تحديات الأمن الرقمي للبيانات

استكشاف ثغرات الاختراق وتطبيقاتها في عصر تدفق البيانات

Digital data security challenges

أ.د. / منـــال البلقـــاسي

أستاذ نظم المعلومات المساعد ووكيل الجودة وخدمة المجتمع معهد الإدارة كفر الشيخ ، كاتبة في المعلوماتية والذكاء الاصطناعي

2024

مقدمة الكتاب :

في ظل تزايد استخدام التكنولوجيا في حياتنا اليومية، أصبحت البيانات لدينا تحت الاختبار المستمر للأمان والحماية. فمع كل تقدم تكنولوجي يأتي تهديد جديد يهدد خصوصيتنا وسلامة بياناتنا. تعتبر الاختراقات الصفرية اليومية للبيانات أحد أكبر التحديات التي نواجهها في عصرنا الحالي.

إن البيانات تشكل الروح التقنية للعديد من الشركات والمؤسسات، وتعتبر أساساً أساسياً لتشغيل الاقتصاد الرقمي الحديث. ومع ذلك، فإن هذه البيانات في خطر مستمر، حيث تتعرض لمخاطر الاختراقات الصفرية التي يتم تنفيذها بشكل يومي وبشكل متزايد حيث تتضمن الاختراقات الصفرية تلك الهجمات التي يتم من خلالها استغلال الثغرات الأمنية في أنظمة المعلومات والشبكات، سواء كانت تلك الثغرات ناتجة عن أخطاء في التصميم أو في تنفيذ البرامج، أو نتيجة للهندسة الاجتماعية والتي تستهدف الجانب البشري من الأمان السيبراني.

تشكل هذه الاختراقات تهديداً حقيقياً للحياة الشخصية والمؤسسية، حيث يمكن أن تتسبب في فقدان البيانات الحساسة، والتسريبات الكبيرة، والتلاعب بالمعلومات، مما يؤدي في النهاية إلى تبعات كبيرة ومدمرة على الصعيدين الشخصي والمهني لذا، يتطلب التصدي لهذه التحديات اتخاذ إجراءات وقائية واحترازية، بما في ذلك تعزيز أمان البيانات، وتحسين الوعي الأمني لدى المستخدمين، وتطوير الحلول التقنية القادرة على اكتشاف ومنع الاختراقات الصفرية.

كما سيتناول هذا الكتاب بشكل شامل وموسع موضوع الاختراقات الصفرية اليومية للبيانات، بما في ذلك تحليل الأساليب المستخدمة في هذه الاختراقات، وتقديم

النصـــائح والإرشـــادات اللازمة لحماية البيانات وتعزيز الأمان الســـيبراني في مجتمعاتنا المتصلة تقنياً.

الفصـل الأول: أمن المعلومات : باسـتكشـاف مفهوم أمن المعلومات وأهميته في عصـر الرقمنة متضـمنا أسـاسـيات الأمن السـيبراني وأهميته في حماية البيانات والمعلومات الحســاســة من التهديدات الخارجية والداخلية. ســنتعرف على أهمية تطبيق مبادئ أمن المعلومات في المؤسسات والشركات وكيفية تقديم حماية فعالة للأنظمة والبيانات ضد الاختراقات والاختراقات الصفرية.

الفصل الثاني: فيروسات الحاسب : سنتعمق في فهم فيروسات الحاسب وأنواعها المختلفة، وســنبحث في كيفية انتشــارها وأســاليب الوقاية منها والتعامل معها. سنتعرف على الأضرار التي يمكن أن تسببها فيروسات الحاسب للأنظمة والبيانات، وسـنبحث في أحدث التقنيات المسـتخدمة في كشـف ومكافحة الفيروسـات. ، أما الفصـل الثالث: اختراق شـبكات البلوتوث (Bluetooth Hacking) : سـنركز على كيفية اســتغلال ثغرات أمان شــبكات البلوتوث وتنفيذ هجمات متقدمة على الأجهزة المتصــلة بهذه الشــبكات. ســنتناول أســاليب الاختراق وأدوات الهجوم المستخدمة، وكيفية حماية الأجهزة الشخصية والأنظمة من هذه الهجمات.

الفصـل الرابع: هجمات الشـبكات الخلوية (Cellular Network Attacks) : دراسـة هجمات الشـبكات الخلوية وكيفية اسـتغلال ثغرات الأمان في شـبكات الجيل الثالث والرابع. ســنتعرف على أنواع الهجمات الممكنة وتأثيرها على الاتصــالات

اللاسلكية وسلامة البيانات، وسنبحث في كيفية تقديم حماية فعالة للأجهزة المتصلة بالشبكات الخلوية.

الفصل الخامس: مكافحة جرائم التصيد والاحتيال الإلكتروني : سنتناول في هذا الفصل جرائم التصيد والاحتيال الإلكتروني وكيفية التعرف عليها والوقاية منها. سنبحث في أساليب الاحتيال الشائعة عبر الإنترنت وكيفية حماية المستخدمين من الوقوع في فخها والحفاظ على سلامة بياناتهم الشخصية والمالية.

الفصل السادس: تخزين وتحليل بيانات الروبوتات الأمنية : موضحا أهمية تخزين وتحليل بيانات الروبوتات الأمنية وكيفية استخدامها في اكتشاف ومكافحة التهديدات السيبرانية. سنتعرف على أدوات وتقنيات تحليل البيانات المستخدمة في تقديم تقارير مفصلة عن أنشطة الشبكات والأنظمة الأمنية.

الفصل السابع: التهديدات الداخلية للروبوتات الأمنية : نتناول التهديدات الداخلية للروبوتات الأمنية وكيفية التعامل معها والوقاية منها. سنبحث في كيفية تأمين الروبوتات الأمنية ضد الهجمات الداخلية والتسللات غير المصرح بها أما الفصل الثامن: تحديات الروبوتات الأمنية : نتناول التحديات التقنية والتنظيمية التي تواجه الروبوتات الأمنية وكيفية التغلب عليها. سنبحث في أحدث التطورات التقنية في مجال الروبوتات الأمنية وتحديات تطبيقها على نطاق واسع.

الفصل التاسع: تقييم جودة البرمجيات المستخدمة في الروبوتات الأمنية ، بعرض أهمية تقييم جودة البرمجيات المستخدمة في الروبوتات الأمنية وكيفية ضمان أمانها وسلامة استخدامها. سنتعرف على أساليب وأدوات التقييم البرمجي وكيفية

تطبيقها على البرمجيات الأمنية لضـــمان جودتها وفعاليتها في مكافحة التهديدات السيبرانية.

الكاتبة ،،،

26 ابريل 2024

Introduction to the book

With the increasing use of technology in our daily lives, our data is constantly being tested for security and protection. With every technological advance comes a new threat to our privacy and the integrity of our data. Zero-day data breaches are one of the biggest challenges we face today.

Data constitutes the technical soul of many companies and institutions, and is considered an essential basis for the operation of the modern digital economy. However, this data is at constant risk, as it is exposed to the risks of zero-day breaches that are increasingly being carried out on a daily basis. Zero-end breaches include those attacks in which security vulnerabilities in information systems and networks are exploited, whether these vulnerabilities result from design errors or errors. In the implementation of programs, or as a result of social engineering that targets the human side of cybersecurity.

These breaches pose a real threat to personal and organizational life, as they can cause the loss of sensitive data, large leaks, and tampering with information, which ultimately leads to major and devastating consequences on both the personal and professional levels. Therefore, addressing these challenges requires taking preventive and precautionary measures, including Enhancing data security, improving users' security awareness, and developing technical solutions capable of detecting and preventing zero-sum intrusions.

This book will also comprehensively and extensively address the topic of zero-day data breaches, including an analysis of the methods used in these breaches, and providing the necessary advice and guidance to protect data and enhance cybersecurity in our technologically connected societies.

Chapter One: Information Security: Exploring the concept of information security and its importance in the age of digitization, including the basics of cybersecurity and its importance in

protecting sensitive data and information from external and internal threats. We will learn about the importance of applying information security principles in institutions and companies and how to provide effective protection for systems and data against hacks and zero-sum intrusions.

Chapter Two: Computer Viruses: We will delve into understanding computer viruses and their different types, and we will examine how they spread and methods of preventing and dealing with them. We will learn about the damage that computer viruses can cause to systems and data, and we will examine the latest technologies used in detecting and combating viruses. As for the third chapter: Bluetooth Hacking: We will focus on how to exploit security vulnerabilities in Bluetooth networks and carry out advanced attacks on devices connected to these networks. We will discuss hacking methods and attack tools used, and how to protect personal devices and systems from these attacks.

Chapter Four: Cellular Network Attacks: Study of cellular network attacks and how to exploit security vulnerabilities in third and fourth generation networks. We will learn about the types of possible attacks and their impact on wireless communications and data integrity, and look at how to provide effective protection for devices connected to cellular networks.

Chapter Five: Combating phishing and electronic fraud crimes: In this chapter, we will discuss phishing and electronic fraud crimes and how to identify and prevent them. We'll look at common online scams and how to protect users from falling for them and keep their personal and financial data safe.

Chapter Six: Storing and analyzing security robot data: Explaining the importance of storing and analyzing security robot data and how to use it to detect and combat cyber threats. We will learn about data analysis tools and techniques used to provide detailed reports on the activities of networks and security systems.

Chapter Seven: Internal threats to security robots: We discuss internal threats to security robots and how to deal with them and prevent them. We will examine how to secure security robots against internal attacks and unauthorized intrusions. Chapter Eight: Challenges of security robots: We address the technical and organizational challenges facing security robots and how to overcome them. We will examine the latest technical developments in security robotics and the challenges of implementing them on a large scale.

Chapter Nine: Evaluating the quality of the software used in security robots. In this chapter, we will focus on the importance of evaluating the quality of the software used in security robots and how to ensure its security and safe use. We will learn about software evaluation methods and tools and how to apply them to security software to ensure its quality and effectiveness in combating cyber threats.

The writer,,,

April 26, 2024

فهرس المحتويات

الفصل الثاني : ..... ص 63

فيروسات الحاسب

- طرق انتشار الفيروسات
- اضرار الفيروسات
- طرق الحماية من اضرار الفيروسات
- اشهر الفيروسات
- خصائص الأنواع المختلفة من الفيروسات
- اضرار الأنواع المختلفة من الفيروسات
- اليات معالجة اضرار الأنواع المختلفة من الفيروسات
- اسباب انتشار الفيروسات
- اهداف فيروسات الحاسب
- نطاق الإصابة بفيروسات الحاسب
- اليات اكتشاف الإصابة بفيروسات الحاسب
- فيروسات نظم التشغيل
- فيروسات الإقلاع(Boot Sector Viruses)
- فيروسات الملفات النظامية(System File Viruses)
- فيروسات الماكرو(Macro Viruses)
- فيروسات التجسس(Spyware)
- برامج التجسس(Spyware)
- برامج مضادات الأنواع المختلفة من الفيروسات
- برمجيات الفدية(Ransomware)
- برامج مكافحة الفيروسات
- البرمجيات الدعائية(Adware)

الفصل الثالث : ..... ص 117

اختراق شبكات البلوتوث(Bluetooth Hacking)

- الثغرات الأمنية في تقنية البلوتوث
- معالجة الثغرات الأمنية في تقنية البلوتوث
- أساليب اختراق تقنية البلوتوث
- الهجمات الشهيرة على شبكات البلوتوث
- إجراءات حماية أجهزة البلوتوث من الاختراق
- تعطيل البلوتوث عندما لا يكون مطلوبًا
- الممارسات الأمنية لتعزيز أمان شبكات البلوتوث والحماية من عمليات الاختراق.

الفصل الرابع : ..... ص 139

هجمات الشبكات الخلوية(Cellular Network Attacks)

- اختراق الأجهزة الفيزيائية
- التصرف غير المصرح به
- سوء الاستخدام العمدي
- التسريب غير المقصود للمعلومات
- التهديدات الداخلية الأخرى
- مهددات الروبوتات الأمنية
- اليات التغلب علي التهديدات الأمنية للروبوتات
- الذكاء الاصطناعي والتعلم الآلي لمعالجة مهددات الروبوتات الأمنية
- التحليل التنبؤي والتوجيه للتصدي للتهديدات المستقبلية
- الكشف عن الاحتيال والتلاعب
- نظام الكشف التلقائي(Automated Detection Systems)

- نظام الكشف التلقائي (Automated Detection Systems)
- الاستجابة السريعة (Rapid Response)
- التحليل التلقائي والتقارير (Automated Analysis and Reporting)
- التعلم الآلي والتحسين المستمر (Machine Learning and Continuous Improvement)
- التنسيق مع البشر (Human Coordination)
- تحسين الأجهزة والبنية التحتية
- تطوير الخوارزميات والتقنيات الجديدة
- تحسين عمليات التخزين والاسترجاع
- قياس كفاءة وأداء الروبوتات الأمنية
- السياسات واللوائح المحلية والدولية لاستخدام الروبوتات الأمنية
- تطبيقات الروبوتات المحسنة بالذكاء الاصطناعي(AIoT)
- تكنولوجيا الواقع المعزز (AR) والواقع الافتراضي(VR)

الفصل الخامس : ..... **ص 223**

مكافحة جرائم التصيد والاحتيال الإلكتروني

- قوانين الأمن السيبراني في القطاع الخاص
- تشريعات التعاون الدولي
- السلوكيات الأخلاقية المتعلقة باختبار الثغرات الأمنية واختبار الاختراق
- اكتشاف الروبوتات الأمنية
- اكتشاف الروبوتات الأمنية
- اقتراحات الروبوتات بناءً على معرفتها بالمستخدم
- تخصيص إعدادات الروبوتات الأمنية وفقًا لتفضيلاتهم الشخصية
- التواصل الإيمائي للروبوتات الامنية

تحديات الروبوتات الأمنية

- الهجمات السيبرانية المتطورة
- هجمات الاختراق المتقدمة والمستهدفة(APT)
- البرمجيات الخبيثة المتقدمة(Advanced Malware)
- التشفير والضغط
- التخفي في الذاكرة
- استغلال الثغرات الصفرية
- الهجمات المتعددة المراحل
- التعديل الديناميكي
- استخدام التقنيات الذكية
- الهجمات الهجينة (Hybrid Attacks)
- التصيد الاجتماعي المستهدف(Spear Phishing)
- الاختراقات الصفرية اليومية(Zero-Day Exploits)
- هجمات الإسقاط الخفي(Evasive Attacks)
- التشفير المتقدم
- التعديل الديناميكي
- الاستخدام المزيف للأوامر الشرعية
- الاستخدام الذكي للبنية التحتية السحابية

الفصل التاسع : ..... **ص 307**

تقييم جودة البرمجيات المستخدمة في الروبوتات الأمنية

- اعتبارات نشر الروبوتات الأمنية في البيئات العامة
- أفضل ممارسات حماية الروبوتات الأمنية من الاختراقات السيبرانية

- تعزيز تكامل الروبوتات الأمنية مع أنظمة الإنذار
- التكامل مع أنظمة الإنذار
- التكامل مع أنظمة الكشف عن الحرائق
- واجهات برمجية موحدة (APIs) للتواصل بين الروبوتات الأمنية وأنظمة الأمان الأخرى
- استخدام تقنيات تحليل البيانات المشتركة لتحليل البيانات المستخرجة من الروبوتات الأمنية
- تنظيم تدريبات مشتركة لفرق الأمان للتعامل مع سيناريوهات الحوادث المحتملة
- تقييم دوري لفعالية التكامل وتحديث الأنظمة والبرمجيات وفقًا لتطور التهديدات الأمنية واحتياجات الأمان
- استراتيجيات تقديم التدريب للمشغلين البشريين حول استخدام الروبوتات الأمنية
- تحسين القدرة على التواصل بين الروبوتات الأمنية والأفراد لتحقيق تجربة استخدام موثوقة وسلسة
- تكامل مصادر بيانات الروبوتات الأمنية
- الكاميرات، وأجهزة الاستشعار، وأنظمة الإنذار
- قوانين الخصوصية والأمان لاستخدام الروبوتات الأمنية
- التقنيات المستقبلية لتطوير الروبوتات الأمنية
- الحوسبة الحيوية (Quantum Computing)
- التشفير والحماية السيبرانية المتقدمة
- تأثير الحوسبة الحيوية (Quantum Computing)على قدرات الروبوتات الأمنية
- الحوسبة الحافية (Edge Computing)
- الروبوتات ذاتية التعلم(Self-Learning Robots)

- تكامل الروبوتات الأمنية مع الطائرات بدون طيار (الدرون)

الفصل العاشر : ..... ص 357

المبادئ الأخلاقية للقرصنة المعلوماتية

- أنواع القرصنة الأخلاقية
- أخلاقيات القرصنة الحاسوبية
- تقنيات اختراق الأمان
- استغلال الثغرات البرمجية(Exploits)
- كتابة برامج الاستغلال(Exploit Development)
- التحليل الأمني(Security Analysis)
- تحليل الثغرة(Vulnerability Analysis)
- تطوير الاستغلال(Exploit Development)
- اختبار الاستغلال(Exploit Testing)
- التضمين في أدوات الاختراق (Integration into Penetration Testing Tools)
- استخدام البيانات المضللة(Fuzzing)
- هجمات التصيّد(Phishing Attacks)
- هجمات التصيّد الاجتماعي(Social Engineering Attacks)
- هجمات فحص الشبكة(Network Scanning Attacks)
- اختراق كلمات المرور (Brute Force Attacks)
- استغلال ضعف بروتوكولات الشبكة(Protocol Exploitation)
- بروتوكول نقل النصف الآمن(SSL/TLS)
- بروتوكول نقل البريد البسيط(SMTP)
- بروتوكول نقل الملفات(FTP)

- بروتوكول نقل النصف الفوري IMAP) و(POP
- بروتوكولات تطبيقات الويب HTTP) و(HTTPS
- اختراق أمان الويب:(Web Security Exploitation)
- ثغرات حقن الشفرة(Code Injection)
- تحليل الضعف الأمني في الأنظمة والتطبيقات والشبكات
- تشريعات القرصنة والأمن السيبراني
- قوانين ولوائح القرصنة الأخلاقية والأمان السيبراني
- حماية البيانات الشخصية
- تأمين البنية التحتية الحيوية