E-mail: coeoffice@csjmu.ac.in

☎🖷: 0512-2246609
☎🖷: 0512-2246608

छत्रपति शाहू जी महाराज विश्वविद्यालय, कानपुर

CHHATRAPATI SHAHU JI MAHARAJ UNIVERSITY, KANPUR

राष्ट्रीय मूल्यांकन एवं प्रत्यायन परिषद् द्वारा **A++** ग्रेड प्राप्त विश्वविद्यालय

(पूर्ववर्ती कानपुर विश्वविद्यालय, कानपुर)

(Formerly Known as Kanpur University, Kanpur- 208024)

सन्दर्भ संः सी.एस.जे.एम.वि.वि./**COE**/ 29 /2025 दिनांकः 15/01/2025

सेवा में,

प्राचार्य/प्राचार्या/नोडल केन्द्राध्यक्ष/केन्द्राध्यक्ष,
समस्त सम्बद्ध महाविद्यालय,
छत्रपति शाहू जी महाराज विश्वविद्यालय,
कानपुर।

विषयः– सत्र 2024–25 के बी0ए0, बी0एससी0 एवं बी0काम0 पाठ्यक्रम के तृतीय अधिसत्र में साइबर सुरक्षा **(Cyber Security)** रोजगार परक पाठ्यक्रम की परीक्षा के सम्बन्ध में।

महोदय/महोदया,

अवगत कराना है कि कार्यालय आदेश संख्या–सी0एस0जे0एम0वि0वि0/Acad/412/2024 दिनांक 24.09.2024 के द्वारा छत्रपति शाहू जी महाराज विश्वविद्यालय, कानपुर से सम्बद्ध महाविद्यालयों में सत्र 2024–25 के बी0ए0, बी0एस–सी0 एवं बी0कॉम पाठ्यक्रम के तृतीय अधिसत्र में अध्ययनरत् सभी छात्र/छात्राओं हेतु साइबर सुरक्षा (Cyber Security) रोजगार परक पाठ्यक्रम अनिवार्य रूप से लागू किया गया था। इस सम्बन्ध में अवगत कराना है कि साइबर सुरक्षा (Cyber Security) रोजगार परक पाठ्यक्रम 100 अंकों का होगा, जिसमें 40 अंक आन्तरिक मूल्यांकन तथा 60 अंक बाह्य/लिखित परीक्षा के आधार पर दिये जायेंगे। आन्तरिक मूल्यांकन के अंक विश्वविद्यालय द्वारा, पाठ्यक्रम अवधि के दौरान छात्र/छात्राओं की उपस्थिति तथा सतत् मूल्यांकन के आधार पर दिये जायेंगे। इसके साथ विश्वविद्यालय द्वारा दिनांक 02.02.2025 को 60 अंकों की बाह्य/लिखित परीक्षा वस्तुनिष्ठ प्रकार (Objective Type) से निम्नानुसार सम्पन्न कराई जाएगीः–

Course	Date	Day	Time
BA-III Sem & BCOM- III Sem	02-02-2025	Sunday	08:30 AM To 09:30 AM
BSC- III Sem	02-02-2025	Sunday	10:30 AM To 11:30 AM

विश्वविद्यालय द्वारा उपरोक्त बाह्य/लिखित परीक्षा से सम्बन्धित Question Bank इस पत्र के साथ संलग्न है तथा विश्वविद्यालय की वेबसाइट पर भी उपलब्ध कराया जा रहा है।

अतः आदेशानुसार आपसे अनुरोध है कि उक्त सूचना से अपने महाविद्यालय के समस्त सम्बन्धित छात्र/छात्राओं को अवगत कराने का कष्ट करें, जिससे निर्धारित तिथि पर सम्बन्धित परीक्षा सुचारू रूप से सम्पन्न कराई जा सके।

Urgent

भवदीय

(राकेश कुमार)
परीक्षा नियंत्रक

प्रतिलिपि : निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित :–

1. अधिष्ठाता, अकादमिक, सी0एस0जे0एम0यू0, कानपुर।
2. निदेशक, महाविद्यालय विकास परिषद्, सी0एस0जे0एम0यू0, कानपुर।
3. निजी सचिव, कुलपति, माननीय कुलपति जी के अवलोकनार्थ।
4. वैय0 सहायक, कुलसचिव/परीक्षा नियंत्रक/वित्त अधिकारी।
5. पी0एम0यू0/कोडिंग।
6. सम्बन्धित पत्रावली।

To Upload in 1- College website 2- Teacher-student Group 3- Notice Board

15.01.25

(अजय कुमार गौतम)
उप–कुलसचिव (परीक्षा)

VICE PRINCIPAL
CHRIST CHURCH COLLEGE
KANPUR

17/1/25

ALL MODULE QUESTION & ANSWER IN HINDI

1. निम्नलिखित में से कौन सा एक सामान्य प्रकार का साइबर खतरा है जिसमें सिस्टम को नुकसान पहुंचाने या बाधित करने के लिए डिज़ाइन किया गया दुर्भावनापूर्ण सॉफ़्टवेयर शामिल है?

a) मैलवेयर
b) फिशिंग
c) मैन-इन-द-मिडिल (MITM) हमला
d) डिनायल-ऑफ-सर्विस (DoS) हमला

उत्तर: a) मैलवेयर

2. फ़िशिंग हमले का प्राथमिक लक्ष्य क्या है?

a) एक वैध इकाई के रूप में संवेदनशील जानकारी चुराना
b) सेवा को बाधित करने के लिए ट्रैफ़िक के साथ एक सिस्टम को ओवरलोड करना
c) दो पक्षों के बीच संचार को रोकना और बदलना
d) लक्ष्य प्रणाली पर दुर्भावनापूर्ण सॉफ़्टवेयर स्थापित करना

उत्तर: a) वैध इकाई के रूप में संवेदनशील जानकारी चुराना

3. सीआईए ट्रायड का कौन सा पहलू डेटा की सटीकता और पूर्णता बनाए रखने पर केंद्रित है?

a) गोपनीयता

b) अखंडता

c) उपलब्धता

d) प्रमाणीकरण

उत्तर: b) अखंडता

4. निम्नलिखित में से कौन सीआईए त्रय में "उपलब्धता" के लिए संभावित खतरे का सबसे अच्छा वर्णन करता है?

a) संवेदनशील डेटा तक अनधिकृत पहुंच

b) डेटा भ्रष्टाचार या छेड़छाड़

c) इनकार-की-सेवा (DoS) हमले

d) डेटा उल्लंघनों

उत्तर: c) डिनायल-ऑफ-सर्विस (DoS) हमले

5. MITRE फ्रेमवर्क के संदर्भ में TTP का क्या अर्थ है?

a) रणनीति, तकनीक और प्रक्रियाएं

b) उपकरण, प्रौद्योगिकी और प्रोटोकॉल

c) खतरे, लक्ष्य और योजनाएं

d) तकनीक, रणनीति और प्रक्रियाएं

उत्तर: a) रणनीति, तकनीक और प्रक्रियाएं

6. साइबर किल चेन मॉडल का उद्देश्य क्या है?

a) साइबर हमले के चरणों की पहचान करना और वर्गीकृत करना

b) मैलवेयर को सिस्टम को संक्रमित करने से रोकने के लिए

c) विसंगतियों के लिए नेटवर्क ट्रैफ़िक की निगरानी करना

d) संचरण के दौरान डेटा एन्क्रिप्ट करने के लिए

उत्तर: a) साइबर हमले के चरणों की पहचान करना और वर्गीकृत करना

7.निम्नलिखित में से कौन सा डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विस (DDoS) हमले का सबसे अच्छा वर्णन करता है?

1. एक लक्ष्य को अभिभूत करने के लिए एक ही स्रोत से शुरू किया गया हमला
2. यातायात के साथ लक्ष्य को बाढ़ करने के लिए कई समझौता प्रणालियों का उपयोग करके एक हमला
3. एक हमला जो सिस्टम तक पहुंच प्राप्त करने के लिए सॉफ्टवेयर कमजोरियों का फायदा उठाता है
4. एक हमला जिसमें उपयोगकर्ता क्रेडेंशियल्स प्राप्त करने के लिए फ़िशिंग शामिल है

उत्तर: b) यातायात के साथ लक्ष्य को बाढ़ करने के लिए कई समझौता प्रणालियों का उपयोग करके एक हमला

8. साइबर सुरक्षा को साइबर अपराध से क्या अलग करता है?

a) साइबर सुरक्षा प्रणालियों की सुरक्षा के बारे में है, जबकि साइबर अपराध उनका शोषण करने के बारे में है
b) साइबर सुरक्षा में शारीरिक सुरक्षा शामिल है, जबकि साइबर अपराध में डिजिटल खतरे शामिल हैं
c) साइबर सुरक्षा हार्डवेयर से संबंधित है, जबकि साइबर अपराध सॉफ्टवेयर से संबंधित है
d) साइबर सुरक्षा कानूनी ढांचा है, जबकि साइबर अपराध तकनीकी कार्यान्वयन है

उत्तर: a) साइबर सुरक्षा प्रणालियों की सुरक्षा के बारे में है, जबकि साइबर अपराध उनका शोषण करने के बारे में है

9. MITRE ATT&CK के संदर्भ में, "प्रतिकूल अनुकरण" का क्या महत्व है?

a) रक्षात्मक उपायों का परीक्षण और सुधार करने के लिए विरोधियों के व्यवहार का अनुकरण करना

b) संवेदनशील डेटा को अनधिकृत पहुंच से बचाने के लिए एन्क्रिप्ट करना

c) कमजोरियों को ठीक करने के लिए सुरक्षा पैच स्थापित करना

d) संदिग्ध गतिविधि के लिए नेटवर्क ट्रैफ़िक की निगरानी करना

उत्तर: ए) रक्षात्मक उपायों का परीक्षण और सुधार करने के लिए विरोधियों के व्यवहार का अनुकरण करना

10. साइबर किल चेन के किस चरण में हमलावर समझौता किए गए सिस्टम को नियंत्रित करता है और संचार स्थापित करता है?

a) वितरण
b) कमान और नियंत्रण
c) शोषण
d) स्थापना

उत्तर: b) कमान और नियंत्रण

11. बहु-कारक प्रमाणीकरण (एमएफए) का उपयोग करने का एक सामान्य उद्देश्य क्या है?

1. पासवर्ड प्रबंधन की जटिलता को कम करने के लिए
2. यह सुनिश्चित करने के लिए कि केवल व्यवस्थापकों के पास सिस्टम तक पहुंच है
3. सत्यापन के कई रूपों की आवश्यकता के द्वारा सुरक्षा बढ़ाने के लिए
4. पासवर्ड वसूली की प्रक्रिया को स्वचालित करने के लिए

उत्तर: c) सत्यापन के कई रूपों की आवश्यकता के द्वारा सुरक्षा बढ़ाने के लिए

12. रिक्त स्थान भरें: _____ हमलों में डेटा चोरी या हेरफेर करने के लिए दो पक्षों के बीच संचार को रोकना और बदलना शामिल है।

a) डीएनएस अपहरण

b) डीडीओएस

c) मैन-इन-द-मिडिल (एमआईटीएम)

d) फिशिंग

उत्तर: c) मैन-इन-द-मिडिल (MITM)

13. डेटा संरक्षण कानूनों का प्राथमिक उद्देश्य क्या है?

1. हर कीमत पर डेटा उल्लंघनों को रोकने के लिए
2. व्यक्तिगत डेटा को एकत्रित, संग्रहीत और उपयोग करने के तरीके को विनियमित करने के लिए
3. यह सुनिश्चित करने के लिए कि सभी डेटा एन्क्रिप्ट किया गया है
4. कंपनियों को व्यक्तिगत डेटा बेचने की अनुमति देने के लिए

उत्तर: b) यह विनियमित करने के लिए कि व्यक्तिगत डेटा कैसे एकत्र, संग्रहीत और उपयोग किया जाता है

14. सर्ट-इन का प्राथमिक कार्य क्या है?

a) निजी कंपनियों के लिए साइबर सुरक्षा ऑडिट करना
b) साइबर सुरक्षा घटनाओं का जवाब देना और उनके समाधान में सहायता करना
c) अवैध गतिविधियों के लिए इंटरनेट ट्रैफ़िक की निगरानी करना
d) भारत में इंटरनेट सेवा प्रदाताओं (ISP) को विनियमित करना

उत्तर: b) साइबर सुरक्षा की घटनाओं का जवाब देना और उनके समाधान में सहायता करना

15. 2022 साइबर सुरक्षा निर्देशों के अनुसार संगठनों को कितनी बार साइबर सुरक्षा घटनाओं की रिपोर्ट CERT-In को करने की आवश्यकता होती है?

a) घटना की पहचान करने के 4 घंटे के भीतर
b) घटना की पहचान करने के 6 घंटे के भीतर
ग) घटना की पहचान करने के 12 घंटे के भीतर
घ) घटना की पहचान करने के 24 घंटे के भीतर

उत्तर: b) घटना की पहचान करने के 6 घंटे के भीतर

16. निम्नलिखित में से कौन सा शून्य ट्रस्ट आर्किटेक्चर को लागू करने का एक प्रमुख घटक है?

a) नेटवर्क की सुरक्षा के लिए एकल फ़ायरवॉल का उपयोग करना
b) यह सुनिश्चित करना कि नेटवर्क के भीतर सभी डिवाइस डिफ़ॉल्ट रूप से विश्वसनीय हैं
ग) सख्त पहचान सत्यापन और अभिगम नियंत्रण लागू करना
d) आंतरिक संसाधनों तक अप्रतिबंधित पहुंच की अनुमति देना

उत्तर: ग) सख्त पहचान सत्यापन और अभिगम नियंत्रण लागू करना

दिए गए परिदृश्य के आधार पर प्रश्नों के उत्तर दें

घटना 1: आधार डेटाबेस, जिसमें भारतीय नागरिकों के नाम, पते, फोन नंबर और बायोमेट्रिक डेटा जैसी संवेदनशील जानकारी शामिल है, से समझौता किया गया है। हमलावरों ने इस डेटा तक अनधिकृत पहुंच प्राप्त कर ली है और संभवतः विभिन्न दुर्भावनापूर्ण गतिविधियों के लिए इसका फायदा उठा रहे हैं।

17. आधार डेटाबेस तक अनधिकृत पहुंच प्राप्त करने की कौन सी रणनीति सबसे अधिक निकटता से मेल खाती है?

a) निष्पादन

b) प्रारंभिक पहुंच

c) पार्श्व गति

d) बहिर्गमन

उत्तर: b) प्रारंभिक पहुंच

18. समझौता किए गए उपयोगकर्ता क्रेडेंशियल्स के माध्यम से आधार डेटाबेस तक पहुंच प्राप्त करने के लिए एक हमलावर किस MITRE ATT&CK तकनीक का उपयोग कर सकता है?

1. T1078: वैध खाते
2. T1059: कमांड और स्क्रिप्टिंग इंटरप्रेटर
3. T1071: अनुप्रयोग परत प्रोटोकॉल
4. T1046: नेटवर्क सेवा स्कैनिंग

उत्तर: a) T1078: वैध खाते

Incident 2: WannaCry ransomware एक प्रकार का दुर्भावनापूर्ण सॉफ़्टवेयर है जो मई 2017 में कंप्यूटर नेटवर्क में तेजी से फैल गया। इसने प्रभावित सिस्टम पर फ़ाइलों को एन्क्रिप्ट किया और डिक्रिप्शन कुंजी के लिए बिटकॉइन में फिरौती भुगतान की मांग की। रैंसमवेयर ने विंडोज ऑपरेटिंग सिस्टम में एक भेद्यता का फायदा उठाया, विशेष रूप से फैलने के लिए इटरनलब्लू शोषण का लाभ उठाया।

19. WannaCry द्वारा तेजी से फैलने के लिए किस विशिष्ट विंडोज भेद्यता का शोषण किया गया था?

1. सीवीई-2017-0144 (इटरनलब्लू)
2. CVE-2016-0051 (SMBv2 सूचना प्रकटीकरण)
3. CVE-2017-0199 (कार्यालय/वर्डपैड रिमोट कोड निष्पादन)
4. CVE-2015-0001 (Windows कर्नेल विशेषाधिकार वृद्धि)

उत्तर: a) सीवीई-2017-0144 (इटरनलब्लू)

20. एक सिस्टम को संक्रमित करने के बाद, WannaCry ने बिटकॉइन में भुगतान की मांग करते हुए एक फिरौती नोट प्रदर्शित किया। यह क्रिया किस MITRE ATT&CK रणनीति का प्रतिनिधित्व करती है?

1. प्रभाव
2. कमान और नियंत्रण
3. निष्कासन
4. खोज

उत्तर: a) प्रभाव

Case Scenario: 1

आपके संगठन, XYZ Inc. ने हाल ही में एक घटना का अनुभव किया जहां कई कर्मचारियों को एक ईमेल प्राप्त हुआ जो सीईओ से प्रतीत होता है। ईमेल ने अनुरोध किया कि ये कर्मचारी संवेदनशील कंपनी डेटा को तत्काल स्थानांतरित करें और एक सुरक्षित कंपनी डेटाबेस के लिए लॉगिन क्रेडेंशियल प्रदान करें। ईमेल में सीईओ के हस्ताक्षर थे और ऑफ-आवर्स के दौरान भेजा गया था। कुछ ही समय बाद, कई कर्मचारियों ने अपने खातों से छेड़छाड़ किए जाने की सूचना दी, और कंपनी के धन का अनधिकृत हस्तांतरण हुआ।

इस परिदृश्य के आधार पर, निम्नलिखित प्रश्नों के उत्तर दीजिए (1-5):

परिदृश्य में वर्णित साइबर खतरे के प्रकार की पहचान करें।

a) मैलवेयर
b) फिशिंग
c) सेवा से इनकार (DoS)
d) मैन-इन-द-मिडिल (MitM)

उत्तर: b) फिशिंग

22: परिदृश्य में किस विशिष्ट फ़िशिंग तकनीक का उपयोग किया जा रहा है?
a) स्मिशिंग
b) विशिंग
c) क्लोन फ़िशिंग
d) व्हेलिंग

उत्तर: d) व्हेलिंग

इस परिदृश्य में हमले के पीछे कौन सी प्रेरणा सबसे अधिक संभावना है?

a) सक्रियतावाद
b) जासूसी
c) वित्तीय लाभ
d) बदला

उत्तर: c) वित्तीय लाभ

24: समझौता का पता चलने पर आईटी सुरक्षा टीम को तत्काल क्या कार्रवाई करनी चाहिए?

a) घटना पर ध्यान न दें
b) अतिरिक्त धनराशि को सुरक्षित खाते में स्थानांतरित करें
c) प्रभावित खातों को अक्षम करें और सुरक्षा ऑडिट शुरू करें
d) सभी कर्मचारियों से अधिक जानकारी का अनुरोध करते हुए एक ईमेल भेजें

उत्तर: c) प्रभावित खातों को अक्षम करें और सुरक्षा ऑडिट शुरू करें

भविष्य में इसी तरह के हमलों को रोकने के लिए XYZ Inc. को कौन से दीर्घकालिक उपाय लागू करने चाहिए?

a) संवेदनशील डेटा को संभालने वाले कर्मचारियों की संख्या में वृद्धि
b) नियमित साइबर सुरक्षा जागरूकता प्रशिक्षण लागू करें
c) सुरक्षा ऑडिट की संख्या कम करें
d) कर्मचारियों को बेहतर पहुंच के लिए पासवर्ड साझा करने के लिए प्रोत्साहित करें

उत्तर: b) नियमित साइबर सुरक्षा जागरूकता प्रशिक्षण लागू करें

Case Scenario: 2

ई-कॉमर्स सॉल्यूशंस इंक ने हाल ही में अपनी ऑनलाइन सेवाओं में एक महत्वपूर्ण व्यवधान का अनुभव किया है। कई घंटों के लिए, वैध ग्राहक कंपनी की वेबसाइट तक पहुंचने में असमर्थ थे, जिससे बिक्री और ग्राहक असंतोष में काफी नुकसान हुआ। जांच करने पर, आईटी टीम ने पाया कि व्यवधान वेबसाइट पर निर्देशित ट्रैफ़िक की भारी बाढ़ के कारण हुआ था, जो दुनिया भर में कई समझौता किए गए उपकरणों से उत्पन्न हुआ था। कंपनी की प्रतिष्ठा को झटका लगा है, और वे भविष्य में ऐसी घटनाओं को रोकने के उपायों पर विचार कर रहे हैं।

इस परिदृश्य के आधार पर, निम्नलिखित प्रश्नों के उत्तर दीजिए (6-10):

परिदृश्य में वर्णित हमले के प्रकार की पहचान करें।

a) फिशिंग
b) मैलवेयर
c) डिस्ट्रिब्यूटेड डिनायल-ऑफ-सर्विस (DDoS)
d) मैन-इन-द-मिडिल (MitM)
उत्तर: c) डिस्ट्रिब्यूटेड डिनायल-ऑफ-सर्विस (DDoS)

27: DoS हमले और DDoS हमले के बीच प्राथमिक अंतर क्या है?

a) एक DoS हमला एक ही सिस्टम को लक्षित करने के लिए कई स्रोतों का उपयोग करता है, जबकि एक DDoS हमला एक ही स्रोत से उत्पन्न होता है।
b) एक DoS हमला लक्ष्य को एक स्रोत से ट्रैफ़िक से भर देता है, जबकि DDoS हमला लक्ष्य को बाढ़ देने के लिए कई समझौता किए गए उपकरणों का उपयोग करता है।
c) DDoS हमले की तुलना में DoS हमला कम हानिकारक होता है।
घ) कोई अंतर नहीं है; दोनों शब्द विनिमेय हैं।

उत्तर: बी) एक डीओएस हमला एक स्रोत से यातायात के साथ लक्ष्य को बाढ़ देता है, जबकि एक डीडीओएस हमला लक्ष्य को बाढ़ के लिए कई समझौता किए गए उपकरणों का उपयोग करता है।

28: निम्नलिखित में से कौन सा DDoS हमले का विशिष्ट प्रभाव नहीं है?

a) वित्तीय हानि
b) वेबसाइट ट्रैफ़िक में वृद्धि
c) प्रतिष्ठित क्षति
d) Loss of Productivity

उत्तर: b) वेबसाइट ट्रैफ़िक में वृद्धि

29: किस शमन रणनीति में DDoS हमले का प्रबंधन करने के लिए सर्वरों के वैश्विक नेटवर्क पर ट्रैफ़िक वितरित करना शामिल है?

a) ट्रैफिक फ़िल्टरिंग
b) दर सीमित करना
c) एनीकास्ट नेटवर्किंग
d) घटना प्रतिक्रिया योजना

उत्तर: c) एनीकास्ट नेटवर्किंग

30: भविष्य के डीडीओएस हमलों के प्रभाव को कम करने के लिए ई-कॉमर्स सॉल्यूशंस इंक को क्या दीर्घकालिक उपाय लागू करना चाहिए?

A. कर्मचारियों की संख्या कम करना
B. DDoS शमन सेवाओं को लागू करें
C. मामूली ट्रैफ़िक स्पाइक्स पर ध्यान न दें
D. बिक्री प्रचार बढ़ाएँ

उत्तर: b) DDoS शमन सेवाओं को लागू करें

Case Scenario: 3

XYZ Tech Solutions Corp. ने हाल ही में अपने नेटवर्क पर असामान्य गतिविधि का पता लगाया है। जांच करने पर, आईटी सुरक्षा टीम ने पाया कि अधिकारियों के बीच संवेदनशील ईमेल को इंटरसेप्ट और बदल दिया गया था, जिससे गलतफहमी और संभावित वित्तीय नुकसान हुआ। इसके अतिरिक्त, कर्मचारियों ने आंतरिक सेवाओं तक पहुंचने की कोशिश करते समय नकली वेबसाइटों पर पुनर्निर्देशित होने की सूचना दी। सुरक्षा दल ने कंपनी के परिसर के भीतर एक दुष्ट वाई-फाई हॉटस्पॉट की उपस्थिति की पहचान की और संदेह किया कि हमलावरों ने नेटवर्क ट्रैफ़िक को बाधित करने और हेरफेर करने के लिए इसे स्थापित किया था।

इस परिदृश्य के आधार पर, निम्नलिखित प्रश्नों के उत्तर दें (11-15):

31: परिदृश्य में वर्णित हमले के प्रकार की पहचान करें।

a) एडवांस्ड पर्सिस्टेंट थ्रेट (APT)
b) इनसाइडर थ्रेट
c) मैन-इन-द-मिडिल (MitM)
d) सेवा से इनकार (DoS)

उत्तर: c) मैन-इन-द-मिडिल (MitM)

32: एमआईटीएम हमलों में उपयोग की जाने वाली कौन सी विधि इस परिदृश्य में सबसे अधिक शामिल है?

a) डीएनएस स्पूफिंग
b) दुर्भावनापूर्ण वाई-फाई नेटवर्क
c) एसएसएल स्ट्रिपिंग
डी) सार्वजनिक यूएसबी चार्जिंग पोर्ट

उत्तर: b) दुर्भावनापूर्ण वाई-फाई नेटवर्क

इस प्रकार के हमले का पता लगाने और रोकने में कौन से निवारक उपाय मदद कर सकते थे?

a) सुरक्षित वाई-फाई नेटवर्क और वीपीएन का उपयोग
b) नेटवर्क पर दर सीमित लागू करना
ग) पासवर्ड प्रबंधन पर प्रशिक्षण कर्मचारियों
d) नियमित सॉफ्टवेयर अपडेट

उत्तर: ए) सुरक्षित वाई-फाई नेटवर्क और वीपीएन का उपयोग

34: उन्नत लगातार खतरों (APTs) की कौन सी विशेषता वर्णित परिदृश्य के लिए सीधे प्रासंगिक नहीं है?

a) लक्षित हमले
b) दृढ़ता
c) चुपके से
d) डीएनएस स्पूफिंग

उत्तर: d) डीएनएस स्पूफिंग

35: निम्नलिखित में से कौन सा XYZ Tech Solutions Corp. के लिए समान MitM हमलों को रोकने के लिए अनुशंसित दीर्घकालिक उपाय है?

a) सार्वजनिक वाई-फाई हॉटस्पॉट की संख्या में वृद्धि
बी) सार्वजनिक यूएसबी चार्जिंग पोर्ट के उपयोग को प्रोत्साहित करें
ग) संवेदनशील प्रणालियों तक पहुँचने के लिए दो-कारक प्रमाणीकरण (2FA) लागू करें
d) कर्मचारी प्रशिक्षण सत्र कम करें

उत्तर: c) संवेदनशील सिस्टम तक पहुँचने के लिए दो-कारक प्रमाणीकरण (2FA) लागू करें

Case Scenario: 4

हाल ही में, XYZ कॉर्पोरेशन साइबर हमले का शिकार हुआ, जिसके परिणामस्वरूप महत्वपूर्ण/भारी वित्तीय नुकसान, परिचालन व्यवधान और प्रतिष्ठित क्षति हुई। हमले ने कंपनी के वित्तीय डेटा और ग्राहक जानकारी को लक्षित किया, जिससे कर्मचारियों और ग्राहकों के बीच समान रूप से व्यापक दहशत फैल गई। जांच से पता चला कि हमला एक परिष्कृत समूह से उत्पन्न हुआ था, जिसकी पहुंच उन्नत हैकिंग टूल और तकनीकों तक थी। जैसा कि सुरक्षा टीम उल्लंघन को रोकने और क्षति को कम करने के लिए अथक प्रयास करती है, कंपनी के अधिकारी संभावित कानूनी और नियामक परिणामों सहित इसके बाद से जूझ रहे हैं।

इस परिदृश्य के आधार पर, निम्नलिखित प्रश्नों के उत्तर दीजिए (16-20):

36: परिदृश्य में वर्णित साइबर हमले के लिए संभावित रूप से जिम्मेदार प्राथमिक खतरे वाले अभिनेता की पहचान करें।

a) राष्ट्र-राज्य
b) साइबर अपराधी
c) हैक्टिविस्ट
d) अंदरूनी सूत्र

उत्तर: b) साइबर अपराधी

37: परिदृश्य में पहचाने गए खतरे के अभिनेता के साथ कौन सी प्रेरणा सबसे अधिक जुड़ी हुई है?

a) वित्तीय लाभ
b) जासूसी
(c) राजनीतिक या सामाजिक कारण
d) हैकिंग का रोमांच

उत्तर: a) वित्तीय लाभ

38: साइबर खतरों के किस प्रभाव का परिदृश्य में सीधे उल्लेख नहीं किया गया है?

a) कानूनी और नियामक परिणाम
b) मनोवैज्ञानिक और भावनात्मक प्रभाव
c) शारीरिक क्षति
d) प्रतिष्ठित क्षति

उत्तर: c) शारीरिक क्षति

39: साइबर हमले के परिणामस्वरूप XYZ Corporation को किस संभावित कानूनी चुनौती का सामना करना पड़ सकता है?

a) ग्राहक विश्वास में वृद्धि
b) सकारात्मक प्रचार
c) नियामक जुर्माना और अनुपालन आवश्यकताएं
d) परिचालन व्यवधानों में कमी

उत्तर: c) परिचालन व्यवधानों में कमी

40: परिदृश्य को ध्यान में रखते हुए, भविष्य के साइबर हमलों को रोकने के लिए XYZ Corporation को किस दीर्घकालिक उपाय को प्राथमिकता देनी चाहिए?

a) उन्नत समापन बिंदु सुरक्षा समाधान लागू करना
b) कर्मचारियों को काम के लिए व्यक्तिगत उपकरणों का उपयोग करने के लिए प्रोत्साहित करना
c) घटना को अनदेखा करना और आगे बढ़ना
d) कर्मचारियों को साइबर सुरक्षा प्रशिक्षण प्रदान करना

उत्तर: d) कर्मचारियों को साइबर सुरक्षा प्रशिक्षण प्रदान करना

41. ओटीपी धोखाधड़ी में हमलावर पीड़ितों को उनके ओटीपी का खुलासा करने के लिए बरगलाने के लिए एक सामान्य तरीके का उपयोग करते हैं?

a) नकली नौकरी की पेशकश भेजना
b) फ़िशिंग ईमेल या कॉल जो बैंक से होने का दावा करते हैं
c) मुफ्त सॉफ्टवेयर अपडेट की पेशकश
d) धोखाधड़ी वाले निवेश के अवसर प्रदान करना

उत्तर: b) फ़िशिंग ईमेल या कॉल जो बैंक से होने का दावा करते हैं

42. साइबर अपराधों की रिपोर्ट करना क्यों महत्वपूर्ण माना जाता है?

a) यह जांच शुरू करने और पीड़ितों की रक्षा करने में मदद करता है।
b) यह टेक कंपनियों के लिए मार्केटिंग अंतर्दृष्टि प्रदान करता है.
c) यह इंटरनेट उपयोग और ट्रैफ़िक को बढ़ाता है।
d) यह साइबर सुरक्षा सॉफ्टवेयर के लिए बिक्री बढ़ाता है।

उत्तर: ए) यह जांच शुरू करने और पीड़ितों की रक्षा करने में मदद करता है।

43. महत्वपूर्ण बुनियादी ढांचे पर साइबर हमला किसी देश की अर्थव्यवस्था को कैसे प्रभावित कर सकता है?

a) वित्तीय लेनदेन की दक्षता में सुधार करके
b) आर्थिक पक्षाघात की ओर अग्रसर होकर और बैंकिंग लेनदेन को प्रभावित करके
(c) माल की उपलब्धता में वृद्धि करके
d) परिवहन नेटवर्क की स्थिरता को बढ़ाकर

उत्तर: b) आर्थिक पक्षाघात की ओर अग्रसर और बैंकिंग लेनदेन को प्रभावित करके

44. किसी संगठन की साइबर सुरक्षा मुद्रा को मजबूत करने के लिए अनुशंसित निवारक उपाय क्या नहीं है?

a) नियमित जोखिम आकलन और प्रबंधन
b) मान्यता प्राप्त साइबर सुरक्षा ढांचे को अपनाना
c) बहु-कारक प्रमाणीकरण (MFA.
d) उद्योग-विशिष्ट मानकों और सर्वोत्तम प्रथाओं को लागू करना

उत्तर: ग) बहु-कारक प्रमाणीकरण (एमएफए) के उपयोग को अनदेखा करना।

45. भारतीय आईटी अधिनियम 2008 के संदर्भ में, कौन सा पहलू विशेष रूप से ई-कॉमर्स विकास को बढ़ावा देने के उद्देश्य से है?

क) इलेक्ट्रॉनिक रिकॉर्ड और अनुबंध
ख) प्रमाणन प्राधिकरणों का विनियमन
c) साइबर अपराध रोकथाम के उपाय
d) डेटा संरक्षण दिशानिर्देश

उत्तर: a) इलेक्ट्रॉनिक रिकॉर्ड और अनुबंध

46. कौन सा उदाहरण भारतीय आईटी अधिनियम 2008 में डिजिटल हस्ताक्षर की भूमिका को सबसे अच्छा दर्शाता है?

a) ऑनलाइन टैक्स रिटर्न दाखिल करना
b) इलेक्ट्रॉनिक अनुबंध सत्यापित करना
c) ई-कॉमर्स प्लेटफॉर्म के माध्यम से सामान खरीदना
d) सुरक्षा के लिए व्यक्तिगत डेटा एन्क्रिप्ट करना

उत्तर: बी) एक इलेक्ट्रॉनिक अनुबंध की पुष्टि करना

47. एक डेटा प्रिंसिपल नोटिस करता है कि वित्तीय सेवा वेबसाइट पर उनकी व्यक्तिगत जानकारी पुरानी है और इसमें त्रुटियां शामिल हैं। वे चिंतित हैं कि ये अशुद्धियां उनके खाता प्रबंधन और वित्तीय लेनदेन को प्रभावित कर सकती हैं। कौन सा अधिकार डेटा प्रिंसिपल को वित्तीय सेवा वेबसाइट पर अपनी व्यक्तिगत जानकारी को सही या अपडेट करने की अनुमति देता है?

a) व्यक्तिगत डेटा के बारे में सूचना तक पहुंच का अधिकार
b) व्यक्तिगत डेटा के सुधार और उन्मूलन का अधिकार
c) शिकायत निवारण का अधिकार
d) डेटा पोर्टेबिलिटी का अधिकार

उत्तर: b) व्यक्तिगत डेटा के सुधार और उन्मूलन का अधिकार

48. एक उपयोगकर्ता नाखुश है क्योंकि उनका व्यक्तिगत डेटा उनकी सहमति के बिना किसी तीसरे पक्ष के साथ साझा किया गया था। वे समझना चाहते हैं कि कौन सा डेटा साझा किया गया था और किसके साथ और इस बारे में स्पष्टता चाहते हैं कि उनका डेटा कैसे संभाला जा रहा है। कौन सा अधिकार उपयोगकर्ता को अपनी व्यक्तिगत डेटा प्रोसेसिंग गतिविधियों का सारांश और तीसरे पक्ष के डेटा साझाकरण के बारे में जानकारी प्राप्त करने में सक्षम बनाता है?

a) व्यक्तिगत डेटा के सुधार और उन्मूलन का अधिकार
b) व्यक्तिगत डेटा के बारे में जानकारी तक पहुँचने का अधिकार
c) शिकायत निवारण का अधिकार
d) डेटा पोर्टेबिलिटी का अधिकार

उत्तर: b) व्यक्तिगत डेटा के बारे में जानकारी प्राप्त करने का अधिकार

49. युद्ध में रणनीतिक योजना का एक प्रमुख उद्देश्य क्या है?

a) विरोधी ताकतों के बीच सीधा जुड़ाव।
b) दुश्मन के बारे में जानकारी इकट्ठा करना और उसका विश्लेषण करना।
ग) लड़ाई जीतने के लिए विशिष्ट संचालन और युद्धाभ्यास को लागू करना।
d) सैन्य लक्ष्यों को प्राप्त करने के लिए दीर्घकालिक रणनीति विकसित करना।

उत्तर: घ) सैन्य लक्ष्यों को प्राप्त करने के लिए दीर्घकालिक रणनीति विकसित करना।

50. डीपीडीपीए धारा 18 में उल्लिखित डेटा प्रोटेक्शन बोर्ड ऑफ इंडिया की प्राथमिक भूमिका क्या है?

a) नए डेटा संरक्षण कानूनों का मसौदा तैयार करना
b) डेटा संरक्षण कानूनों के कार्यान्वयन और प्रवर्तन की निगरानी करना
c) डेटा संरक्षण के लिए विपणन और जनसंपर्क को संभालना
d) डेटा भंडारण और क्लाउड कंप्यूटिंग सेवाओं को विनियमित करने के लिए

उत्तर: b) डेटा संरक्षण कानूनों के कार्यान्वयन और प्रवर्तन की निगरानी करना

51. **निम्नलिखित में से कौन सा क्रिप्टोग्राफिक एल्गोरिथ्म का एक प्रकार नहीं है?**

a) सममित कुंजी एल्गोरिथ्म
b) असममित कुंजी एल्गोरिथ्म
c) हैशिंग एल्गोरिथम
d) रैखिक खोज एल्गोरिथ्म

उत्तर: d) रैखिक खोज एल्गोरिथ्म

52. सममित कुंजी क्रिप्टोग्राफी में, एन्क्रिप्शन और डिक्रिप्शन के लिए उपयोग की जाने वाली कुंजी है:

a) भिन्न
b) वही
c) सार्वजनिक
d) निजी

उत्तर: b) वही

53. निम्नलिखित में से कौन सा एल्गोरिदम असममित कुंजी क्रिप्टोग्राफी का एक उदाहरण है?

a) डीईएस
b) एईएस
c) आरएसए
d) एमडी 5

उत्तर: c) आरएसए

54. सादे पाठ को सिफर पाठ में परिवर्तित करने की प्रक्रिया को किस रूप में जाना जाता है?

a) डिक्रिप्शन
b) एन्क्रिप्शन
c) हैशिंग
d) एन्कोडिंग

उत्तर: b) एन्क्रिप्शन

55. क्रिप्टोग्राफी में "ब्रूट फोर्स अटैक" शब्द क्या संदर्भित करता है?

a) हर संभव संयोजन की कोशिश करके कुंजी का अनुमान लगाना
b) संचरण के दौरान कुंजी को रोकना
c) एन्क्रिप्टेड पाठ में पैटर्न का विश्लेषण करना
d) कुंजी के बिना सिफर पाठ को संशोधित करना

उत्तर: a) हर संभव संयोजन की कोशिश करके कुंजी का अनुमान लगाना

56. निम्नलिखित में से कौन सा क्रिप्टोग्राफिक हैश फ़ंक्शन का एक उदाहरण है?

a) आरएसए
b) एईएस
ग) एसएचए -256
d) डिफी-हेलमैन

उत्तर: c) एसएचए -256

57. सार्वजनिक कुंजी अवसंरचना (PKI) में, प्रमाणपत्र प्राधिकरण (CA) की भूमिका क्या है?

a) डेटा एन्क्रिप्ट करना
b) डेटा को डिक्रिप्ट करना
c) डिजिटल प्रमाणपत्र जारी करना
d) निजी कुंजी उत्पन्न करना

उत्तर: c) डिजिटल प्रमाणपत्र जारी करना

58. ईमेल संचार में एसएसएल / टीएलएस प्रोटोकॉल का उद्देश्य क्या है?

a) ईमेल सामग्री एन्क्रिप्ट करना
b) प्राप्तकर्ता के ईमेल पते का सत्यापन करना
c) ईमेल अटैचमेंट को कंप्रेस करना
d) स्पैम ईमेल फ़िल्टर करना

उत्तर: ए) ईमेल सामग्री को एन्क्रिप्ट करना

59. निम्नलिखित में से कौन सा ईमेल संदेश की प्रामाणिकता सुनिश्चित करने की एक विधि है?

a) डिजिटल हस्ताक्षर
b) स्पैम फ़िल्टर
c) एंटीवायरस सॉफ्टवेयर
d) फ़ायरवॉल

उत्तर: a) डिजिटल हस्ताक्षर

60. ईमेल सुरक्षा में स्पैम फ़िल्टर का प्राथमिक कार्य क्या है?

a) ईमेल एन्क्रिप्ट करना
b) अवांछित ईमेल को ब्लॉक करना
c) प्रेषक की पहचान सत्यापित करना
d) ईमेल संग्रह करना

उत्तर: b) अवांछित ईमेल को ब्लॉक करना

61. एसएसएल प्रोटोकॉल के संबंध में निम्नलिखित में से कौन सा गलत है?

1. एसएसएल एक प्रोटोकॉल है जो गोपनीयता सुनिश्चित करने के लिए प्रेषक और रिसीवर के बीच एक सुरक्षित सुरंग स्थापित करता है।
2. एसएसएल एक प्रोटोकॉल है जो अखंडता सुनिश्चित करने के लिए प्रेषक और रिसीवर के बीच एक सुरक्षित सुरंग स्थापित करता है।
3. एसएसएल एक प्रोटोकॉल है जो उपलब्धता सुनिश्चित करने के लिए प्रेषक और रिसीवर के बीच एक सुरक्षित सुरंग स्थापित करता है।
4. SSL एक प्रोटोकॉल है जो सेवा प्रदाता प्रमाणीकरण सुनिश्चित करने के लिए डिजिटल प्रमाणपत्र का उपयोग करता है।

उत्तर: C) SSL एक प्रोटोकॉल है जो उपलब्धता सुनिश्चित करने के लिए प्रेषक और रिसीवर के बीच एक सुरक्षित सुरंग स्थापित करता है।

62. कौन सी संस्थाएं सार्वजनिक कुंजी अवसंरचना (PKI) की सदस्य नहीं हैं?

1. प्रमाणपत्र प्राधिकरण: प्रमाण पत्र जारी करने के लिए जिम्मेदार एक सर्वर या प्राधिकरण
2. उपयोगकर्ता: प्रमाणपत्र के लिए क्लाइंट अनुरोध
1. पंजीकरण प्राधिकरण: एक सर्वर या प्राधिकरण अनुरोध का पंजीकरण करता है
2. DNS सर्वर: प्रमाणपत्र अनुरोध भेजने के लिए IP पता प्रदान करने के लिए जिम्मेदार सर्वर

उत्तर: डीएनएस सर्वर: प्रमाणपत्र अनुरोध भेजने के लिए आईपी पता प्रदान करने के लिए जिम्मेदार सर्वर

63. निम्नलिखित में से कौन सा विंडोज के इनबाउंड फ़ायरवॉल नियम में एक पैरामीटर नहीं है?

1. स्रोत और दूरस्थ डिवाइस पता
2. स्रोत और गंतव्य डिवाइस पोर्ट
3. ट्रांसपोर्ट और नेटवर्क लेयर प्रोटोकॉल
4. डोमेन नाम

उत्तर: D) डोमेन नाम

64. DNS अपहरण उपयोगकर्ताओं को दुर्भावनापूर्ण वेबसाइट पर ले जाता है ताकि _____

1. उपयोगकर्ता क्रेडेंशियल्स एकत्र किए जाएंगे
2. उपयोगकर्ता गतिविधि रिकॉर्ड की जाएगी
3. उपयोगकर्ता को गलत जानकारी प्रदान की जाएगी
4. उपरोक्त सभी

उत्तर: D) उपरोक्त सभी

65. निम्नलिखित में से कौन "विषाक्तता करने के लिए कैश में संसाधन रिकॉर्ड बदलने" को संदर्भित करता है?

1. डीएनएस विषाक्तता
2. एआरपी विषाक्तता
3. एसएसएल प्रमाणपत्र स्पूफिंग
4. फ़ायरवॉल नियम विषाक्तता

उत्तर: A) डीएनएस विषाक्तता

66. सार्वजनिक वाई-फाई तक पहुँचने से सुरक्षा समस्या क्यों आती है?

1. उपकरणों के बीच वाई-फाई एक्सेस प्वाइंट पर संचार असुरक्षित हो सकता है, जिससे बीच के हमले में आदमी को अनुमति मिलती है।
2. HTTPS- आधारित संचार हमेशा डिवाइस और सर्वर के बीच पहुंच बिंदु के माध्यम से एक सुरक्षित सुरंग सुनिश्चित करता है।
3. कोई भी दुर्भावनापूर्ण उपयोगकर्ता संवेदनशील जानकारी एकत्र करने के लिए हवा में बहने वाले पैकेटों तक पहुंच सकता है।
1. वाई-फाई एक्सेस प्वाइंट उन सभी वेबसाइटों तक पहुंच प्रदान नहीं करेगा जिन्हें हम एक्सेस करने का इरादा रखते हैं।

उत्तर: ए) वाई-फाई एक्सेस प्वाइंट पर उपकरणों के बीच संचार असुरक्षित हो सकता है, जिससे बीच के हमले में आदमी को अनुमति मिलती है।

67. निम्नलिखित में से कौन मशीन के फ़ायरवॉल और एंटी-वायरस को अलग करता है?
a) फ़ायरवॉल नेटवर्क को सुरक्षित करने के लिए है, और एंटी-वायरस मशीन को सुरक्षित करने के लिए है
b) फ़ायरवॉल अभिगम नियंत्रण सुनिश्चित करता है, और एंटी-वायरस प्राधिकरण को नियंत्रित करता है।
ग) एक फ़ायरवॉल द्वारपाल के रूप में काम करता है और आने वाले और बाहर जाने वाले पैकेट को नियंत्रित करता है, लेकिन एंटी-वायरस निरीक्षक है जो मशीन में दुर्भावनापूर्ण गतिविधि को नियंत्रित करता है।
d) फ़ायरवॉल नेटवर्क लेयर पैकेट को नियंत्रित करता है, और एंटी-वायरस एप्लिकेशन लेयर पैकेट को नियंत्रित करता है।

उत्तर: C) एक फ़ायरवॉल द्वारपाल के रूप में काम करता है और आने वाले और बाहर जाने वाले पैकेट को नियंत्रित करता है, लेकिन एंटी-वायरस निरीक्षक है जो मशीन में दुर्भावनापूर्ण गतिविधि को नियंत्रित करता है।

68. वेब सर्वर SSL प्रमाणपत्र बनाने के लिए क्या आवश्यक है?

a) डोमेन नाम
b) IP पता
c) मालिक का नाम
d) उपरोक्त सभी

उत्तर: a) डोमेन नाम

69. फ़िशिंग संदर्भित करता है

a) एक हमलावर एक दुर्भावनापूर्ण पृष्ठ विकसित करता है जो वास्तविक वेब पेज के समान दिखता है। पीड़ित दुर्भावनापूर्ण पृष्ठ तक पहुंचता है, जो समान लगता है, और क्रेडेंशियल प्रदान करता है।
b) एक हमलावर वास्तविक डोमेन के समान डोमेन नाम का उपयोग करता है, जिससे पीड़ित अपने पृष्ठ तक पहुंच जाते हैं।
c) एक हमलावर वायरशार्क के माध्यम से नेटवर्क में जाने वाले उपयोगकर्ता अनुरोध पैकेट को कैप्चर करता है और क्रेडेंशियल्स निकालता है।
d) एक हमलावर क्रेडेंशियल एकत्र करने के लिए एक असुरक्षित वेब पेज विकसित करता है।

उत्तर: A) एक हमलावर एक दुर्भावनापूर्ण पृष्ठ विकसित करता है जो वास्तविक वेब पेज के समान दिखता है। पीड़ित दुर्भावनापूर्ण पृष्ठ तक पहुंचता है, जो समान लगता है, और क्रेडेंशियल प्रदान करता है।

70. एक नया टैब जो होम टैब से खोला जाता है, होम टैब को दुर्भावनापूर्ण वेब पेज पर रीडायरेक्ट करता है, उसे क्या कहा जाता है?

a) फॉरवर्ड टैबस्टेल
b) रिवर्स टैबनाबिंग
c) फॉरवर्ड टैबनाबिंग
d) क्लिपबोर्ड चोरी

Ans: B) रिवर्स टैबनाबिंग

71. सीआईए के संक्षिप्त नाम में 'मैं' क्या है?

a) सूचना
b) बुद्धि
c) अखंडता
d) इंटरैक्ट

उत्तर- अखंडता

72) निम्नलिखित में से कौन सी सेवा गति में सुरक्षित डेटा में मदद करती है?

a) एफ़टीपी
b) जियो-फेंसिंग
c) वीपीएन
d) नेटकैट

उत्तर- वीपीएन

73) SHA1 हैश कितने बिट का होता है?

अ) 256
ब) 160
स) 128
घ) 64

उत्तर- 160

74) OWASP का पूर्ण रूप क्या है?

a) ऑनलाइन वेब अनुप्रयोग सुरक्षा परियोजना
ख) ओपन वेब एक्सेस सुरक्षा परियोजना
ग) ऑनलाइन वेब एक्सेस सुरक्षा परियोजना
d) वेब अनुप्रयोग सुरक्षा परियोजना खोलें

उत्तर- ओपन वेब एप्लिकेशन सिक्योरिटी प्रोजेक्ट

75) कौन सी भेद्यता ब्रोकन एक्सेस कंट्रोल का हिस्सा है?

a) इंजेक्शन
b) स्थानीय फ़ाइल समावेशन
c) एक्सएसएस
d) फ़ाइल अपलोड भेद्यता

उत्तर- स्थानीय फ़ाइल समावेशन

76) लिनक्स में किस निर्देशिका में अधिकांश सेवाओं और अनुप्रयोगों के लॉग शामिल हैं?

a) /usr/log
बी) /var/लॉग
सी) /etc/लॉग
d) /होम/लॉग

उत्तर- /var/log

77) डीएमएल का क्या अर्थ है?

a) डेटा प्रबंधन भाषा
b) डिस्क प्रबंधन भाषा
c) डिस्क प्रबंधन भाषा
d) डेटा मैनिपुलेशन लैंग्वेज

Ans- डेटा मैनिपुलेशन लैंग्वेज

78) कौन सी कमजोरियां डेटाबेस की अनधिकृत पहुंच में मदद करती हैं?

a) एसक्यूएलआई
b) एक्सएसएस
c) सीएसआरएफ
d) आरएफआई

उत्तर- एसक्यूएलआई

79) निम्नलिखित में से कौन सी भेद्यता सत्र अधिग्रहण में मदद करती है?

a) एसक्यूएलआई
b) एक्सएसएस
c) एसएसआरएफ
d) एलएफआई

उत्तर- XSS

80) कैसे एक SQLi vulnerabiltiy पैच किया जा सकता है?

a) आईपी की ब्लैकलिस्टिंग का उपयोग करना
b) HTML एन्कोडिंग का उपयोग करना
c) HTTPOnly ध्वज का उपयोग करना
d) पैरामीटर किए गए प्रश्नों का उपयोग करना

उत्तर- पैरामीटर किए गए प्रश्नों का उपयोग करना

81. लिनक्स में, किस फाइल में उपयोगकर्ता खाता जानकारी होती है?

a) /etc/छाया
b) /etc/passwd
ग) /etc/उपयोगकर्ता
d) /etc/accounts

उत्तर: b) /etc/passwd

82. विंडोज़ में उपयोगकर्ता खातों को प्रबंधित करने के लिए किस उपकरण का उपयोग किया जाता है?

a) उपयोगकर्ता प्रबंधक
b) खाता प्रबंधक
c) स्थानीय उपयोगकर्ता और समूह
d) उपयोगकर्ता प्रोफाइल

उत्तर: c) स्थानीय उपयोगकर्ता और समूह

83. लिनक्स में एक फ़ाइल के लिए अनुमति 'rwxr-xr--' का क्या अर्थ है?

ए) मालिक के लिए पढ़ें, लिखें और निष्पादित करें; समूह के लिए पढ़ें और निष्पादित करें; दूसरों के लिए पढ़ें
बी) मालिक के लिए पढ़ें और निष्पादित करें; समूह के लिए लिखें; दूसरों के लिए कोई अनुमति नहीं
ग) मालिक के लिए लिखें और निष्पादित करें; समूह के लिए पढ़ें; दूसरों के लिए निष्पादित करें
डी) मालिक के लिए पढ़ें और लिखें; समूह के लिए पढ़ें; दूसरों के लिए लिखें

उत्तर: ए) मालिक के लिए पढ़ें, लिखें और निष्पादित करें; समूह के लिए पढ़ें और निष्पादित करें; दूसरों के लिए पढ़ें

84. एंटीवायरस सॉफ़्टवेयर को कितनी बार अद्यतन किया जाना चाहिए?

a) वर्ष में एक बार
b) महीने में एक बार
c) साप्ताहिक
d) नियमित रूप से, क्योंकि अपडेट उपलब्ध हैं

उत्तर: d) नियमित रूप से, क्योंकि अपडेट उपलब्ध हैं

85. लिनक्स में, स्थापित पैकेजों को अपडेट करने के लिए किस कमांड का उपयोग किया जाता है?

a) एपीटी-गेट अपडेट
b) यम अद्यतन
C) डीएनएफ अपडेट
d) उपरोक्त सभी

उत्तर: d) उपरोक्त सभी

86. फ़ाइल अनुमतियों का प्राथमिक उद्देश्य क्या है?

a) सिस्टम प्रदर्शन को बढ़ाने के लिए
b) फ़ाइलों और निर्देशिकाओं तक पहुंच को नियंत्रित करने के लिए
c) फाइलों को व्यवस्थित करने के लिए
d) भंडारण क्षमता बढ़ाने के लिए

उत्तर: b) फ़ाइलों और निर्देशिकाओं तक पहुंच को नियंत्रित करने के लिए

87. लिनक्स में /etc/shadow **फाइल का प्राथमिक उद्देश्य क्या है?**

a) उपयोगकर्ता अनुमतियों को स्टोर करें
b) एन्क्रिप्टेड पासवर्ड स्टोर करें
c) उपयोगकर्ता समूहों को स्टोर करें
d) उपयोगकर्ता प्रोफ़ाइल संग्रहीत करें

उत्तर: b) एन्क्रिप्टेड पासवर्ड स्टोर करें

88. लिनक्स में कौन सी लॉग फ़ाइल प्रमाणीकरण प्रयासों को रिकॉर्ड करती है?

a) /var/log/syslog
बी) /वार/लोग/आठ।लोग
ग) /var/log/kern.log
d) /var/log/dmesg

उत्तर: b) /var/log/auth.log

89. लिनक्स में, लॉग फ़ाइल की अंतिम कुछ पंक्तियों को देखने के लिए किस कमांड का उपयोग किया जा सकता है?

A) सिर
b) पूंछ
C) जीआरईपी
d) बिल्ली

उत्तर: b) पूंछ

90. निम्नलिखित में से कौन सा आमतौर पर सिस्टम लॉग में शामिल नहीं है?

a) उपयोगकर्ता लॉगिन प्रयास
b) नेटवर्क ट्रैफ़िक आँकड़े
c) अनुप्रयोग त्रुटियाँ
d) सिस्टम बूट इवेंट

उत्तर: b) नेटवर्क ट्रैफ़िक आँकड़े

QUIZ (MODULE-1)

1.Which of the following is a common type of cyber threat that involves malicious software designed to damage or disrupt systems?

a) Malware
b) Phishing
c) Man-in-the-Middle (MITM) attack
d) Denial-of-Service (DoS) attack
Answer: a) Malware

2. What is the primary goal of a phishing attack?

a) To steal sensitive information by masquerading as a legitimate entity
b) To overload a system with traffic to disrupt service
c) To intercept and alter communications between two parties
d) To install malicious software on a target system
Answer: a) To steal sensitive information by masquerading as a legitimate entity

3. Which aspect of the CIA triad focuses on maintaining the accuracy and completeness of data?

a) Confidentiality
b) Integrity
c) Availability
d) Authentication

Answer: b) Integrity

4. Which of the following best describes a potential threat to "Availability" in the CIA triad?

a) Unauthorized access to sensitive data
b) Data corruption or tampering
c) Denial-of-Service (DoS) attacks
d) Data breaches

Answer: c) Denial-of-Service (DoS) attacks

5. What does TTP stand for in the context of the MITRE framework?

a) Tactics, Techniques, and Procedures
b) Tools, Technologies, and Protocols
c) Threats, Targets, and Plans
d) Techniques, Tactics, and Processes

Answer: a) Tactics, Techniques, and Procedures

6. **What is the purpose of the Cyber Kill Chain model?**

a) To identify and categorize stages of a cyber attack

b) To prevent malware from infecting systems

c) To monitor network traffic for anomalies

d) To encrypt data during transmission

Answer: a) To identify and categorize stages of a cyber attack

7.Which of the following best describes a Distributed Denial of Service (DDoS) attack?

a) An attack launched from a single source to overwhelm a target
b) An attack using multiple compromised systems to flood the target with traffic
c) An attack that exploits software vulnerabilities to gain access to a system
d) An attack that involves phishing to obtain user credentials

Answer: b) An attack using multiple compromised systems to flood the target with traffic

8. What distinguishes cybersecurity from cybercrime?

a) Cybersecurity is about protecting systems, while cybercrime is about exploiting them
b) Cybersecurity involves physical security, while cybercrime involves digital threats
c) Cybersecurity deals with hardware, while cybercrime deals with software
d) Cybersecurity is the legal framework, while cybercrime is the technical implementation
Answer: a) Cybersecurity is about protecting systems, while cybercrime is about exploiting them

9. In the context of MITRE ATT&CK, what is the significance of "Adversary Emulation"?

a) Simulating the behavior of adversaries to test and improve defensive measures

b) Encrypting sensitive data to protect it from unauthorized access

c) Installing security patches to fix vulnerabilities

d) Monitoring network traffic for suspicious activity

Answer: a) Simulating the behavior of adversaries to test and improve defensive measures

10. Which stage of the Cyber Kill Chain involves the attacker taking control of the compromised system and establishing communication?

a) Delivery
b) Command and Control
c) Exploitation

d) Installation

Answer: b) Command and Control

11. What is a common purpose of using multi-factor authentication (MFA)?

a) To reduce the complexity of password management

b) To ensure that only administrators have access to systems

c) To enhance security by requiring multiple forms of verification

d) To automate the process of password recovery

Answer: c) To enhance security by requiring multiple forms of verification

12.Fill in the blank: _____ attacks involve intercepting and altering the communication between two parties to steal or manipulate data.

a) DNS Hijacking

b) DdoS

c) Man-in-the-Middle (MITM)

d) Phishing

Answer: c) Man-in-the-Middle (MITM)

13. What is the primary purpose of data protection laws?

a) To prevent data breaches at all costs

b) To regulate how personal data is collected, stored, and used

c) To ensure that all data is encrypted

d) To allow companies to sell personal data

Answer: b) To regulate how personal data is collected, stored, and used

14. What is the primary function of CERT-In?

a) To conduct cybersecurity audits for private companies

b) To respond to cybersecurity incidents and assist in their resolution

c) To monitor internet traffic for illegal activities

d) To regulate internet service providers (ISPs) in India

Answer: b) To respond to cybersecurity incidents and assist in their resolution

15. How often are organizations required to report cybersecurity incidents to CERT-In according to the 2022 cybersecurity directions?

a) Within 4 hours of identifying the incident

b) Within 6 hours of identifying the incident
c) Within 12 hours of identifying the incident
d) Within 24 hours of identifying the incident

Answer: b) Within 6 hours of identifying the incident

16. Which of the following is a key component of implementing Zero Trust Architecture?

a) Using a single firewall to protect the network
b) Ensuring all devices within the network are trusted by default
c) Implementing strict identity verification and access controls
d) Allowing unrestricted access to internal resources

Answer: c) Implementing strict identity verification and access controls

Answer the questions based on the given scenario

Incident 1: The Aadhar database, which contains sensitive information such as names, addresses, phone numbers, and biometric data of Indian citizens, has been compromised. Attackers have gained unauthorized access to this data and are possibly exploiting it for various malicious activities.

17. Which MITRE ATT&CK tactic does gaining unauthorized access to the Aadhar database most closely align with?

a) Execution

b) Initial Access

c) Lateral Movement

d) Exfiltration

Answer: b) Initial Access

18. What MITRE ATT&CK technique could an attacker use to gain access to the Aadhar database through compromised user credentials?

a) T1078: Valid Accounts

b) T1059: Command and Scripting Interpreter

c) T1071: Application Layer Protocol

d) T1046: Network Service Scanning

Answer: a) T1078: Valid Accounts

Incident 2: WannaCry ransomware is a type of malicious software that spread rapidly across computer networks in May 2017. It encrypted files on affected systems and demanded a ransom payment in Bitcoin for the decryption key. The ransomware exploited a vulnerability in the Windows operating system, specifically leveraging the EternalBlue exploit to spread.

19. Which specific Windows vulnerability was exploited by WannaCry to spread rapidly?

a) CVE-2017-0144 (EternalBlue)
b) CVE-2016-0051 (SMBv2 Information Disclosure)
c) CVE-2017-0199 (Office/WordPad Remote Code Execution)
d) CVE-2015-0001 (Windows Kernel Privilege Escalation)

Answer: a) CVE-2017-0144 (EternalBlue)

20. After infecting a system, WannaCry displayed a ransom note demanding payment in Bitcoin. Which MITRE ATT&CK tactic does this action represent?

a) Impact
b) Command and Control
c) Exfiltration
d) Discovery

Answer: a) Impact

Case Scenario: 1

Your organization, XYZ Inc., recently experienced an incident where several employees received an email that appeared to be from the CEO. The email requested that these employees urgently transfer sensitive company data and provide login credentials for a secure company database. The email had the CEO's signature and was sent during off-hours. Shortly after, multiple employees reported their accounts being compromised, and there was an unauthorized transfer of company funds.

Based on this scenario, answer the following questions (1-5):

1: Identify the type of cyber threat described in the scenario.
A. Malware
B. Phishing
C. Denial of Service (DoS)
D. Man-in-the-Middle (MitM)

2: What specific phishing technique is being used in the scenario?
A. Smishing
B. Vishing
C. Clone Phishing
D. Whaling

3: Which motivation is most likely behind the attack in this scenario?
A. Activism
B. Espionage
C. Financial Gain
D. Revenge

4: What immediate action should the IT security team take upon discovering the compromise?
A. Ignore the incident
B. Transfer additional funds to a secure account
C. Disable affected accounts and initiate a security audit
D. Send out an email requesting more information from all employees

5: What long-term measure should XYZ Inc. implement to prevent similar attacks in the future?
A. Increase the number of employees handling sensitive data
B. Implement regular cybersecurity awareness training
C. Reduce the number of security audits
D. Encourage employees to share passwords for better access

Answers: 1: B, 2: D, 3: C, 4: C, 5: B

Case Scenario: 2

E-Commerce Solutions Inc. has recently experienced a significant disruption in its online services. For several hours, legitimate customers were unable to access the company's website, causing a substantial loss in sales and customer dissatisfaction. Upon investigation, the IT team discovered that the disruption was caused by an overwhelming flood of traffic directed at the website, originating from numerous compromised devices worldwide. The company's reputation has taken a hit, and they are considering measures to prevent such incidents in the future.

Based on this scenario, answer the following questions (6-10):

6: Identify the type of attack described in the scenario.
A. Phishing
B. Malware
C. Distributed Denial-of-Service (DDoS)
D. Man-in-the-Middle (MitM)

7: What is the primary difference between a DoS attack and a DDoS attack?
A. A DoS attack uses multiple sources to target a single system, whereas a DDoS attack originates from a single source.
B. A DoS attack floods the target with traffic from one source, while a DDoS attack uses multiple compromised devices to flood the target.
C. A DoS attack is less harmful than a DDoS attack.
D. There is no difference; both terms are interchangeable.

8: Which of the following is NOT a typical impact of a DDoS attack?
A. Financial Loss
B. Increased website traffic
C. Reputational Damage
D. Loss of Productivity

9: Which mitigation strategy involves distributing traffic across a global network of servers to manage a DDoS attack?
A. Traffic Filtering
B. Rate Limiting
C. Anycast Networking
D. Incident Response Plan

10: What long-term measure should E-Commerce Solutions Inc. implement to minimize the impact of future DDoS attacks?
A. Reduce the number of employees
B. Implement DDoS Mitigation Services
C. Ignore minor traffic spikes
D. Increase sales promotions

Answers: 6: C, 7: B, 8: B, 9: C, 10: B

Case Scenario: 3

XYZ Tech Solutions Corp. has recently detected unusual activity on its network. Upon investigation, the IT security team discovered that sensitive emails between executives had been intercepted and altered, leading to misunderstandings and potential financial losses. Additionally, employees reported being redirected to fake websites when trying to access internal services. The security team identified the presence of a rogue Wi-Fi hotspot within the company's premises and suspected that attackers had set it up to intercept and manipulate the network traffic.

Based on this scenario, answer the following questions (11-15):

11: Identify the type of attack described in the scenario.
A. Advanced Persistent Threat (APT)
B. Insider Threat
C. Man-in-the-Middle (MitM)
D. Denial of Service (DoS)

12: Which method used in MitM attacks is most likely involved in this scenario?
A. DNS Spoofing
B. Malicious Wi-Fi Networks
C. SSL Stripping
D. Public USB Charging Ports

13: What preventive measure would have helped in detecting and preventing this type of attack?
A. Use of secure Wi-Fi networks and VPNs
B. Implementing rate limiting on the network
C. Training employees on password management
D. Regular software updates

14: Which characteristic of Advanced Persistent Threats (APTs) is NOT directly relevant to the scenario described?
A. Targeted Attacks
B. Persistence
C. Stealthy
D. DNS Spoofing

15: Which of the following is a recommended long-term measure for XYZ Tech Solutions Corp. to prevent similar MitM attacks?
A. Increase the number of public Wi-Fi hotspots
B. Encourage the use of public USB charging ports
C. Implement two-factor authentication (2FA) for accessing sensitive systems
D. Reduce employee training sessions

Answers: 11: C, 12: B, 13: A, 14: D, 15: C

Case Scenario: 4

Recently, XYZ Corporation fell victim to a cyberattack, resulting in significant/huge financial losses, operational disruptions, and reputational damage. The attack targeted the company's financial data and customer information, leading to widespread panic among employees and customers alike. Investigations revealed that the attack originated from a sophisticated group with access to advanced hacking tools and techniques. As the security team works tirelessly to contain the breach and mitigate the damage, the company's executives are grappling with the aftermath, including potential legal and regulatory consequences.

Based on this scenario, answer the following questions (16-20):

16: Identify the primary threat actor likely responsible for the cyberattack described in the scenario.
A. Nation-States
B. Cybercriminals
C. Hacktivists
D. Insiders

17: What motivation is most commonly associated with the identified threat actor in the scenario?
A. Financial gain
B. Espionage
C. Political or social causes
D. Thrill of hacking

18: Which impact of cyber threats is NOT directly mentioned in the scenario?
A. Legal and regulatory consequences
B. Psychological and emotional impact
C. Physical damage
D. Reputational damage

19: What potential legal challenge might XYZ Corporation face as a result of the cyberattack?
A. Increased customer trust
B. Positive publicity
C. Regulatory fines and compliance requirements
D. Decreased operational disruptions

20: Considering the scenario, what long-term measure should XYZ Corporation prioritize to prevent future cyberattacks?
A. Implementing advanced endpoint security solutions
B. Encouraging employees to use personal devices for work
C. Ignoring the incident and moving on
D. Providing cybersecurity training to employees

Answers: 16: B, 17: A, 18: C, 19: C, 20: D

21. What do attackers in OTP fraud use a common method to trick victims into revealing their OTP?
A. Sending a fake job offer
B. Phishing emails or calls claiming to be from a bank
C. Offering free software updates
D. Providing fraudulent investment opportunities

22. Why is reporting cybercrimes considered crucial?
A. It helps initiate investigations and protect victims.
B. It provides marketing insights for tech companies.
C. It increases internet usage and traffic.
D. It boosts sales for cybersecurity software.

23. How can a cyber attack on critical infrastructure affect a nation's economy?
A. By improving the efficiency of financial transactions
B. By leading to economic paralysis and affecting banking transactions
C. By increasing the availability of goods
D. By boosting the stability of transportation networks

24. What is NOT a recommended preventive measure for strengthening an organization's cybersecurity posture?
A. Regular risk assessments and management
B. Adoption of recognized cybersecurity frameworks
C. Ignoring the use of multi-factor authentication (MFA.
D. Implementing industry-specific standards and best practices

25. In the context of the Indian IT Act 2008, which aspect is specifically aimed at fostering e-commerce growth?
A. Electronic Records and Contracts
B. Regulation of Certifying Authorities
C. Cybercrime Prevention Measures
D. Data Protection Guidelines

26. Which example best demonstrates the role of digital signatures in the Indian IT Act 2008?
A. Filing an online tax return
B. Verifying an electronic contract
C. Purchasing goods through an e-commerce platform
D. Encrypting personal data for security

Answers: 21: B, 22: A, 23: B, 24: C, 25: A, 26: B

27. A data principal notices that their personal information on a financial services website is outdated and includes errors. They are concerned that these inaccuracies might affect their account management and financial transactions. Which right allows the data principal to correct or update their personal information on the financial services website?
A. Right to Access Information About Personal Data
B. Right to Correction & Erasure of Personal Data
C. Right of Grievance Redressal
D. Right to Data Portability

28. A user is unhappy because their personal data was shared with a third party without their consent. They want to understand what data was shared and with whom and seek clarity on how their data is being handled. Which right enables the user to obtain a summary of their personal data processing activities and information about third-party data sharing?
A. Right to Correction & Erasure of Personal Data
B. Right to Access Information About Personal Data
C. Right of Grievance Redressal
D. Right to Data Portability

29. What is a key objective of strategic planning in warfare?
A. Direct engagement between opposing forces.
B. Gathering and analyzing information about the enemy.
C. Implementing specific operations and maneuvers to win battles.
D. Developing long-term strategies to achieve military goals.

30. What is the primary role of the Data Protection Board of India, as outlined in DPDPA Section 18?
A. To draft new data protection laws
B. To oversee the implementation and enforcement of data protection laws
C. To handle marketing and public relations for data protection
D. To regulate data storage and cloud computing services

Answers: 27: B, 28: B, 29: D, 30: B

QUIZ (MODULE-3)

1. Which of the following is NOT a type of cryptographic algorithm?

a) Symmetric Key Algorithm

b) Asymmetric Key Algorithm

c) Hashing Algorithm

d) Linear Search Algorithm

Answer: d) Linear Search Algorithm

2. In symmetric key cryptography, the key used for encryption and decryption is:

a) Different

b) The same

c) Public

d) Private

Answer: b) The same

3. Which of the following algorithms is an example of asymmetric key cryptography?

a) DES

b) AES

c) RSA

d) MD5

Answer: c) RSA

4. The process of converting plain text into cipher text is known as:

a) Decryption

b) Encryption

c) Hashing

d) Encoding

Answer: b) Encryption

5. What does the term "brute force attack" refer to in cryptography?

a) Guessing the key by trying every possible combination

b) Intercepting the key during transmission

c) Analyzing the patterns in the encrypted text

d) Modifying the cipher text without the key

Answer: a) Guessing the key by trying every possible combination

6. Which of the following is an example of a cryptographic hash function?

a) RSA

b) AES

c) SHA-256

d) Diffie-Hellman

Answer: c) SHA-256

7. In public key infrastructure (PKI), what is the role of a Certificate Authority (CA)?

a) Encrypting data

b) Decrypting data

c) Issuing digital certificates

d) Generating private keys

Answer: c) Issuing digital certificates

8.What is the purpose of the SSL/TLS protocol in email communication?

a) Encrypting email contents

b) Verifying the recipient's email address

c) Compressing email attachments

d) Filtering spam emails

Answer: a) Encrypting email contents

9.Which of the following is a method to ensure the authenticity of an email message?

a) Digital Signature

b) Spam Filter

c) Antivirus Software

d) Firewall

Answer: a) Digital Signature

10.What is the primary function of a spam filter in email security?

a) Encrypting emails

b) Blocking unsolicited emails

c) Verifying sender identity

d) Archiving emails

Answer: b) Blocking unsolicited emails

QUIZ (MODULE-4)

1. Which of the following is incorrect concerning the SSL protocol?
    a) SSL is a protocol that establishes a secure tunnel between the sender and receiver to ensure confidentiality.
    b) SSL is a protocol that establishes a secure tunnel between the sender and receiver to ensure integrity.
    c) SSL is a protocol that establishes a secure tunnel between the sender and receiver to ensure availability.
    d) SSL is a protocol that uses a digital certificate to ensure the service provider authentication.

Ans: C

2. Which entities are not members of the Public Key Infrastructure (PKI)?
    a) Certificate Authority: A server or authority responsible for issuing the certificate
    b) User: A client request for the certificate
    c) Registration Authority: A server or authority does the registration of the request
    d) DNS server: A server responsible for providing the IP address to send the certificate request

Ans: D

3. Which of the following is NOT a parameter in the INBOUND firewall rule of Windows?
    a) Source and the Remote device Address
    b) Source and the Destination device Port
    c) Transport and Network Layer Protocols
    d) Domain Name

Ans: D

4. DNS hijacking takes the users to the malicious website so that _____
    a) User credentials will be collected
    b) User activity will be recorded
    c) User will be provided with incorrect information
    d) All the above

Ans: D

5. Which of the following refers to the “changing the resource record in the cache to perform the poisoning”?
    a) DNS Poisoning
    b) ARP Poisoning
    c) SSL Certificate Spoofing
    d) Firewall rule poisoning

Ans: A

6. Why does accessing public Wi-Fi bring a security issue?
    a) The communication between the devices to the Wi-Fi access point may be insecure, allowing for the man in the middle attack.
    b) HTTPS-based communication always ensures a secure tunnel through the access point between the device and the server.
    c) Any malicious user can access the packets flowing in the air to collect sensitive information.

d) The Wi-Fi access point will not provide access to all the websites that we are intended to access.
Ans: A

7. Which of the following differentiates the firewall and the Anti-Virus of the machine?
a) Firewall is to secure the network, and Anti-Virus is to secure the machine
b) The firewall ensures access control, and the anti-virus controls authorization.
c) A firewall works as the gatekeeper and controls the incoming and outgoing packets, but the Anti-Virus is the invigilator that controls the malicious activity in the machine.
d) The firewall controls the network layer packets, and the anti-virus controls the application layer packets.
Ans: C

8. What is required to create the Web Server SSL certificate?
a) Domain Name
b) IP address
c) Owner Name
d) All the above
Ans: A

9. Phishing refers to
a) An attacker develops a malicious page that looks precisely the same as the genuine web page. The victim accesses the malicious page, which seems the same, and provides the credentials.
b) An attacker uses the same domain name as the genuine domain, making victims access their page.
c) An attacker captures the user request packet going in the network through wireshark and extracts the credentials.
d) An attacker develops an insecure web page to collect the credentials.
Ans: A

10. A new tab that gets opened from a home tab redirects the home tab to a malicious web page is called as
a) Forward Tabsteal
b) Reverse Tabnabbing
c) Forward Tabnabbing
d) Clipboard stealing
Ans: B

QUIZ (MODULE-5)

1. What is 'I' in acronym CIA?

a) Information

b) Intelligence

c) Integrity

d) Interact

Ans- Integrity

2) Which of the following services help in secure data in motion?

a) FTP

b) Geo-fencing

c) VPN

d) netcat

Ans- VPN

3) SHA1 hash is of how many bits?

a) 256

b) 160

c) 128

d) 64

Ans- 160

4) What is the full form of OWASP?

a) Online Web Application Security Project

b) Open Web Access Security Project

c) Online Web Access Security Project

d) Open Web Application Security Project

Ans- Open Web Application Security Project

5) Which vulnerability is the part of Broken Access Control?

a) Injection

b) Local File Inclusion

c) XSS

d) File upload vulnerability

Ans- Local File Inclusion

6) Which directory in linux include logs of most of the services and applications?

a) /usr/log

b) /var/log

c) /etc/log

d) /home/log

Ans- /var/log

7) What does DML stands for?

a) Data Managing Language

b) Disk Management Language

c) Disk Managing Language

d) Data Manipulation Language

Ans- Data Manipulation Language

8) Which of the vulnerabilities help in unauthorized access of database?

a) SQLi

b) XSS

c) CSRF

d) RFI

Ans- SQLi

9) Which of the following vulnerabilities help in session takeover?

a) SQLi

b) XSS

c) SSRF

d) LFI

Ans- XSS

10) How an SQLi vulnerabiltiy can be patched?

a) Using blacklisting of IPs

b) Using HTML encoding

c) Using HTTPOnly flag

d) Using parameterized queries

Ans- Using parameterized queries

OS PROTECTION QUIZ

1. In Linux, which file contains user account information?

a) /etc/shadow
b) /etc/passwd
c) /etc/users
d) /etc/accounts

Answer: b) /etc/passwd

2. Which tool is used to manage user accounts in Windows?

a) User Manager
b) Account Manager
c) Local Users and Groups
d) User Profiles

Answer: c) Local Users and Groups

3.What does the permission 'rwxr-xr--' mean for a file in Linux?

a) Read, write, and execute for owner; read and execute for group; read for others
b) Read and execute for owner; write for group; no permissions for others
c) Write and execute for owner; read for group; execute for others
d) Read and write for owner; read for group; write for others

Answer: a) Read, write, and execute for owner; read and execute for group; read for others

4. How often should antivirus software be updated?

a) Once a year
b) Once a month
c) Weekly
d) Regularly, as updates are available

Answer: d) Regularly, as updates are available

5. In Linux, which command is used to update installed packages?

a) apt-get update
b) yum update
c) dnf update
d) All of the above

Answer: d) All of the above

6. What is the primary purpose of file permissions?

a) To enhance system performance
b) To control access to files and directories
c) To organize files
d) To increase storage capacity

Answer: b) To control access to files and directories

7. What is the primary purpose of the /etc/shadow **file in Linux?**

a) Store user permissions
b) Store encrypted passwords
c) Store user groups
d) Store user profiles

Answer: b) Store encrypted passwords

8. Which log file in Linux records authentication attempts?

a) /var/log/syslog
b) /var/log/auth.log
c) /var/log/kern.log
d) /var/log/dmesg

Answer: b) /var/log/auth.log

9. In Linux, which command can be used to view the last few lines of a log file?

a) head
b) tail
c) grep
d) cat

Answer: b) tail

10.Which of the following is NOT typically included in system logs?

a) User login attempts
b) Network traffic statistics
c) Application errors
d) System boot events

Answer: b) Network traffic statistics