**900103-000-00-KM-02, Cyber Threats and Attacks, NQF Level 4, Credits 7**

**LEARNER GUIDE**

**MODULE TWO (2)**

|  |  |
| --- | --- |
| **Module #** | 900103-000-00-KM-02 |
| **NQF Level** | 4 |
| **Notional hours** | 70 |
| **Credit(s)** | 7 |
| **Occupational Code** | 900103-000-00-00 |
| **SAQA QUAL ID** | SP - 220330 |
| **Qualification Title** | Cybersecurity Defender |

|  |  |
| --- | --- |
| **Name** |  |
| **Contact Address** |  |
| **Telephone (H)** |  |
| **Telephone (W)** |  |
| **Facsimile** |  |
| **Cellular** |  |
| **E-mail** |  |

**Note to the learner**

This Learner Guide provides a comprehensive overview of the module. It is designed to improve the skills and knowledge of learners, and thus enabling them to effectively and efficiently complete specific tasks.

**Purpose of the Module**

The main focus of the learning in this knowledge module is to build an understanding of the categories of cyber threats and attacks and which counter measures can be implemented to avoid or prevent breaches and attacks

The learning will enable learners to demonstrate an understanding of:

* KM-02-KT01 : Social engineering 35%
* KM-02-KT02 : Physical vulnerability and security 33%
* KM-02-KT03 : Malware and ransomware

**Entry Requirements**

NQF 3 (Gr 11) with Computer Literacy, English and Math Lit

**Provider Accreditation Requirements for the Knowledge Module**

*Physical Requirements:*

* The provider must have lesson plans and structured learning material or provide learners with access to structured learning material that addresses all the topics in all the knowledge modules as well as the applied knowledge in the application modules
* QCTO/ MICT SETA requirements

*Human Resource Requirements:*

* Lecturer/learner ratio of 1:20 (Maximum)
* Qualification of lecturer (SME):

NQF 5 qualified in industry recognised qualifications with 1 years’ experience in the IT industry

Cybersecurity vendor certification

* Assessors and moderators: accredited by the MICT SETA

*Legal Requirements:*

* Legal (product) licences to use the software for learning and training
* OHS compliance certificate
* Ethical clearance (where necessary)

AM

*Physical Requirements:*

* Valid licenses software and application, including OS.
* Internet connection and hardware availability.
* Examples and information specified in the scope statement and all the case studies, scenarios and access to hardware and software implied in the scope statements of the modules.
* Remote learners: Provider must provide business IT simulation system (e.g. invoice processing).

*Human Resource Requirements:*

* Qualification of lecturer (SME):  
  o NQF 5 industry recognised qualification with 1 year relevant experience
* Assessors and moderators: accredited by the MICT SETA

*Legal Requirements:*

* + Legal (product) licences to use the software for learning and training
  + OHS compliance certificate
  + Ethical clearance (where necessary)

**Venue, Date and Time:**

Consult your facilitator should there be any changes to the venue, date and/or time.

Refer to your timetable.

**Assessments**

**Associated Assessment Criteria (AACs)**

* Basic governance principles and concepts related to cybersecurity are understood.
* Basic concepts and principles of cybersecurity are understood.
* Basic concepts and principles of cyber threats and attacks are understood.
* Basic concepts and principles of cyber defence are understood.
* Ethical considerations in ethical hacking and penetration testing are understood.
* Procedures to respond to cybersecurity incidents are understood.

**Associated Assessment Criteria (AACs)**

* User and host identities are verified.
* Mechanisms are put in place to prevent system intrusions.
* Automated tools are used to guard against intrusions.
* Network confidentiality is ensured.
* The security posture is evaluated to detect vulnerabilities and to enhance resilience.

**Associated Assessment Criteria (AACs)**

* Threats to the cybersecurity of the company are detected.
* Adversary techniques, tactics and practices (TTPs) are emulated
* using an emulation platform.
* Network traffic is monitored and analysed using a suitable platform.
* Incidents are identified, responded to and reported.

**Associated Assessment Criteria (AACs)**

* Foot-printing tools are used against a target and intelligence is gathered.
* Vulnerabilities are identified using penetration testing tools.
* Servers and devices are attacked to build better defences.
* Clients are manipulated to uncover internal threats.
* Targets are exploited to increase cybersecurity.

Antivirus and intruder detection systems (IDS) are tested

# PURPOSE OF THE QUALIFICATION

Cybersecurity Defenders are responsible for proactively protecting organisations’ systems from attacks, they are the first line of defence against cyberattacks, the first responders to cybersecurity breaches and are responsible for the hardening of the information systems of organisations ensuring compliance with legislation

# QUALIFICATION RULES

This Skills Programme consist of two components namely Knowledge/Theory component and Application component. The following are compulsory modules in each of the two components:

**Knowledge/Theory Component:**

The following Modules are compulsory:

* 900103-000-00-KM-01, Cyber Defence Introduction, NQF Level 4, Credits 7
* 900103-000-00-KM-02, Cyber Threats and Attacks, NQF Level 4, Credits 7
* 900103-000-00-KM-03, Cybersecurity, NQF Level 4, Credits 7
* 900103-000-00-KM-04, Responding to Cybersecurity Incidents, NQF Level 4, Credits 5

Total number of credits for Knowledge Component: 26

**Application Component:**

* 900103-000-00-PM-01, Protect against cybersecurity threats, intrusions and attacks, NQF Level 4, Credits 11
* 900103-000-00-PM-02, Detect cybersecurity threats, intrusions and attacks, NQF Level 4, Credits 11
* 900103-000-00-PM-03, Conduct Penetration Testing Techniques to Determine Security, NQF Level 4, Credits 12

Total number of credits for Application Component: 34

# EXIT LEVEL OUTCOMES

**Exit Level Outcomes (ELO) 1**

Demonstrate knowledge and understanding of cybersecurity, cyber

threats and attacks and cyber defence

**Exit Level Outcomes (ELO) 2**

Protect against cybersecurity intrusions and attacks

**Exit Level Outcomes (ELO) 3**

Detect cybersecurity threats and attacks

**Exit Level Outcomes (ELO) 4**

Use different penetration testing tools to identify vulnerabilities in the security posture of an organisation

# KM-02-KT01: Social engineering 35%

**Topic elements to be covered include:**

* KT0101 Social engineering attacks and the educated internet user
* KT0102 Commonly used attacks
* KT0103 Pharming attacks
* KT0104 Exploitation of personal information on the internet
* KT0105 Whaling works
* KT0106 Insider attacks

**KT0101 Social engineering attacks and the educated internet user**

Social engineering attacks are deceptive tactics used by cybercriminals to manipulate and exploit human psychology rather than directly targeting technical vulnerabilities. These attacks aim to trick individuals into revealing sensitive information, performing certain actions, or providing access to protected systems. Even educated internet users can fall victim to social engineering attacks, as the attacks often exploit psychological and emotional triggers, making them highly effective. Here's how social engineering attacks can target educated internet users:

1. **Phishing**: Phishing is one of the most common social engineering attacks. Cybercriminals send deceptive emails, messages, or websites that appear legitimate, imitating trusted entities like banks, service providers, or government agencies. Educated users might be aware of phishing threats, but attackers continually refine their techniques to make the emails look more convincing, increasing the chances of success.
2. **Spear Phishing**: Spear phishing is a more targeted form of phishing, where attackers personalize their messages based on information gathered about the victim. For educated users who share a lot of personal information online, attackers can craft sophisticated and convincing spear-phishing emails that seem highly relevant.
3. **Pretexting**: In pretexting attacks, the attacker fabricates a scenario or pretext to gain the target's trust and extract sensitive information. Educated users might be cautious about sharing sensitive data but could be convinced by a well-crafted pretext that appears credible.
4. **Baiting**: Baiting attacks involve luring users into downloading malware or revealing information by enticing them with something of value, such as a free software download or a tempting offer. Even educated users might be curious or enticed by an attractive bait.
5. **Quizzes and Surveys**: Social media quizzes and surveys can be used to harvest personal information about users. Educated users may not immediately recognize the potential risks of participating in these seemingly harmless activities.
6. **Impersonation**: Attackers may impersonate authority figures, colleagues, or service providers to manipulate educated users into complying with their requests. The sense of authority might override skepticism in such cases.
7. **Urgency and Fear**: Attackers often create a sense of urgency or fear to pressure users into quick action, bypassing their critical thinking. Even educated users might react impulsively when facing urgent situations.
8. **Publicly Available Information**: Educated users who are active on social media or have an online presence might unknowingly share valuable information that attackers can use to customize their social engineering attacks.

To protect themselves from social engineering attacks, even educated internet users should:

* Be skeptical of unsolicited messages, especially those asking for sensitive information or immediate action.
* Verify the identity of individuals or organizations making requests before sharing sensitive information or performing tasks.
* Be cautious when clicking on links or downloading attachments in emails, particularly from unknown sources.
* Regularly update passwords and use multi-factor authentication for added security.
* Educate themselves about the latest social engineering tactics and stay informed about cybersecurity best practices.

Ultimately, cyber awareness and a healthy dose of skepticism are essential for all internet users, regardless of their level of education or technical knowledge, to defend against social engineering attacks effectively.

**KT0102 Commonly used attacks**

Social engineering attacks are diverse and take advantage of human psychology to manipulate individuals into divulging sensitive information or performing actions that benefit the attacker. Here are some commonly used social engineering attacks:

1. **Phishing**: In phishing attacks, attackers send deceptive emails or messages that appear to be from trusted sources, such as banks, online services, or colleagues. The goal is to trick the recipient into clicking on malicious links, downloading malware, or revealing login credentials.
2. **Spear Phishing**: Similar to phishing, spear phishing targets specific individuals or organizations. Attackers customize their messages based on information gathered about the target to make the attack more convincing.
3. **Pretexting**: Pretexting involves creating a fabricated scenario or pretext to gain the target's trust and elicit sensitive information. Attackers may pose as someone with authority or a legitimate reason to request data.
4. **Baiting**: Baiting attacks entice users into taking specific actions by offering something of value, such as a free software download, movie, or gift card. In return, the user unknowingly downloads malware or provides sensitive information.
5. **Quizzes and Surveys**: Social media quizzes and surveys may seem harmless but can be used to collect personal information about users, which attackers can exploit.
6. **Impersonation**: Attackers impersonate trusted individuals, such as IT support personnel, colleagues, or company executives, to convince targets to reveal sensitive data or perform certain tasks.
7. **Watering Hole Attack**: In this attack, the attacker infects websites that are frequently visited by the target audience. When users visit these compromised sites, they may unknowingly download malware or become victims of other attacks.
8. **Tailgating (Piggybacking)**: In physical social engineering attacks, an attacker gains unauthorized access to a restricted area by following closely behind an authorized person. For example, an attacker may enter a building by pretending to be an employee and holding the door open after someone else has used their access card.
9. **Quid Pro Quo**: Attackers promise something in return for the target's cooperation. For example, an attacker may pose as a technical support agent and offer to help the target resolve an issue in exchange for access to their system.
10. **Diversion Theft**: In this attack, the attacker creates a diversion to distract the target's attention while stealing valuable information or belongings.
11. **Scareware**: Scareware involves tricking users into believing their systems are infected with malware or other threats, prompting them to purchase fake antivirus software or pay for unnecessary services.
12. **Vishing (Voice Phishing)**: Vishing uses phone calls to deceive targets into providing sensitive information over the phone.

Social engineering attacks can be highly effective because they exploit human behavior and emotions rather than technical vulnerabilities. Awareness, education, and a healthy dose of skepticism are essential for individuals and organizations to defend against these types of attacks effectively.

**KT0103 Pharming attacks**

Pharming is a type of cyber attack that involves redirecting website traffic to a fraudulent or malicious website without the user's knowledge or consent. In a pharming attack, attackers manipulate the domain name system (DNS) or compromise the user's local DNS settings to direct legitimate website requests to a malicious server. The goal of a pharming attack is to deceive users into visiting a fake website that appears identical to the legitimate site, with the intention of stealing sensitive information or spreading malware.

There are two main types of pharming attacks:

1. **DNS Pharming**: In DNS pharming, attackers tamper with the domain name resolution process. They might compromise the DNS server settings or inject malicious DNS records, causing legitimate domain name queries to be resolved to the attacker's IP address instead of the correct IP address of the legitimate website.
2. **Hosts File Pharming**: In hosts file pharming, attackers modify the "hosts" file on the victim's computer. The hosts file is a local file that maps domain names to IP addresses before the DNS resolution process. By altering this file, attackers redirect traffic for specific websites to malicious IP addresses.

The consequences of a successful pharming attack can be severe:

* **Identity Theft**: Attackers can use pharming to create fake login pages for banking or social media sites, tricking users into revealing their usernames and passwords.
* **Financial Fraud**: By redirecting users to fake e-commerce websites, attackers can capture payment card details and other sensitive financial information.
* **Malware Distribution**: Pharming attacks can also lead users to malicious websites that distribute malware, infecting their systems with viruses, ransomware, or other malicious software.
* **Reputation Damage**: If users unknowingly visit malicious websites, they might associate the negative experience with the legitimate organization whose website was impersonated.

To protect against pharming attacks, users and organizations can take the following measures:

1. **Use Secure Websites (HTTPS)**: Always access websites using the "https://" protocol, as it encrypts communications between the user and the website, making it harder for attackers to intercept data.
2. **Keep Software Updated**: Ensure that operating systems, browsers, and security software are up to date with the latest patches to protect against known vulnerabilities.
3. **Verify Website URLs**: Manually type website URLs or use bookmarks instead of clicking on links in emails or messages.
4. **Use DNSSEC**: Domain Name System Security Extensions (DNSSEC) provide additional security measures to ensure the integrity of DNS data.
5. **Monitor DNS Settings**: Regularly check DNS settings and configurations for any unauthorized changes.
6. **Implement Network Security Measures**: Use firewalls, intrusion detection/prevention systems (IDS/IPS), and secure DNS services to enhance network security.
7. **Educate Users**: Train users about the risks of pharming attacks and how to recognize suspicious website behavior.

By adopting these preventive measures and remaining vigilant, users and organizations can reduce the risk of falling victim to pharming attacks and better protect their sensitive information and online activities.

**KT0104 Exploitation of personal information on the internet**

The exploitation of personal information on the internet is a significant concern in the digital age. With the proliferation of online services, social media platforms, and e-commerce websites, individuals share vast amounts of personal data. This data, when misused or obtained by malicious actors, can lead to various risks and consequences:

1. **Identity Theft**: Personal information, such as full names, addresses, social security numbers, and birth dates, can be used for identity theft, where attackers impersonate individuals to commit fraud, open accounts, or make unauthorized transactions.
2. **Financial Fraud**: Stolen personal information, including credit card details and bank account numbers, can be exploited for financial fraud, resulting in unauthorized charges and monetary losses.
3. **Phishing and Social Engineering**: Attackers use personal information to create convincing phishing emails or messages tailored to individuals, increasing the likelihood of success in tricking them into revealing sensitive data or login credentials.
4. **Online Harassment and Cyberbullying**: Personal information shared online can be used by malicious individuals to harass, intimidate, or cyberbully victims, causing emotional distress and harm.
5. **Data Breaches**: Companies and organizations may experience data breaches, leading to the exposure of customers' personal information. This can result in reputational damage for the affected entity and potential legal consequences.
6. **Profiling and Targeted Advertising**: Online platforms and advertisers collect personal data to build user profiles and target individuals with personalized ads. While this can improve user experience, it also raises concerns about privacy and data usage.
7. **Location Tracking**: Mobile devices and certain apps collect location data, which can be exploited to track individuals' movements, compromising their privacy and security.
8. **Social Media Risks**: Oversharing personal information on social media can make individuals vulnerable to scams, stalking, and identity theft.
9. **Healthcare Data Exploitation**: Personal health information is highly valuable to cybercriminals, who may exploit it for medical identity theft or sell it on the dark web.
10. **Employment Discrimination**: Employers or hiring managers may misuse personal information found online during the hiring process, leading to potential discrimination.
11. **Data Aggregation and Surveillance**: Companies may aggregate personal data from various sources to build detailed profiles, potentially eroding individual privacy.

To mitigate the exploitation of personal information on the internet, individuals can take the following steps:

* Be cautious about sharing sensitive information online and limit what is posted on public platforms.
* Use strong, unique passwords and enable multi-factor authentication for online accounts.
* Regularly review privacy settings on social media and online accounts.
* Be wary of phishing attempts and suspicious emails or messages requesting personal information.
* Use virtual private networks (VPNs) and secure Wi-Fi networks to protect data while online.
* Regularly monitor financial accounts and credit reports for unauthorized activity.
* Install reputable security software and keep devices and software up to date with the latest patches.

Overall, understanding the risks associated with sharing personal information on the internet and practicing good cybersecurity habits are essential in safeguarding against exploitation and maintaining online privacy and security.

**KT0105 Whaling works**

Whaling, also known as CEO fraud or business email compromise (BEC), is a social engineering attack targeting high-profile individuals within organizations, such as CEOs, executives, or senior management. This type of attack is highly sophisticated and aims to deceive the target into taking specific actions that benefit the attacker. Here's how whaling works:

1. **Research and Reconnaissance**: Attackers conduct extensive research on the target and the organization. They gather information from publicly available sources, social media, company websites, and other online platforms to understand the target's role, communication style, and potential weaknesses.
2. **Spoofing Email Addresses**: The attacker uses various techniques to spoof the sender's email address, making it appear as if the email is coming from a trusted source within the organization, such as the CEO or a high-ranking executive.
3. **Impersonation**: The attacker impersonates the high-profile target to gain the trust of the recipient. They may use a similar writing style, signature, or official language used by the target.
4. **Urgency and Authority**: Whaling attacks often involve urgent requests or demands for action, using language that implies the request is coming from a person of authority. This creates pressure on the recipient to respond quickly without questioning the legitimacy of the request.
5. **Fraudulent Requests**: The attacker's email typically contains a request for sensitive information, such as financial data, login credentials, or payment transfers. In some cases, they may ask the recipient to perform a financial transaction or approve a fund transfer.
6. **Deception and Manipulation**: The attacker uses psychological manipulation to exploit the recipient's trust in the high-profile target. They may create a sense of confidentiality or secrecy around the request to prevent the recipient from seeking verification from other colleagues.
7. **Lack of Verification**: Whaling attacks exploit the absence of proper verification mechanisms within organizations. The attacker relies on the recipient's willingness to comply without independently verifying the request through other means of communication.

Whaling attacks can be devastating for organizations as they target individuals with high-level access and authority, making it easier for attackers to bypass security measures. If successful, whaling attacks can result in significant financial losses, data breaches, reputational damage, and legal implications for the targeted organization.

To protect against whaling attacks, organizations should:

* Educate employees about the risks of whaling attacks and train them to recognize suspicious requests.
* Implement strict verification processes for any financial transactions or sensitive information requests.
* Enable multi-factor authentication for email and other critical systems to prevent unauthorized access.
* Encourage a culture of cybersecurity awareness and openness, where employees feel comfortable reporting suspicious emails or requests.
* Establish clear communication channels for verifying critical requests from high-profile individuals.

By being vigilant and implementing strong security practices, organizations can significantly reduce the risk of falling victim to whaling attacks and enhance their overall cybersecurity posture.

**KT0106 Insider attacks**

Insider attacks, also known as insider threats, occur when individuals with authorized access to an organization's systems, networks, or sensitive information misuse their privileges to carry out malicious activities. These individuals could be current or former employees, contractors, business partners, or anyone else with legitimate access. Insider attacks pose a significant risk to organizations, as insiders have valuable knowledge of the organization's operations and often bypass traditional security measures. There are different types of insider attacks:

1. **Malicious Insider Attacks**: These are intentional insider attacks where the individual deliberately carries out malicious activities, such as stealing sensitive data, sabotaging systems, or causing financial harm to the organization.
2. **Negligent Insider Actions**: Insider threats can also result from unintentional actions by employees who make errors that lead to security breaches or data leaks. These actions may be the result of carelessness, lack of awareness, or inadequate training.
3. **Compromised Insider Attacks**: In some cases, an insider may become unwittingly involved in an attack due to external factors, such as falling victim to phishing or social engineering, resulting in the compromise of their account.

Motivations for Insider Attacks:

* **Financial Gain**: Malicious insiders may seek financial gain through data theft, selling proprietary information, or conducting fraudulent activities.
* **Revenge or Disgruntlement**: Former or current employees with grudges against the organization may retaliate through insider attacks.
* **Espionage**: Insiders may be recruited by external entities to steal sensitive information for competitive advantage or to support nation-state interests.
* **Curiosity or Challenge**: Some insiders may engage in unauthorized activities out of curiosity or to demonstrate their hacking skills.

Detecting and Preventing Insider Attacks:

* **User Behavior Monitoring**: Implementing user behavior analytics and monitoring can help identify suspicious activities or deviations from normal user behavior.
* **Access Controls**: Limiting access privileges based on the principle of least privilege can prevent insiders from accessing sensitive information unnecessarily.
* **Security Awareness Training**: Educate employees about the risks of insider threats and the importance of reporting suspicious behavior.
* **Background Checks**: Conduct thorough background checks on new employees and contractors to identify any potential red flags.
* **Data Loss Prevention (DLP) Solutions**: Deploy DLP solutions to prevent unauthorized data exfiltration and ensure data protection.
* **Regular Auditing and Review**: Conduct regular audits of user activities and review access logs to identify any abnormal behavior.
* **Secure Termination Processes**: Implement strict processes to revoke access for employees who leave the organization to prevent disgruntled insiders from causing harm.

Combining these prevention and detection measures can significantly reduce the risk of insider attacks and protect an organization's sensitive information and resources. However, it is essential to strike a balance between security measures and maintaining a positive work environment that fosters trust and cooperation among employees.

***Internal Assessment Criteria and Weight***

* IAC0101 Vulnerabilities related to social engineering are defined.
* IAC0102 Various types of attacks related to social engineering are listed and described in terms of method of attack and how severe it is.
* IAC0103 Counter measures are described in terms of application and success.

***(Weight 35%)***

# KM-02-KT02 : Physical vulnerability and security 33%

**Topic elements to be covered include:**

* KT0201 Different attacks to gain access to the organization
* KT0202 Popular file formats used for cyber attacks
* KT0203 Comparison of anti-virus and firewall systems
* KT0204 Definition of confidential information
* KT0205 Patch management and updates

**KT0201 Different attacks to gain access to the organization**

Attackers use various methods to gain unauthorized access to an organization's systems, networks, and sensitive information. Here are some common attacks used to breach organizational defenses:

1. **Phishing**: Phishing is a social engineering attack where attackers send deceptive emails or messages to trick employees into revealing login credentials or clicking on malicious links. It's one of the most prevalent attack vectors.
2. **Spear Phishing**: Similar to phishing, spear phishing targets specific individuals within the organization, often high-profile employees, using personalized and convincing messages.
3. **Password Attacks**: These attacks involve using techniques like brute force attacks, dictionary attacks, or credential stuffing to guess or steal user passwords and gain unauthorized access.
4. **Malware**: Attackers use various types of malware, such as viruses, trojans, and ransomware, to infect systems and gain control over the organization's network or steal sensitive data.
5. **Man-in-the-Middle (MitM) Attack**: In a MitM attack, the attacker intercepts communication between two parties, e.g., the user and a server, to eavesdrop, modify data, or steal information.
6. **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks**: These attacks overload an organization's systems or network resources, disrupting services and making them inaccessible to legitimate users.
7. **Insider Threats**: As mentioned earlier, malicious or negligent insiders with authorized access can cause significant harm to an organization's security.
8. **SQL Injection (SQLi)**: SQLi attacks exploit vulnerabilities in web applications that allow attackers to inject malicious SQL code and gain unauthorized access to databases.
9. **Cross-Site Scripting (XSS)**: XSS attacks inject malicious scripts into web applications viewed by other users, enabling attackers to steal session cookies or user data.
10. **Zero-Day Exploits**: Attackers target unpatched or previously unknown vulnerabilities (zero-days) in software or operating systems to gain access before a fix is available.
11. **Physical Attacks**: Physical security breaches, such as unauthorized entry, can provide attackers with direct access to an organization's assets and infrastructure.
12. **USB Dropping**: Attackers leave infected USB drives in areas accessible to employees, hoping that someone will plug them into a computer, spreading malware.
13. **Watering Hole Attacks**: Attackers compromise websites frequented by employees, infecting them with malware to target specific organizations.
14. **Wi-Fi Hacking**: Attackers set up rogue Wi-Fi networks to intercept data transmitted by employees using unsecured Wi-Fi connections.
15. **Bypassing Authentication**: Attackers exploit misconfigurations or vulnerabilities to bypass authentication mechanisms and gain unauthorized access.

To defend against these attacks, organizations must implement a robust cybersecurity strategy, including:

* Educating employees about security best practices and the risks of social engineering attacks.
* Implementing multi-factor authentication (MFA) to enhance login security.
* Regularly updating and patching software and systems.
* Deploying strong network security measures, firewalls, and intrusion detection/prevention systems.
* Conducting regular security assessments and audits to identify vulnerabilities.
* Restricting access based on the principle of least privilege.
* Monitoring network traffic and user behavior for suspicious activities.

By staying vigilant and proactive, organizations can better protect their assets and sensitive information from unauthorized access and cyber threats.

**KT0202 Popular file formats used for cyber attacks**

Cyber attackers often use various file formats to deliver and execute malicious payloads on target systems. The choice of file format depends on the specific attack vector and the intended target. Some popular file formats used for cyber attacks include:

1. **Executable Files (.exe)**: Executable files are common carriers of malware, including viruses, trojans, ransomware, and other malicious software. Attackers often disguise malware as legitimate-looking executable files to trick users into running them.
2. **Microsoft Office Documents (.doc, .docx, .xls, .xlsx, .ppt, .pptx)**: Office documents can contain macros or embedded scripts that, when executed, download and install malware on the system. Malicious macros are often used in phishing campaigns.
3. **JavaScript Files (.js)**: JavaScript files can be used to deliver malicious scripts that exploit vulnerabilities in web browsers or execute drive-by download attacks.
4. **PDF Files (.pdf)**: PDF files can be used to deliver malware through embedded scripts or malicious links. Exploiting vulnerabilities in PDF readers can also allow attackers to execute code.
5. **ZIP and Archive Files (.zip, .rar)**: Attackers use archive files to package and deliver multiple files, including malware or malicious scripts. Sometimes, the archive file is password-protected to evade detection.
6. **HTML Files (.html)**: HTML files can be used for phishing attacks, where users are redirected to fake login pages or websites designed to steal their credentials.
7. **Shortcut Files (.lnk)**: Shortcut files can be used in shortcut-spoofing attacks, where the shortcut icon appears legitimate, but it points to a malicious executable or script.
8. **Java Archive Files (.jar)**: Java files can carry Java-based malware, and attackers may use Java exploits to compromise systems.
9. **Flash Files (.swf)**: Flash files may contain malicious Flash scripts or vulnerabilities that attackers exploit to deliver malware.
10. **Batch Files (.bat)**: Batch files can execute a series of commands and are sometimes used to download and run malware on the system.
11. **Shell Script Files (.sh)**: Shell scripts can be used in Unix-like systems to execute malicious commands or download and install malware.
12. **DLL Files (.dll)**: Dynamic Link Libraries (DLLs) can be manipulated to load malicious code into legitimate applications, enabling attackers to execute arbitrary commands.

It's important to note that these file formats are not inherently malicious, and they are widely used for legitimate purposes as well. However, cybercriminals exploit the functionalities and vulnerabilities of these file formats to carry out their attacks. To protect against such attacks, users and organizations should maintain up-to-date security software, follow best practices for safe browsing and email usage, and be cautious when opening files from unknown or untrusted sources. Additionally, implementing strong security measures and conducting regular security training for employees can help mitigate the risks associated with these file formats.

**KT0203 Comparison of anti-virus and firewall systems**

Anti-virus and firewall systems are both essential components of a comprehensive cybersecurity strategy, but they serve different purposes and provide distinct layers of protection. Here's a comparison of anti-virus and firewall systems:

**1. Purpose:**

* **Anti-virus (AV) Systems**: Anti-virus software is designed to detect, prevent, and remove malicious software (malware) such as viruses, trojans, worms, ransomware, and spyware. It focuses on identifying and eliminating specific patterns and signatures associated with known malware.
* **Firewall Systems**: Firewalls act as a barrier between a trusted internal network (like an organization's network) and untrusted external networks (like the internet). They control incoming and outgoing network traffic based on predetermined security rules to block potentially malicious connections and unauthorized access.

**2. Functionality:**

* **Anti-virus (AV) Systems**: AV systems primarily scan files, programs, and email attachments for known malware signatures. Some advanced AV solutions also use heuristics and behavior analysis to identify previously unknown threats.
* **Firewall Systems**: Firewalls examine network packets and data streams to enforce access control policies. They can block or allow traffic based on source and destination IP addresses, ports, protocols, and other characteristics.

**3. Detection Method:**

* **Anti-virus (AV) Systems**: AV relies on signature-based detection, where known patterns of malware are compared against files and processes. Some AV solutions also use behavioral analysis to detect suspicious activities.
* **Firewall Systems**: Firewalls use rule-based detection to determine whether network traffic is allowed or denied based on predefined policies.

**4. Scope of Protection:**

* **Anti-virus (AV) Systems**: AV primarily protects against malware that is stored on the computer's storage or runs as executable files. It may not be as effective against sophisticated or zero-day threats for which no signatures are available.
* **Firewall Systems**: Firewalls protect against unauthorized network traffic, helping to prevent external attackers from gaining access to the internal network. They can also help in controlling outgoing traffic to some extent.

**5. Deployment:**

* **Anti-virus (AV) Systems**: Anti-virus software is typically installed on individual computers or devices and may be centrally managed in enterprise environments.
* **Firewall Systems**: Firewalls are deployed at the network perimeter, such as between an internal network and the internet, and can be physical appliances or software-based solutions.

**6. Complementary Role:**

* **Anti-virus (AV) Systems**: AV complements the firewall by focusing on the detection and removal of malware that has already entered the system. It helps protect against malware spreading through file transfers and email attachments.
* **Firewall Systems**: Firewalls complement AV by preventing unauthorized access to the network and stopping threats before they reach individual devices. They can also block outbound connections from infected devices, preventing malware from communicating with command-and-control servers.

**7. Interoperability:**

* **Anti-virus (AV) Systems**: AV can be used alongside firewalls to provide layered protection, as they address different aspects of cybersecurity.
* **Firewall Systems**: Firewalls can work in conjunction with AV and other security tools to provide comprehensive defense against a wide range of threats.

In conclusion, anti-virus and firewall systems play complementary roles in cybersecurity. Anti-virus software focuses on identifying and removing malware from individual devices, while firewalls act as a barrier to control and monitor network traffic between trusted and untrusted networks. Combining these two security measures provides a stronger defense against various cyber threats.

**KT0204 Definition of confidential information**

Confidential information refers to sensitive and private data that is intended to be kept secret and protected from unauthorized access, use, or disclosure. This information is typically considered valuable and critical to an individual, organization, or entity, and its exposure or compromise can lead to various negative consequences.

Confidential information can take different forms, including but not limited to:

1. **Personal Identifiable Information (PII)**: This includes data that can be used to identify an individual, such as their name, address, Social Security number, driver's license number, financial account details, and medical records.
2. **Business Trade Secrets**: Trade secrets are confidential business information, such as proprietary formulas, manufacturing processes, marketing strategies, customer lists, or unique product designs that give a company a competitive advantage.
3. **Intellectual Property (IP)**: Intellectual property refers to intangible assets, such as patents, trademarks, copyrights, and trade secrets, which require protection from unauthorized use or disclosure.
4. **Financial Information**: Confidential financial data includes company financial statements, budget information, investment plans, and revenue forecasts.
5. **Legal Documents**: Legal contracts, non-disclosure agreements (NDAs), and other legal documents that contain sensitive terms or confidential clauses.
6. **Research and Development (R&D) Data**: Sensitive R&D data, such as ongoing research, experimental findings, and prototypes, is typically considered confidential to protect innovation and prevent competitors from gaining an advantage.
7. **Customer and Client Information**: Information about customers and clients, including contact details, purchase history, and preferences, is often considered confidential and protected under privacy laws.
8. **Government Classified Information**: Governments classify certain information as confidential to safeguard national security or diplomatic interests.

The classification of confidential information may vary depending on the industry, organization, or legal requirements. Companies and individuals must take appropriate measures to safeguard this information from unauthorized access, disclosure, or theft. These measures may include implementing access controls, encryption, secure storage, and regular employee training on handling confidential data. Non-disclosure agreements (NDAs) are also commonly used to legally protect confidential information shared between parties.

**KT0205 Patch management and updates**

Patch management and updates are crucial components of a comprehensive cybersecurity strategy aimed at maintaining the security and integrity of software, operating systems, and applications. These processes involve regularly applying updates, patches, and fixes to address vulnerabilities, bugs, and known security issues in software products. Here's an overview of patch management and updates:

**Patch Management:** Patch management refers to the process of identifying, acquiring, testing, and deploying software updates and patches to systems within an organization. The primary goal of patch management is to keep software up to date with the latest security fixes and improvements to prevent exploitation by cyber threats.

The patch management process typically involves the following steps:

1. **Patch Identification**: Organizations identify software products, applications, and operating systems that require updates. This can be done by monitoring vendor websites, security advisories, and vulnerability databases.
2. **Patch Acquisition**: Once patches are identified, organizations obtain the necessary updates directly from the software vendors or trusted sources. It is essential to download patches from official sources to avoid potential security risks from downloading patches from unauthorized or compromised locations.
3. **Patch Testing**: Before deploying patches across the entire network, it is crucial to test them in a controlled environment or on a limited number of systems. This helps ensure that the patches do not cause any compatibility issues or unintended consequences.
4. **Patch Deployment**: After successful testing, patches are deployed across the organization's systems. This can be done manually or automated using patch management tools or systems.
5. **Monitoring and Verification**: Organizations continually monitor their systems to ensure that patches are applied successfully and have not introduced any new issues. Regular verification and auditing are important to maintain a secure and up-to-date environment.

**Software Updates:** Software updates refer to the release of newer versions of software or applications that include feature enhancements, bug fixes, performance improvements, and security updates. Updates are released to provide users with the latest features and functionalities while also addressing any known vulnerabilities or issues.

Unlike patches that focus on specific security fixes, software updates often encompass a broader range of changes. Updating software regularly helps ensure that users can benefit from new features and security improvements while maintaining compatibility with the latest technologies.

**Importance of Patch Management and Updates:** Effective patch management and regular software updates are critical for several reasons:

* \*\*Security: Patching vulnerabilities promptly helps prevent cyberattacks that target known weaknesses in software.
* \*\*Stability: Updates and patches can improve software stability and performance, reducing crashes and system errors.
* \*\*Compatibility: Keeping software up to date ensures compatibility with other applications and systems.
* \*\*Compliance: Many industries and regulatory frameworks require organizations to maintain updated software for compliance purposes.
* \*\*Feature Enhancements: Software updates often bring new features and functionalities that enhance user experience and productivity.

By prioritizing patch management and software updates, organizations can significantly reduce their exposure to security risks, enhance system stability, and ensure that their software remains optimized and secure.

***Internal Assessment Criteria and Weight***

* IAC0201 Physical vulnerabilities and security are defined.
* IAC0202 Various types of attacks related to physical vulnerabilities are listed and described in terms of method of attack, how severe it is and how it can be prevented.
* IAC0203 Counter measures are described in terms of application and success.

***(Weight 33%)***

# KM-02-KT03 : Malware and ransomware 32%

**Topic elements to be covered include:**

* KT0301 Patient zero and the spread of ransomware across an entire company
* KT0302 Implications of ransomware attacks in everyday life
* KT0303 Typical threats, attacks and exploits used in cyber attacks
* KT0304 Rogue security software
* KT0305 Patch management and updates

**KT0301 Patient zero and the spread of ransomware across an entire company**

In the context of cybersecurity and ransomware attacks, "patient zero" refers to the first individual or system within a company or organization to become infected with ransomware. Patient zero is the point of origin from which the ransomware starts spreading throughout the network, infecting other systems and potentially causing widespread damage.

Here's how the spread of ransomware can occur across an entire company:

1. **Initial Infection**: The ransomware infection typically begins when an employee unknowingly opens a malicious email attachment, clicks on a malicious link, or visits a compromised website. This action triggers the ransomware to execute on the employee's computer, making them the patient zero.
2. **Lateral Movement**: Once the ransomware infects the patient zero's computer, it begins seeking other vulnerable systems within the company's network. It can use various techniques to move laterally through the network, such as exploiting unpatched vulnerabilities, leveraging stolen credentials, or taking advantage of weak network segmentation.
3. **Network Propagation**: The ransomware spreads rapidly, scanning for and infecting other connected systems, including servers, workstations, and shared network drives. It can also target other users within the same network to continue its propagation.
4. **Encryption and Ransom Demand**: As the ransomware infects additional systems, it encrypts files on each compromised device, making them inaccessible to users. After completing the encryption process, the ransomware displays a ransom note, demanding payment in cryptocurrency for the decryption key needed to restore the files.
5. **Potential Impact**: If the ransomware spreads undetected and quickly, it can cause significant disruptions to the company's operations. Critical data may be encrypted, affecting business continuity, productivity, and customer service.
6. **Detection and Response**: Ideally, the organization's security systems and monitoring mechanisms should detect the ransomware's activity early, allowing security teams to isolate infected systems and stop the spread. Quick response and containment are crucial to minimizing the impact of the attack.

Preventing the Spread of Ransomware:

To prevent ransomware from spreading across an entire company, organizations should implement a range of proactive security measures:

* **Employee Education**: Train employees about the risks of phishing emails, suspicious attachments, and malicious links to reduce the likelihood of patient zero occurrences.
* **Regular Backups**: Maintain secure and updated backups of critical data to avoid data loss in case of a ransomware attack.
* **Patch Management**: Keep all software, operating systems, and applications up to date with the latest security patches to mitigate vulnerabilities.
* **Network Segmentation**: Employ network segmentation to limit the lateral movement of ransomware and other malware within the network.
* **Strong Access Controls**: Implement robust access controls and least privilege principles to restrict unauthorized access to sensitive data and resources.
* **Intrusion Detection/Prevention Systems**: Deploy security solutions that can detect ransomware activity and suspicious behavior, triggering timely alerts to security teams.

By combining these preventive measures with a well-defined incident response plan, organizations can minimize the risk of ransomware spreading across their network and respond effectively if an attack occurs.

**KT0302 Implications of ransomware attacks in everyday life**

Ransomware attacks have significant implications on individuals, businesses, and society as a whole. These attacks disrupt normal operations, compromise sensitive data, and can lead to financial losses, emotional distress, and broader consequences for the affected individuals and communities. Here are some of the key implications of ransomware attacks in everyday life:

1. **Data Loss and Disruption**: Ransomware encrypts files and data, making them inaccessible to the victim. This can lead to data loss, including personal files, work documents, family photos, and other important information. The loss of critical data can disrupt personal and professional life, leading to frustration and stress.
2. **Financial Loss**: Ransomware attackers demand ransom payments to provide decryption keys and restore access to the encrypted data. Paying the ransom does not guarantee that the data will be recovered, and it fuels the cybercriminal ecosystem. Moreover, even if the ransom is paid, the victim may still suffer financial losses from downtime, recovery efforts, and potential reputational damage.
3. **Identity Theft and Privacy Concerns**: Some ransomware attacks steal sensitive personal information before encrypting data. This can lead to identity theft, where personal information is used for fraudulent activities such as opening accounts, making unauthorized transactions, or spreading further malware.
4. **Healthcare Impact**: Ransomware attacks on healthcare organizations can disrupt medical services, delay treatments, and compromise patient records. Patient care may be affected, and in critical situations, lives could be at risk.
5. **Educational Disruptions**: Ransomware attacks on educational institutions can disrupt online learning platforms, course materials, and student records. Students and educators may face difficulties accessing educational resources and participating in virtual classes.
6. **Small Business Vulnerabilities**: Small businesses may be particularly vulnerable to ransomware attacks due to limited resources and cybersecurity measures. An attack can severely impact their operations and financial stability.
7. **Cybersecurity Costs**: In response to ransomware attacks, individuals and organizations may need to invest in cybersecurity solutions, incident response plans, and staff training to enhance their defenses. These measures add additional costs to daily operations.
8. **Trust and Reputation**: Ransomware attacks can erode trust between customers, clients, and organizations. Individuals may become wary of conducting online transactions or sharing sensitive information, affecting e-commerce and online services.
9. **Economic Impact**: Widespread ransomware attacks can have broader economic consequences, affecting industries, supply chains, and overall economic stability. Businesses that suffer significant financial losses may be forced to reduce staff, leading to job losses and economic downturns in certain regions.
10. **Psychological Impact**: Ransomware attacks can cause emotional distress, anxiety, and feelings of vulnerability and violation. Victims may experience a loss of control over their personal data and privacy.

To mitigate the implications of ransomware attacks, individuals and organizations should take proactive measures to enhance cybersecurity, such as implementing strong security practices, regularly backing up data, staying vigilant against phishing and social engineering, and educating employees about cyber threats. Additionally, collaboration between governments, law enforcement agencies, and the cybersecurity industry is crucial to combat the growing threat of ransomware.

**KT0303 Typical threats, attacks and exploits used in cyber attacks**

Cyber attacks can involve various threats, attacks, and exploits, each with specific objectives and methods of execution. Here are some typical threats, attacks, and exploits commonly used in cyber attacks:

**1. Phishing Attacks:**

* Threat: Social engineering attack designed to deceive individuals into revealing sensitive information, such as login credentials or financial data.
* Attack: Attackers send fraudulent emails or messages that appear legitimate, urging recipients to click on malicious links or open infected attachments.
* Exploit: Exploits human psychology and trust to trick victims into taking harmful actions.

**2. Ransomware Attacks:**

* Threat: Malicious software that encrypts the victim's data and demands a ransom payment to provide the decryption key.
* Attack: Ransomware is delivered through various vectors, such as malicious email attachments, infected websites, or exploiting software vulnerabilities.
* Exploit: Exploits security weaknesses in systems to gain unauthorized access and deploy the ransomware.

**3. Distributed Denial of Service (DDoS) Attacks:**

* Threat: Overloads a target's server or network infrastructure with a flood of traffic, rendering it inaccessible to legitimate users.
* Attack: Attackers use botnets or coordinated systems to generate massive amounts of traffic aimed at overwhelming the target's resources.
* Exploit: Exploits the target's inability to handle an unusually high volume of traffic.

**4. Man-in-the-Middle (MitM) Attacks:**

* Threat: Intercepts and eavesdrops on communication between two parties, often without their knowledge.
* Attack: The attacker secretly relays and possibly alters the communication between the victims, making them believe they are directly communicating with each other.
* Exploit: Exploits insecure communication channels or compromised routers to intercept and control the data flow.

**5. SQL Injection (SQLi) Attacks:**

* Threat: Exploits vulnerabilities in web applications to manipulate or extract data from databases.
* Attack: Attackers insert malicious SQL code into input fields, tricking the application into executing unauthorized database commands.
* Exploit: Exploits improper handling of user input in web applications.

**6. Zero-Day Exploits:**

* Threat: Targets previously unknown vulnerabilities in software before the vendor releases a patch.
* Attack: Attackers use undisclosed exploit code to take advantage of the zero-day vulnerability, making it challenging for organizations to defend against the attack.
* Exploit: Exploits software weaknesses that are not yet known or patched by the software vendor.

**7. Malware (Viruses, Trojans, Worms, etc.):**

* Threat: Malicious software designed to infiltrate and damage systems or steal sensitive information.
* Attack: Malware can be delivered via infected files, email attachments, compromised websites, or through exploiting software vulnerabilities.
* Exploit: Exploits security weaknesses to gain unauthorized access and execute malicious code.

**8. Social Engineering Attacks:**

* Threat: Psychological manipulation of individuals to trick them into divulging sensitive information or taking certain actions.
* Attack: Attackers use social engineering techniques, such as pretexting, baiting, or tailgating, to gain access to restricted areas or obtain confidential information.
* Exploit: Exploits human nature and trust to bypass technical security measures.

**9. Advanced Persistent Threats (APTs):**

* Threat: Sophisticated and targeted attacks conducted over an extended period to gain unauthorized access and steal valuable information.
* Attack: APTs employ multiple attack vectors, including social engineering, zero-day exploits, and custom malware to avoid detection.
* Exploit: Exploits multiple vulnerabilities and techniques to maintain a long-term presence in the victim's network.

These are just some examples of common threats, attacks, and exploits used in cyber attacks. Cybercriminals continually develop new tactics and techniques, making it crucial for individuals and organizations to stay vigilant and implement robust cybersecurity measures to protect against these threats.

**KT0304 Rogue security software**

Rogue security software, also known as fake antivirus or scareware, is a type of malicious software that masquerades as legitimate security software but is, in fact, a scam. The primary goal of rogue security software is to deceive and trick users into believing that their computer is infected with viruses or malware. The attackers then attempt to extort money from the users by offering a fake solution to remove the non-existent threats.

Here's how rogue security software typically works:

1. **Deceptive Pop-up Messages**: Rogue security software often uses deceptive pop-up messages that appear when users browse the internet or visit compromised websites. These pop-ups display alarming warnings, such as "Your computer is infected with viruses!" or "Your system is at risk!".
2. **False Scan Results**: After the pop-up appears, the rogue software simulates a system scan, which invariably results in the detection of numerous malware infections, even on clean and secure systems.
3. **Urgent Warnings and Alerts**: The rogue software bombards users with urgent warnings and alerts, claiming that their computer is in imminent danger and that immediate action is required to prevent data loss or system damage.
4. **Fake Security Software**: The rogue security software offers a solution to remove the detected threats but requires payment for the full version of the software.
5. **No Real Protection**: Even if the user pays for the full version, the rogue software does not provide any real security protection or malware removal. It may even install actual malware or unwanted software on the victim's computer.
6. **Persistence and Evasion**: Rogue security software can be persistent and difficult to remove. It may try to disable legitimate security software or employ tactics to evade detection by genuine antivirus programs.

Rogue security software preys on users' fears and lack of knowledge about cybersecurity, attempting to manipulate them into making impulsive decisions out of panic. These scams can lead to financial loss, installation of actual malware, and compromise of personal information.

To protect against rogue security software and other scams:

* Be cautious of pop-up messages and alerts, especially those claiming immediate threats.
* Only download security software from reputable and official sources.
* Keep your operating system and security software up to date.
* Perform regular scans with a reputable antivirus program to detect and remove actual threats.
* Educate yourself and others about common cybersecurity scams and how to recognize them.

By staying informed and vigilant, users can better protect themselves from falling victim to rogue security software and other deceptive schemes.

**KT0305 Patch management and updates**

Patch management and updates are crucial processes in maintaining the security, stability, and performance of software, operating systems, and applications. They involve regularly applying updates, patches, and fixes released by software vendors to address known vulnerabilities, bugs, and issues. Let's explore patch management and updates in more detail:

**Patch Management:** Patch management refers to the systematic process of identifying, acquiring, testing, deploying, and verifying updates or patches for software applications and operating systems. The primary goal of patch management is to keep software up to date with the latest security fixes and improvements, reducing the risk of exploitation by cyber threats.

The patch management process typically involves the following steps:

1. **Patch Identification**: IT teams or administrators identify software products, applications, and operating systems that require updates. This is usually done through vendor notifications, security advisories, or vulnerability databases.
2. **Patch Acquisition**: Once patches are identified, organizations obtain the necessary updates directly from the software vendors or trusted sources. It is essential to download patches from official sources to avoid potential security risks from downloading patches from unauthorized or compromised locations.
3. **Patch Testing**: Before deploying patches across the entire network or system, organizations often test them in a controlled environment or on a limited number of systems. This helps ensure that the patches do not cause compatibility issues or unintended consequences.
4. **Patch Deployment**: After successful testing, patches are deployed across the organization's systems. This can be done manually or automated using patch management tools or systems.
5. **Monitoring and Verification**: Organizations continually monitor their systems to ensure that patches are applied successfully and have not introduced any new issues. Regular verification and auditing are essential to maintaining a secure and up-to-date environment.

**Software Updates:** Software updates refer to the release of newer versions of software or applications that include bug fixes, performance improvements, new features, and security updates. Updates are usually broader in scope than patches, which often focus on specific security fixes.

The purpose of software updates is to:

* Improve the overall functionality and performance of the software.
* Address bugs and issues that may affect user experience.
* Provide additional features and capabilities.
* Address security vulnerabilities and protect users from potential threats.

**Importance of Patch Management and Updates:** Effective patch management and regular software updates are critical for several reasons:

* **Security Enhancement**: Applying security patches promptly helps prevent cyberattacks that target known vulnerabilities in software.
* **Stability and Performance**: Updates and patches can improve software stability, fix bugs, and optimize performance.
* **Compatibility**: Keeping software up to date ensures compatibility with other applications and systems.
* **Compliance**: Many industries and regulatory frameworks require organizations to maintain updated software for compliance purposes.
* **Feature Enhancement**: Software updates often bring new features and functionalities that enhance user experience and productivity.

By prioritizing patch management and software updates, organizations can significantly reduce their exposure to security risks, enhance system stability, and ensure that their software remains optimized and secure. It is essential to have a well-defined and regularly updated patch management policy as part of an organization's cybersecurity strategy.

***Internal Assessment Criteria and Weight***

* IAC0301 Malware and ransomware are defined.
* IAC0302 Various types of attacks related to malware and ransomware are listed and described in terms of method of attack, how severe it is and how it can be prevented.
* IAC0303 Counter measures are described in terms of application and success.

***(Weight 32%)***

# REFERENCES

1. *Young, A.; M. Yung (1996). Cryptovirology: extortion-based security threats and countermeasures. IEEE Symposium on Security and Privacy. pp.*
2. *Schofield, Jack (28 July 2016). "How can I remove a ransomware infection?". The Guardian. Retrieved 28 July 2016.*
3. *Mimoso, Michael (28 March 2016). "Petya Ransomware Master File Table Encryption". threatpost.com. Retrieved 28 July 2016.*
4. *Justin Luna (21 September 2016). "Mamba ransomware encrypts your hard drive, manipulates the boot process". Neowin. Retrieved 5 November 2016.*
5. *Min, Donghyun; Ko, Yungwoo; Walker, Ryan; Lee, Junghee; Kim, Youngjae (July 2022). "A Content-Based Ransomware Detection and Backup Solid-State Drive for Ransomware Defense". IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.****41****(7): 2038–2051.*
6. *Cameron, Dell (13 May 2017). "Today's Massive Ransomware Attack Was Mostly Preventable; Here's How To Avoid It". Gizmodo. Retrieved 13 May 2017.*
7. *Dunn, John E. "Ransom Trojans spreading beyond Russian heartland". TechWorld. Archived from the original on 2 July 2014. Retrieved 10 March 2012.*