non-critical system. CRITICAL SYSTEMS DATA BREACH - Data pertaining to a critical system has been Exfiltrated CORE CREDENTIAL COMPROMISE – Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated. DESTRUCTION OF CRITICAL SYSTEM – Destructive techniques, such as MBR overwrite; have been used against a critical system.
Recoverability – Identifies the scope of resources needed to recover from the incident	REGULAR – Time to recovery is predictable with existing resources. SUPPLEMENTED – Time to recovery is predictable with additional resources. EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed. NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly)

Question 2

Part A

Meanwhile, after discovering that the malware virus has infected the network, GlobalTech Solutions quickly proceeds with the containment process which aims to limit the spread and minimizes the chances of negative impact on its network and systems. The method for containment differs by the nature and the scale of the malware. Disconnecting brief or non-infectious cases systems from the network, and shutting them down immediately, are required of prompt action. This minimizes any further command and control channel and halts the execution of the attack codified into the malware thereby reducing the extent of damage. Nevertheless, when an attack is aimed at decentralized covert infections, a comprehensive plan is required. The contained strategy addresses the issue of speediness across most systems and cut down on the amount the infected computer in the potential damage, hence promote a quick recovery. GlobalTech should pay attention to crucial systems; precisely delineating what the consequences of disconnecting or powering down critical

functions versus carrying on with operations albeit possibly the security threat could be detrimental. For the critical systems which failings can bring more serious consequences; internet segmented network and access controls are perhaps good solution. Moreover, network subdividing, blocking communication channels through that the malware spreads, impairing services that are not in use and the monitoring for signs of the attack continuing are also crucial steps. Such recognition should be remembered that said malware containing all necessary tools will work further even though the malware's spread was halted. This implies that the staff should always be ready to start off immediate eradication process including disconnected systems by applying anti-viruses' power, executing forensic analysis, installing clean backups, or the last step may be to rebuild affected systems from the scratch. Through this process, we will keep careful records of all containment actions, system state, and those decisions made as these will serve as indispensable references for post incident analysis, reports, and optimizing the protocols in handling future incidents. This structured approach to containment aligns with GlobalTech's risk tolerance, ensuring a focused and effective response to the malware incident while safeguarding critical operations and data.

(ii) Identifying and Removing Each Malware Component-

Identification Of Malware -

Virus	Worms	Rootkit
Simple computer viruses replicate by copying themselves byte-by-byte to infect new files, easily detected by searching for a specific "virus signature" within their code.	Broadcast messages or attempts to exploit known vulnerabilities	Utilize anti-virus programs that specifically search for known rootkits based on their signatures.
if your computer's performance suddenly drops (or freezes repeatedly), it could be a virus. Alternatively, a slowdown can be the result of a corrupted file or application.	Recognize that adversaries may seek to gain administrator-level access, potentially leading to data theft or compromise of multiple systems.	Monitor the system for sluggish performance, extended startup times, frequent freezing, or unresponsive behaviour to mouse and keyboard input.
Some viruses are designed to hijack your computer's internet connection — either to send files without your knowledge, act as a part of a botnet in a distributed denial-of-service (DDoS) attack, or run processor-heavy tasks like	Look out for increased network traffic, unusual consumption of bandwidth, and excessive use of hard-drive space.	Dedicated rootkit detection tools can scan for specific signatures or employ heuristic techniques to identify hidden processes, files, or kernel hooks.

mining cryptocurrencies. In these cases, you will see higher-than-usual network usage — especially if your device is on a mobile network.		
Some viruses create or modify files on your computer. You may see applications you do not recognize, missing files, or new ones mysteriously appearing with legitimate-sounding names (sometimes even copying reputable brands, such as Microsoft or Google).	Processes running without user knowledge related to worm propagation	Changes to system settings without user knowledge.

Removal Of Malwares-
Virus Component Eradication:

Upon detecting the virus in GlobalTech Solutions' network, the Incident Response Team isolates infected machines to prevent further spread. They run remote antivirus scans on isolated hosts, removing the virus from infected files. Simultaneously, vulnerabilities allowing the virus entry are patched, securing the network. This comprehensive approach combines antivirus scans, vulnerability patches, and containment measures to eradicate the virus and fortify the network against future threats.

Worm Component Eradication:

After containing the worm, the Incident Response Team identifies infected hosts using utilities and applies necessary patches remotely. Automated antivirus scans efficiently remove the worm from most systems. However, for critical systems causing significant damage, manual isolation and handling are necessary. The team ensures all infected hosts are either remotely updated on a separate VLAN or manually patched. This combination of automated and manual actions eliminates the worm and prevents reinfections.

Rootkit Component Eradication:

The Cybersecurity Team employs specialized rootkit detection tools to scan systems thoroughly. For compromised hosts, they opt for a meticulous approach, rebuilding systems from secure backups. Manual inspection supplements rootkit detection, ensuring no remnants remain. Hosts showing extensive infection or instability post-eradication attempts are prioritized for rebuilding. By restoring from backups and thorough manual inspections, the team ensures complete rootkit eradication, restoring network integrity and security.

(iii)

Post-Incident Analysis

Forensic Analysis-

Finding out the scope of a cybersecurity issues following the forensics gives a well-defined picture of the event and helps to reinforce the next defence line. A rigorous review of the documentation is essential which includes diaries and reports of incidents. Therefore, GlobalTech Solutions can ensure the response protocols are followed and the vulnerabilities are addressed. The calculated monetary damage that the incident brought about presented a concrete number objective, which represented the level of criticality of its effect on business processes. Additionally, pinpointing the attack's pre-condition, the route of attack, and the exploited software weakness helps to fashion countermeasure that narrow down the chances of such happenings in future. The notions and feedback from resource owners during the team reference will offer their valuable subjective insights, which could be used to address root causes and apply improvements in incident response strategies. Regular tests of response protocols against conventional standards and prevailing regulations enable the continuous improvement of cyber protection and defence capabilities.

Future Prevention-

To bridge the effectiveness gap in incident response, GlobalTech Solutions plans to invest in critical resources essential for managing incidents swiftly and efficiently. This includes acquiring encryption software, network diagrams, digital forensic tools, and backup copies. These resources streamline the investigation and emergency response processes, ensuring a well-prepared response team.

Moreover, preventing incidents from occurring in the first place is a key focus. This is achieved through the development and maintenance of robust security measures for various networks, systems, and applications. Constant risk assessments help identify vulnerabilities, reducing risks to an acceptable level and lowering the frequency of occurrences.

Specialist skills within the team involve identifying precursors and indicators of incidents using intrusion detection systems, antivirus software, and file integrity checks. Additionally, leveraging third-party monitoring services enhances the chances of incident identification.

Establishing avenues for external groups to report incidents fosters collaboration and timely responses. This could involve having an incident reporting channel readily available.

Logging and auditing practices become foundational, with critical systems requiring enhanced levels of monitoring. Detailed logs provide valuable insights during investigations, tracing the attacker's path and identifying affected assets.

Profiling networks and systems aids in swiftly detecting deviations from normal activity levels, enabling proactive response measures. A comprehensive log retention policy ensures critical data is preserved for analysis, with event log correlation across systems helping build a coherent incident story.

Synchronizing host clocks facilitates efficient event correlation, crucial for building incident timelines. A central knowledge base facilitates quick access to needed responses during incident analysis, enabling a cohesive problem-solving approach.

Documenting all steps taken during an incident is vital for evidentiary purposes, including timestamps and detailed records of actions. Safeguarding incident data with restricted access protects sensitive information related to vulnerabilities and breaches.

Prioritizing incident handling based on impact and recoverability optimizes resource allocation and justifies actions to management and system owners. Clear procedures for evidence gathering and handling, meeting legal requirements, and obtaining forensic system snapshots ensure evidence preservation.

Post-incident lessons learned meetings contribute to ongoing improvements in security measures and the incident handling process. Overall, these tools, strategies, and procedures fortify GlobalTech Solutions' incident response capabilities, enhancing its cybersecurity posture.

PART B

Social Engineering Attacks Used in the "employer21" Incident:

Phishing:

Teacher gets the attack vector through a spearfishing mail. This email looks like the original one but is full of macros used for launching an attack. The attacker fools the teacher by seeming the official communication and tries to execute the attack.

Reason: Phishing attacks make use of social engineering to persuade deceived individuals to convey sensitive information or to carry out actions contravening the security. In this instance the scammer will impersonate as a proven source of trust (school or workplace) to allure people to open the dangerous attachment. The attack kicks off when a spear-phishing email is received by the teacher. The email looks like a legitimate assignment. phishing is a social engineering scam where criminals use email messages and other messaging services to make people share confidential data, click on infected links, or open malicious attachments.

In this case, hackers use the advantage of the trust that the teacher has when s/he is expected to get assignments through email. The sender's name as well as its email address may look like the one from the school administration or the employer. The email can have official-looking logos, language, and formatting to trick people on thinking it is from an actual person. The attackers use the macros, which are planted into the attachment, as the vulnerable vector to compel the teacher to open the file and then trigger the malicious code.

Ransomware Demand:

The malicious program moves to encrypt the victim's file. Then, when it is finished, a message about the £500 ransom in Bitcoin is displayed on the screen. This exact verdict is ensued by dread and urgency, and compels the victim to obey attackers’ demands.

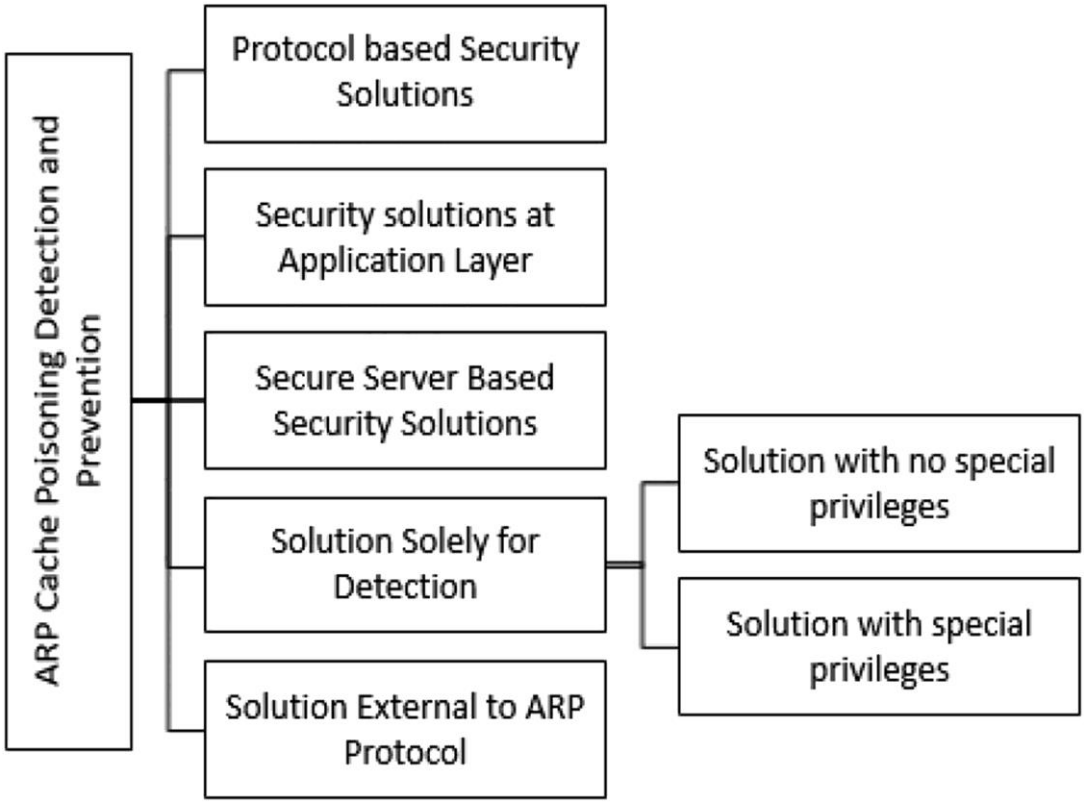
Reason: For instance, ransomware onslaughts often use lack of calmness and anxiety to pressure the victims to settle the ransom on time. The hackers are banking on the victim quickly re-gaining access to their most important files against railing loss of access. The attack goes into a spear-phishing email sent to the teacher, shorter than it seems a regular assignment. Phishing is an example of social engineering, where attackers use email or similar services to deceive users into

revealing their sensitive information, clicking on connections that are not secure, or downloading harmful documents.

In this scenario, the hacker can capitalize on the trust that the student has in the teacher and sending assignments via email. The e-mail possibly pretentious to be from a recognized source; might be the school management or the employer. The email can be displayed with a variety of official-looking logos, font, and design to make it appear to be genuine. Malicious macros embedded into the attachment serve to lure the teacher's natural curiosity, duty, or recklessness to open the file and execute the malicious code.

Question 3

A malicious user can use ARP cache poisoning to impersonate any user in a network or to disrupt the services of a network. Such attacks are highly intentional and result in loss of privacy and unavailability of network services. There are several security solutions that have been proposed by researchers which provide detection of (and/or protection against) ARP cache poisoning attacks. The classification of existing schemes is shown in Fig.



PART A

1. A technique using fake packets - In this approach, spoof and spoiled packets are sent with trap packets to network hosts. It shows that only the malicious host is the one that can respond to the

fake request. Nevertheless, in this instance an originating host carrying IP packet routing is presumed hostile which may not be true in all the cases. Numerous legitimate reasons to execute IP packet route forwarding can be caused by devices that use Bluetooth, USB, or Wi-Fi for network services.

Moreover, elaborates this by viewing hosts with IP routing enabled as suspect instead of immediate representations of malicious intent. This extension uses two approaches to identify potentially malicious hosts among the suspicious ones: violating the ARP cache of each patient and violating the CAM table of each switch.

2. Tracing the Source of ARP Cache Poisoning Attack with Wireshark –

Using Wireshark, we analyse ARP packets in the effected network segments by means of applying filters, used to identify inconsistencies like multiple MAC address for one IP or inappropriate broadcasts. We utilize inspection of ARP Tables which involves comparison of legitimate entries with potential malicious ones, with malicious entries been captured as unauthorized mappings. Some of the Wireshark facilities test blocks like repeated requests to the same IP or conflicts in MAC addresses and this helps to detect ARP spoofing. Moreover, we use the ARP packet captures to link the network event data with a timeline spotting unusual spikes or simultaneous requests from multiple devices for the same IP address. Such as a case, the Wireshark mode contributed that find the origin(s) of ARP cache poisoning attack is rigorous.

3. To conduct ARP poisoning attacks in the corporate network, the usage of network security tool to guide the research process is inevitable. Putting IDS and IPS in place and attention to network traffic and indicators of energetic during exploitation of certain vulnerabilities, for example, port 445 in the case of SMB, allow us to control the traffic. Furthermore, the review of firewall logs becomes particularly important looking for outbound traffic on SMB v1's ports TCP 445 and 139, non-responsiveness of the Port 445 port (another indicator of a potential stealth attack), and scanning of multiple ports to UDP ports 137 and 138. Such patterns may be a sign of the actual attacks of the attackers endeavouring to explore the systems vulnerable points. Consequently, we should make the immediate response as the action is to prevent the leakage of any traffic on Port 445. Through the implementation of SIEM tool Americas Like Event Log Analyzer will be able to provide insightful notifications and real-time analytics about the source, the effected network resources, and the time of the attack. About the investigation, it provides a detailed forensic analysis, allowing the company to counter the approach quickly and establish mitigation measures against future extensive assaults within the highly divergent network infrastructure.

PART B

1. Enabling DAI (Dynamic ARP Inspection):

Dynamic ARP Inspection (DAI) is like a security guard for the building. It checks every message (ARP packet) to see if the sender's name (IP address) matches the box it is going to (MAC address) based on past deliveries (DHCP snooping database). If something does not match, like a different

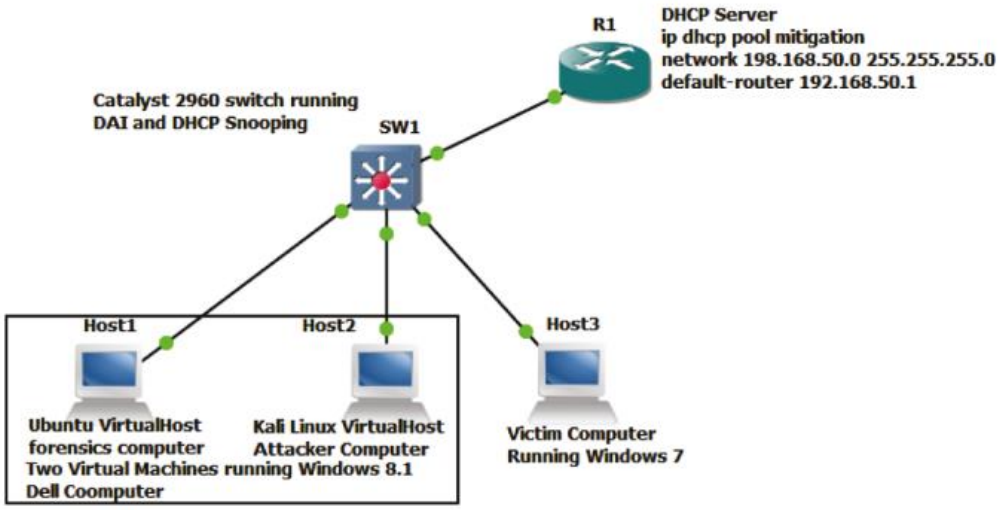
neighbour claiming your box, DAI throws the message away (drops the packet). This prevents the attacker from stealing your mail (intercepting traffic). However, if you have a personal mailbox key (static IP address) and do not use the regular mail system (DHCP), DAI needs to be informed separately (static mapping) to ensure your mail gets delivered correctly.

Phased Implementation:

Start with critical segments: Begin by implementing DAI in the most crucial parts of the network, where security breaches can have the biggest impact. This allows for testing and refinement of the strategy before broader deployment.

Gradual rollout: Implement DAI incrementally across different network segments, monitoring for any compatibility issues or disruptions with existing technologies. This gradual approach allows for adjustments and minimizes potential network downtime

.



2. Isolation - The immediate response to the ARP cache poisoning attack in this diverse network must balance effective containment with minimal operational disruptions. First and foremost, segmentation and isolation are critical steps. By immediately isolating affected systems and segments using VLANs and firewall rules, the spread of the attack can be halted. This includes separating the compromised Windows production servers and Linux R&D servers into distinct VLANs to contain the impact.

3. Patching and Update - Simultaneously, patching and updating vulnerable systems is paramount. This includes addressing outdated Windows systems vulnerable to SMB exploits and securing SSH configurations on Linux servers. Resetting potentially compromised credentials, especially those used for SSH and SMB access, helps prevent further unauthorized access. Enhanced monitoring through IDS/IPS rules tailored to detect ARP poisoning attempts, coupled with real-time alerting mechanisms, enables swift detection of ongoing malicious activities.

PART C

Access Controls: Effective access control measures play a pivotal role in bolstering the security of the company's network infrastructure against potential threats such as ARP cache poisoning. By implementing role-based access control (RBAC) and access control lists (ACLs), unauthorized access to critical network resources is curtailed. This ensures that only authorized personnel with specific roles and responsibilities can interact with sensitive systems and data. Network segmentation, facilitated by access control, divides the network into isolated segments, limiting the scope of potential attacks like ARP cache poisoning. Additionally, access control logs and monitoring tools help detect anomalous or unauthorized access attempts, enabling prompt response and mitigation. The principle of least privilege ensures that users and devices have minimal access rights necessary for their tasks, reducing the attack surface. Integration with strong authentication methods like multi-factor authentication (MFA) adds an extra layer of security, requiring multiple factors for user verification. Regular review and updates of access control policies ensure alignment with evolving security needs, ensuring a resilient network defence posture against emerging threats.

Guideline for Future - Incident response and forensic readiness are crucial for mitigating the impact of potential ARP cache poisoning attacks. A well-defined incident response plan ensures swift identification, containment, and mitigation of the attack, minimizing downtime and business disruption. Forensic readiness enables the preservation of digital evidence such as ARP tables and network logs, aiding in identifying attack vectors and attributing them to specific actors. Insights from forensic analysis guide the improvement of security measures, strengthening the network's resilience against future attacks. Compliance with legal requirements, continuous improvement of incident response plans, and building trust with stakeholders are additional benefits of these practices.

Question 4

Part A

1. The development of rate limiting is a vitally important part in the strategy of keeping DNS fabulous about ECMM464 Inc. in the future, and it helps to declare DDoS attacks. This is where the number of requests to either individual users or continuously the IP addresses within a specific time frame drops significantly, and this prevents the attackers from overburdening the system. It makes sure that the attacks on these networks will not bring any ill consequences and, ultimately, protects the availability of services. Such a rate limit will contribute to effectively distinction of the dishonest activities shortly and will largely provide security. Besides that, it will guarantee just distribution of resources to legitimate users while at the same time not creating a bottleneck in the scenario of a cyber-attack. This must be done hand in hand with multicasting, DNS traffic for the distribution and those services for advanced threat identification will be provided. These services are coupled with

DDOS (Distributed Denial of Service) mitigation services for regular security checks will also be done. DDOS attack classifying by rate limitation in wholly DNS resilience framework for ECMM464 Inc. will augment their safety, immunization against DDoS attackers, and give them serenity to run in any location of the world.

2. Round-robin DNS -Load balancing is the process of dividing the traffic among the more than one server for performance improvement and to prevent the traffic's absence in some part of the net. A variety of node and network level methods of load balancing can be employed by organizations to speed up both websites and private networks. Load balancing in the Internet world is a foundation without which, most applications and websites would work poorly or not at all. the most widely used example load balancing DNS techniques is called round-robin DNS. Round robin DNS possesses a viable long-term solution that fortifies the system resilience against DNS attacks and beyond. This method just like load balancers of past, achieve the same output by using authoritative nameservers to distribute traffic across numerous servers. The round-robin DNS allots to each server a different IP address in DNS manner, virtually “rotating” them with each query and in a sequential manner. For example, where there are five different IP addresses, the DNS query will cycle the return, so that traffic will route to each one, evenly and equally.
   This will thin out the workload on each server individual, so just one of the servers will not get loads after requests as other servers are also working on it. Involved in this, it acts in a similar way that a company distributing mails through various PO boxes — for each client they map out the route, which suits PO Box number in a sequential manner.

Part B

1. MFA (Multi-Factor Authentication) should be deployed to hinder the chances of falling prey to DNS hijacking. Although it is the most guaranteeing security layer, it can also become complex and difficult to monitor, especially for the institutions that are deficient in information technologies. Proper planning is paramount and should prepare the user for no inconvenience including lockouts. This could be achieved by, for example, through ensuring interoperability of various sources. However, the strong side of MFA results in the increase of user safety (ex. protection against fraudulent access violation). A major difficulty is in creating a good harmony of security and convenience, thus, is protects DNS from DNS attacks, privacy of data, and secure access to vital systems.

2. The domain account can be registered with the complement of Registry Lock to upgrade the security further against DNS hijacking Registry Lock embodies an additional safety sleeve. It requires manual confirmation and approval for any changes within the domain settings, including DNS records. Through this, any malicious attempts at modifying the original DNS that may arise out of a DNS session hijacking is prevented. MFA and Registry Lock are example of the combination of methods that will form ECMM464 Inc. defence system, that will secure DNS infrastructure and domain name.

3. Another crucial step to prevent DNS hijacking is to restrict zone transfers. This security measure limits the ability of unauthorized parties to obtain sensitive DNS information, reducing the risk of attackers gathering data needed for a successful hijack. By controlling which servers can perform zone transfers, organizations mitigate the risk of DNS enumeration, zone poisoning, and unauthorized access to DNS data.

PART C

1. Encryption of DNS –

Implementing DNS with DNS over TLS (DoT) and DNS Queries over HTTPS (DoH) encryption is necessary for suppressing the effect of the DNS cache poisoning attacks. DoT uses encrypted TLS channel and transfers DNS packet, thereby protecting the packet from attempts of eavesdropping and tampering during transit. It verifies the authenticity of the server through the use of certificates; preventing the attacker from impersonating a different server. Similarly, DoH encapsulates DNS queries into a protected HTTPS flow and uses the popular tcp/443 port to handle any possible blocking issues. Similarly, it blocks devices from the main route to DNS requests reducing security vulnerabilities. Enforcing DoT or DoH, ECMM464 Inc. eliminates the threat of DNS cache poisoning, so the DNS data can be kept intact and encrypted. By using these encrypting protocols, only authorized DNS resolvers can be able to respond to the asked query, hence the chances of being maliciously directed to an unsafe website are significantly reduced. The reinforcing in DNS security with DoT or DoH equalizing ECMM464 Inc's infrastructure against DNS cache poisoning and leading more user privacy and trust in DNS resolution.

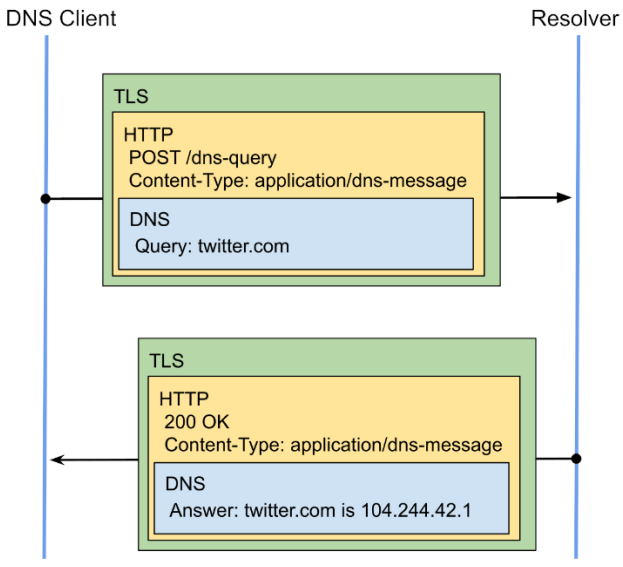


Fig- DoH: DNS query and response transported over a secure HTTPS stream

2. Flushing the DNS cache-

our computer holds the recently visited webpage addresses and their respective IP in the temp database structures called DNS cache. This cache accelerates the process of searching for your computer by avoiding the process of contacting the DNS server again, when you want to visit a particular website.

Clearing the cache does not prevent poisoning directly, but it removes all potentially grave entries the attacker might have found to exploit. This way, your computer will utilize the latest DNS data for website address resolution and it will be highly responsible in the case of a previous poisoning.

PART D

DNSSEC –

DNSSEC works to protect the internet community from forged Domain Name System (DNS) data by using public key cryptography to digitally sign authoritative zone data. DNSSEC validation helps to assure users that the data originated from the stated source and that it was not modified in transit. DNSSEC also can prove that a domain name does not exist.

DNSSEC, or Domain Name System Security Extensions, offers a powerful solution for addressing internal DNS misconfigurations within ECMM464 Inc.'s infrastructure. This protocol provides a range of benefits that significantly bolster the security of DNS servers and the overall integrity of the domain name system. One of the primary advantages of DNSSEC is its ability to ensure data integrity through cryptographic authentication. By utilizing digital signatures to sign DNS records, DNSSEC safeguards against unauthorized modifications or tampering of DNS data, whether due to misconfigurations within the system or malicious attacks.

A critical concern for any organization's DNS infrastructure is the risk of DNS spoofing attacks, where incorrect DNS data can lead users to malicious websites. DNSSEC serves as a potent defence against such attacks by verifying the authenticity of DNS responses using cryptographic signatures. This validation ensures that only legitimate responses from authoritative servers are accepted, effectively preventing users from being redirected to rogue websites. Additionally, DNSSEC plays a vital role in mitigating the risks associated with DNS cache poisoning, a technique used by attackers to corrupt the cache of a DNS resolver with false information. With DNSSEC, resolvers can validate the authenticity of DNS responses and reject any tainted data, preserving the integrity of the DNS resolution process.

The implementation of DNSSEC involves the use of cryptographic key pairs for authentication and validation purposes. Each authoritative name server maintains a key pair comprising a private key and a corresponding public key. The private key is used to sign DNS records, while the public key is employed by resolvers to verify the authenticity of these signed records. To further enhance security, DNSSEC introduces the concept of a Key-Signing-Key (KSK) pair, providing an additional layer of authentication.

In conclusion, the adoption of DNSSEC by ECMM464 Inc. represents a proactive and robust approach to addressing internal DNS misconfigurations and enhancing overall security. By providing cryptographic authentication, preventing DNS spoofing and cache poisoning, and establishing a secure

chain of trust, DNSSEC significantly strengthens the integrity and reliability of the organization's DNS infrastructure, safeguarding critical services and internal resources from potential cyber threats.

References:

C. Manusankar, S. Karthik and T. Rajendran, "Intrusion Detection System with packet filtering for IP Spoofing," 2010 International Conference on Communication and Computational Intelligence (INCOCCI), Erode, India, 2010, pp. 563-567.

https://www.academia.edu/13998260/IP_Spoofing_and_Sniffing

Wireshark user guide – https://www.wireshark.org/download/docs/Wireshark%20User%27s%20Guide.pdf

https://www.manageengine.com/products/eventlog/logging-guide/firewall/how-to-detect-and-prevent-tcp-445-exploit-and-attack.html

US-CERT Federal Incident Notification Guidelines
https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf

Computer Security Incident Handling Guide
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Y. P. Atmojo, I. M. D. Susila, I. B. Suradarma, L. Yuningsih, E. S. Rini and D. P. Hostiadi, "A New Approach for ARP Poisoning Attack Detection Based on Network Traffic Analysis," 2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 2021, pp. 18-23, doi: 10.1109/ISRITI54043.2021.9702860.

Sakhawat, D., Khan, A.N., Aslam, M. and Chronopoulos, A.T. (2019), Agent-based ARP cache poisoning detection in switched LAN environments. IET Netw., 8: 67-73. https://doi.org/10.1049/iet-net.2018.5084

Understanding and Using Dynamic ARP Inspection (DAI)
https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/topic-map/understanding-and-using-dai.html

DNS Encryption Explained - https://blog.cloudflare.com/dns-encryption-explained/

DNSSEC explained: Why you might want to implement it on your domain- https://www.csoonline.com/article/569685/dnssec-explained-why-you-might-want-to-implement-it-on-your-domain.html