هل شبكتك آمنة؟ 5 هجمات سيبرانية شائعة لازم تعرفها!

التهديدات السيبرانية دايمًا بتتطور. فهم الهجمات الشائعة لاختراق الشبكات هو أول خطوة لحماية مؤسستك.

Omar Hamed | omarhamed.sec@gmail.com
Google Cybersecurity Notes

Made with GAMMA

1. Spoofing & Sniffing: التهديدات المخفية

Packet Sniffing

الهجوم ده بيكون عن طريق قراءة **Data Packets** وهي ماشية جوه الشبكة.
ممكن يكون **Passive** (مجرد قراءة بس) أو **Active** (تغيير أو التلاعب بالبيانات وهي في الطريق).

IP Spoofing

المهاجمين بيغيّروا عنوان الـ **Source IP** في الـ **Data Packets** علشان يتقمصوا نظام مُصرَّح له، وبكده يقدروا ياخدوا وصول للشبكة من غير إذن.

الطرق دي بتسمح للمهاجمين إنهم يعترضوا أو يغيّروا البيانات، وده ممكن يؤدي لتسريب معلومات أو اختراق النظام.

Omar Hamed | omarhamed.sec@gmail.com
Google Cybersecurity Notes

Made with GAMMA

2. Denial of Service (DoS) Attacks: غزاة الشبكة

DoS Attack

بيستهدف شبكة أو سيرفر عن طريق إغراقه بحركة مرور بيانات غير مرغوب فيها، علشان يخليه غير متاح للمستخدمين الشرعيين.

DDoS Attack

نوع من هجمات الـ **DoS** بيستخدم أجهزة كتير من أماكن مختلفة لإغراق شبكة الهدف بحركة مرور بيانات.

SYN Flood Attack

بيحاكي اتصال **TCP** عن طريق إغراق السيرفر بـ **SYN Packets** علشان يستهلك موارده.

الهجمات دي هدفها تعطيل الخدمات، وده بيؤدي لتوقف التشغيل وتأثير كبير على سير العمليات.

Omar Hamed | omarhamed.sec@gmail.com
Google Cybersecurity Notes

Made with GAMMA

3. ICMP Flood & Ping of Death: تكتيكات متقدمة لهجمات الحرمان من الخدمة (DoS)

1

ICMP Flood Attack

المهاجم بيبعت بشكل متكرر **ICMP Packets** لسيرفر الشبكة، وده بيغرقه ويؤدي لحرمانه من تقديم الخدمة (**Denial of Service**).

2

Ping of Death

الهاكر بيبعت **ICMP Packet** بحجم أكبر من 64KB للنظام، وده بيخليه ينهار أو يهنج.

الأنواع المحددة دي من هجمات الـ **DoS** بتستغل بروتوكولات الشبكة علشان تحقق أهدافها التخريبية.

Omar Hamed | omarhamed.sec@gmail.com
Google Cybersecurity Notes

Made with GAMMA

4. Brute Force Attacks: خمن طريقة دخولك

Simple Brute Force

المهاجمين بيجربوا تركيبات مختلفة من أسماء المستخدمين وكلمات المرور لحد ما يلاقوا بيانات الدخول الصحيحة.

Dictionary Attacks

مشابه لهجوم الـ **Brute Force**، لكن بيستخدم قائمة جاهزة بكلمات مرور شائعة أو كلمات من القاموس علشان يحصل على الوصول.

الهجمات دي بتعتمد على الإصرار والقوة الحاسوبية علشان تكسر كلمات المرور الضعيفة أو الشائعة.

Omar Hamed | omarhamed.sec@gmail.com
Google Cybersecurity Notes

Made with GAMMA

5. On-Path & Replay Attacks: اعتراض البيانات

1

On-Path Attack

جهة خبيثة بتحط نفسها في النص بين طرفين بيتواصلوا، وبتعترض أو تغيّر البيانات وهي في الطريق.

2

Replay Attack

هجوم شبكي بيقوم فيه الفاعل الخبيث باعتراض **Data Packet** وهي في الطريق، وبعدها يأخر إرسالها أو يعيد إرسالها في وقت تاني.

الهجمات دي بتضر **سلامة البيانات – Data Integrity** وسريتها – **Confidentiality** عن طريق التلاعب في تدفق الاتصال.

Omar Hamed | omarhamed.sec@gmail.com
Google Cybersecurity Notes

Made with GAMMA

إزاي الهجمات بتضر مؤسستك

Information Leaks

البيانات الحساسة ممكن تتسرق، وده بيؤدي لانتهاك الخصوصية ودفع غرامات تنظيمية.

Damaged Reputation

الحوادث الأمنية بتقوّض ثقة العملاء وبتأثر سلبًا على الصورة العامة للشركة.

Financial Costs

التعافي من الهجمات بيتطلب وقت ومجهود وفلوس كتير، وده بيشمل أتعاب قانونية وإصلاح الأنظمة.

Customer Retention

فقدان الثقة ممكن يخلي العملاء يسيبوا الشركة ويروحوا للمنافسين.

عواقب اختراقات الشبكات بتتجاوز بكتير المشاكل التقنية الفورية.

Omar Hamed | omarhamed.sec@gmail.com
Google Cybersecurity Notes

Made with GAMMA

احمي شبكتك: الإجراءات الأساسية

Security Hardening

تقوية الأنظمة وتقليل الثغرات عبر الـ **Hardware**، وأنظمة التشغيل (**OS**)، والتطبيقات، والشبكات.

MFA & Strong Passwords

تطبيق **Multi-Factor Authentication** وسياسات كلمات مرور قوية علشان تمنع الوصول غير المصرح به.

Firewalls & Encryption

استخدم جدران الحماية (Firewalls) عشان تصفي حركة البيانات وتشفّرها، وبكده بتحمي البيانات سواء وهي في طريقها (في الانتقال) أو لما تكون مخزنة (في الراست).

الإجراءات الأمنية الاستباقية ضرورية عشان تبني دفاع قوي ومرن ضد التهديدات السيبرانية.

Omar Hamed | omarhamed.sec@gmail.com
Google Cybersecurity Notes

Made with GAMMA

أدوات الأمن الشبكي الأساسية

Firewall	بيسمح أو بيمنع حركة البيانات حسب قواعد معينة.	بيصفّي بس بناءً على رؤوس الحزم (packet headers)، ومش بيقدر يوقف الهجمات المعقدة والمتطورة.
IDS	بيرصد وبيبلغ المسؤولين عن الاختراقات اللي بتحصل.	بيفحص بس الهجمات المعروفة، ومبيوقفش حركة البيانات الواردة.
IPS	بيراقب النشاط وبيتخذ إجراءات عشان يوقف الاختراقات.	ممكن يمنع حركة بيانات شرعية، ولو فشل في الحماية، الاتصال بينقطع.
SIEM	بيجمع ويحلل بيانات السجلات (LOG) من أكتر من جهاز.	بيبلغ بس عن المشاكل اللي بتحصل، ومبيعملش أي إجراءات عشان يوقف الأحداث دي.

اختيار الأدوات المناسبة مهم جدًا لحماية شاملة للشبكة.

Omar Hamed | omarhamed.sec@gmail.com
Google Cybersecurity Notes

Made with GAMMA

ابقَ سابق التهديدات السيبرانية!

هم الهجمات الشائعة على اختراق الشبكات مهم جدًا لأي مؤسسة. حماية أصولك الرقمية بتحتاج مراقبة مستمرة وممارسات أمان قوية.

Don't wait for an attack to happen. Strengthen your defences today!

شارك البوست ده عشان تساعد غيرك يحمي شبكاته

Made with GAMMA