مشروع متكامل حول الحماية من الاختراقات،

مشروع: حماية المعلومات وتقليل المخاطر

مقدمة
تعد الاختراقات الأمنية من أكبر التهديدات التي تواجه المؤسسات والأفراد في العصر الرقمي. يشملهذا المشروع دراسة شاملة حول كيفية حماية المواقع والشبكات من الاختراقات، بالإضافة إلى استراتيجيات وتقنيات تقليل المخاطر.

1.تعريف الاختراقات
الاختراق هو عملية تمكن المهاجم من الوصول غير المصرح به إلى الأنظمة أو البيانات. يمكن تقسيم

الاختراقات إلى:
- اختراق المواقع: مثل هجمات SQL Injection، Cross-Site Scripting (XSS)، وInclusion (RFI) Remote File
- اختراق الشبكات: مثل هجمات Man-in-the-Middle، والاستغلال من خلال الشبكات اللاسلكية.

2.أسباب الاختراقات
- ضعف كلمات المرور.
- ثغرات البرمجيات.
- عدم تحديث الأنظمة.
- نقص الوعي الأمني بين المستخدمين.

3.تقنيات الحماية من الاختراقات
أ. حماية المواقع
- تحديث البرمجيات: الحفاظ على تحديثات النظام وإصلاح الثغرات.
- تشفير البيانات: استخدام بروتوكولات HTTPS لتأمين البيانات أثناء النقل.
- تحقق من المدخلات: التحقق من صحة المدخلات لمنع هجمات SQL Injection وXSS.
- جدران الحماية :(Firewalls) استخدام جدران الحماية لحماية الخوادم من الهجمات.

ب. حماية الشبكات
- تأمين الشبكة اللاسلكية: استخدام تشفير WPA3وكلمات مرور قوية.
- تجزئة الشبكة: تقسيم الشبكة إلى شبكات فرعية لتحسين الأمان.
- استخدام :VPN حماية البيانات أثناء نقلها عبر الشبكات العامة.
- مراقبة الشبكة: استخدام أدوات لمراقبة نشاط الشبكة واكتشاف الهجمات.

4.استراتيجيات تقليل المخاطر
- إجراء تدقيق أمني منتظم: تقييم الثغرات بشكل دوري.
- تدريب المستخدمين: تعزيز الوعي الأمني بين الموظفين والمستخدمين.
- تطوير سياسة أمنية: وضع سياسات واضحة للأمان تتضمن إجراءات الاستجابة للحوادث.

5.مشروع عملي
أداة اختبار اختراق
يمكنك إنشاء أداة بسيطة باستخدام Python لفحص الثغرات في المواقع، مثل:
- التحقق من نقاط ضعف SQL Injection.
- اختبار XSS.

مستند توثيق
قم بتوثيق خطوات الأداة واستخدامها وتقديم النتائج.

6.خاتمة
تلخيص أهم النقاط حول كيفية حماية المواقع والشبكات، والتأكيد على أهمية الوعي الأمني والتحديث المستمر للأنظمة.

7.المراجع
1.كتب وأدلة
- "Web Application Security: A Beginner's Guide" by Bryan Sullivan and Vincent Liu
- "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto
- "Metasploit: The Penetration Tester's Guide" by David Kennedy et al.
- "Hacking: The Art of Exploitation" by Jon Erickson

2.برامج أدوات الأمان مثل:
- **Nmap:** Nmap
- **Burp Suite:** Burp Suite
- **Wireshark:** Wireshark
- **Metasploit Framework:** Metasploit
- **OWASP ZAP:** OWASP ZAP

3.أنظمة التشغيل مثل:
- **Kali Linux:** Kali Linux
- **Parrot Security OS:** Parrot Security
- **BackBox:** BackBox

4.مواقع متخصصة في حماية البيانات:
- **OWASP:** OWASP
- **CIS:** CIS
- **SANS Institute:** SANS
- **NIST:** NIST
- **US-CERT:** US-CERT

5.تحديثات البرمجيات:
- **WSUS:** WSUS
- **apt:** APT
- **yum:** YUM

6.أبحاث ومقالات أكاديمية:
- **IEEE Xplore:** IEEE Xplore
- **ACM Digital Library:** ACM
- **Google Scholar:** Google Scholar

7.منصات تعليمية:
- **Coursera:** Coursera
- **edX:** edX
- **Udemy:** Udemy

8.مدونات ومقالات تقنية:
- **Krebs on Security:** Krebs
- **Dark Reading:** Dark Reading
- **Security Weekly:** Security Weekly

9.مواقع توفر أدوات تقييم الثغرات:
- **Qualys:** Qualys
- **Nessus:** Nessus

- قام بتصميم هذا الملف: م / مشاري الشراري
- حسابات التواصل:
- تويترVXV10_Q
- ميتاء_F5X9
- مكان رفع الملفGITHUB:

URL: https://github.com/HACK-MR-B/Cyber-prevention.git