مقدمة في المعلومات

الجزء الثاني: القراصنة

أ. د. أسامة حسام الدين

2021

المحتوى العام

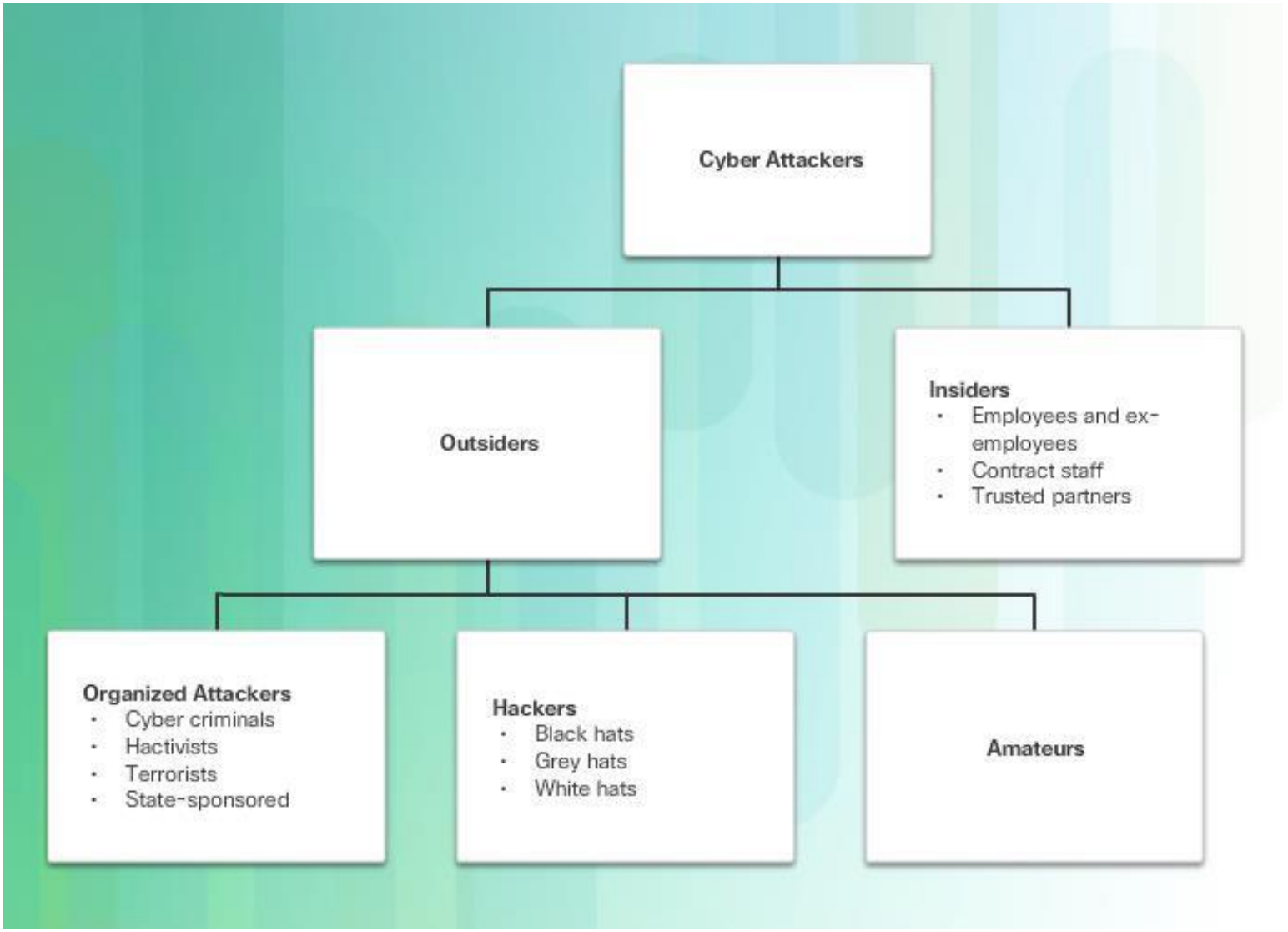
- الجزء الأول: المستخدم.
- **الجزء الثاني: القراصنة.**
- الجزء الثالث: الهجمات.
- الجزء الرابع: طرق الحماية.

القراصنة

أنواع القراصنة

- صغار القراصنة script kiddies.
- القراصنة المحترفون hackers، القبعة البيضاء والسوداء والرمادية.

أنواع القراصنة



- داخليون.
- خارجيون.

المنظمات الإجرامية

.هي عبارة عن مجموعات من القراصنة المنظمين من النشطاء والإرهابيين وأحيانا يتم دعمهم من قبل الدولة.

.*المجرمون السيبرانيون* :هم مجموعة من المجرمين المحترفين يركزون على التحكم والسيطرة والثروة. هم محترفون للغاية ومنظمون جدا. ومن الممكن أن يقوموا بعرض خدماتهم الإجرامية لغيرهم من المجرمين مقابل المال.

.*المخترقون النشطاء* :يقومون بالدفاع عن موقف سياسي لجلب الانتباه لهم ودعم موقفهم السياسي.

.*المخترقون الدوليون* :يتم تبنيهم من قبل الدول وتدريبهم على اعلى درجة من التدريب والتعقيد مع تمويلهم بما يلزم من عتاد

الثغرات الأمنية

الثغرات الأمنية هي عادة تحدث بسبب وجود خلل في البرامج أو العتاد

يستخدم المهاجم البرمجية وتسمى " "**Exploit**وهي برنامج مكتوب بغرض الاستفادة من الثغرات الأمنية. استخدام البرمجية في استغلال الثغرة الأمنية يسمى في الأمن المعلوماتي عملية الهجوم "**Attack**"

الفرق بين **الثغرة** vulnerability **التهديد** :Threat الثغرة خلل داخلي للنظام، أما التهديد فهو الخطر من الخارج. يوجد أيضا المخاطرة Riskوتعني احتمال حدوث الهجوم

الثغرة مثل وجود خلل معين في البرنامج يفتح منفذ دون حاجة، والتهديد مثل القراصنة والزلازل، والمخاطرة مثل نقل البيانات غير مشفرة.

الثغرات البرمجية

تحدث الثغرات في البرامج بسبب خطأ في برمجة نظام التشغيل أو تطبيق.

- على الرغم من محاولة سد الثغرات من قبل المطورين إلا انه دائما ما تظهر ثغرات جديدة، ويحتاج بعدها التطبيق إلى تعديل أو ترقية.
- في عام 2015م حدث اختراق لنظام التشغيل الخاص بشركة سيسكو (IOS) والمثبت على الموجهات الخاصة بالشركة، وقد حدث هذا الاختراق بعد انزال نسخة غير كاملة من نظام التشغيل (IOS) على الموجهات.
- لتجنب مثل هذه الاختراقات تأكد من إعطاء صلاحيات محدودة للأشخاص ذوي الاختصاص للوصول للعتاد (مثل الموجهات في الشبكة السابقة)

ثغرات العتاد Hardware

- عادة ما تحدث الثغرات الأمنية للعتاد بسبب عيب في التصميم.
- على سبيل المثال الذاكرة العشوائية يتم تصميمها باستخدام مكثفات متجاورة، ونظرا لهذا التجاور فأن التأثير على احدها من الممكن أن يؤثر على المكثف المجاور.
- بناء على هذا العيب في التصميم تم استغلال التجاور في الوصول إلي مناطق في الذاكرة غير مصرح بها فيما يسمى بهجمة Rowhammer.
- على الرغم من أن هجمات العتاد هي هدف للهجمات الكبرى إلا أن الحماية منها تتم ببرمجيات ونظم حماية فيزيائية بسيطة.

أنواع الثغرات البرمجية

.فيض الذاكرة المؤقتة buffer overflow: يتم ملئ الذاكرة المؤقتة حتى تكتب في مكان غير مسموح به بغرض تجاوز تعطيل الذاكرة أو نظام التحكم بالوصول

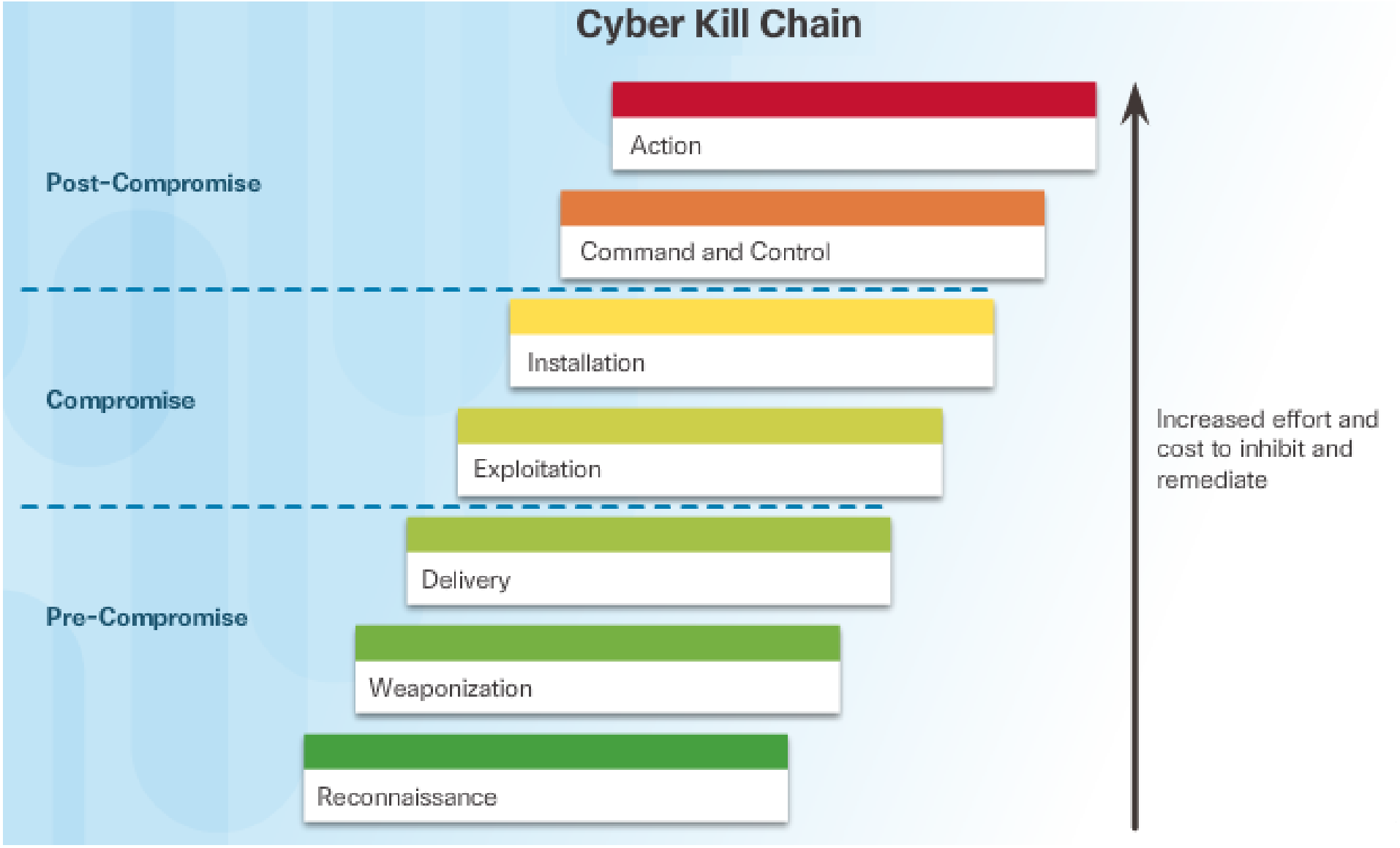
.المدخلات غير الصحيحة :مثل محاولة تعطيل البرنامج بأن يجعل تعليمة برمجية فيه تقسم على الصفر مثلا < خطأ قاتل >

.حالات التسابق Race conditions: محاولة الوصول لنفس المكان في نفس الوقت من أكثر من عملية أو مستخدم.

.ضعف في النظام الأمني :النظام الأمني مبرمج بشكل ضعيف

.أخطاء في نظم التحكم بالوصول :إعطاء صلاحيات لشخص ليس لديه تلك الصلاحيات عن طريق الخطأ.

سلسلة القتل


Cyber Kill Chain
Post-Compromise
Compromise
Pre-Compromise
Action
Command and Control
Installation
Exploitation
Delivery
Weaponization
Reconnaissance
Increased effort and cost to inhibit and remediate

سلسلة القتل

1) الاستكشاف – يتم تجميع أكبر قدر من المعلومات عن الضحية.
2) التسلح – يقوم المهاجم بإعداد العدة بمعنى عمل برنامج مخصص لثغرة ما ثم كتابة الشفرة الخاصة بالوظيفة الخبيثة ثم يرسل ذلك إلى الضحية.
3) التسليم – يقوم المهاجم بإرسال البرمجية الخبيثة إلى الضحية عن طريق البريد الإلكتروني أو أي طريقة أخرى.
4) الاستغلال – استغلال الثغرة في توصيل البرمجية الخبيثة إلى الهدف.
5) التثبيت – يتم تثبيت "باب خلف "أو أي برمجية خبيثة على الجهاز الضحية.
6) الأمر والتحكم – يتم التحكم عن بعد بالضحية من خلال قنوات التحكم أو عن طريق خادم.
7) الفعل الخبيث – وفيها يقوم المهاجم بالفعل الخبيث كسرقة الهوية، أو استخدام الأجهزة المسيطر عليها في الهجوم على أجهزة أخرى بداخل الشبكة أو بالمرور بسلسلة القتل والمعاودة باستخدامها مرة أخرى.

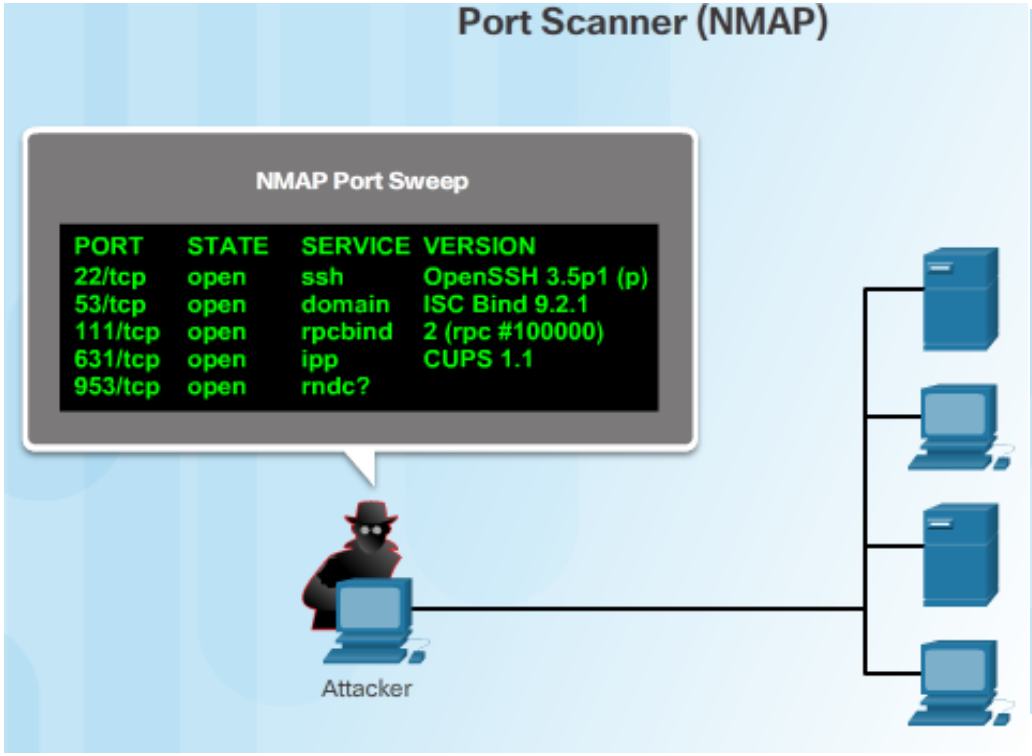
سلسلة القتل | مثال

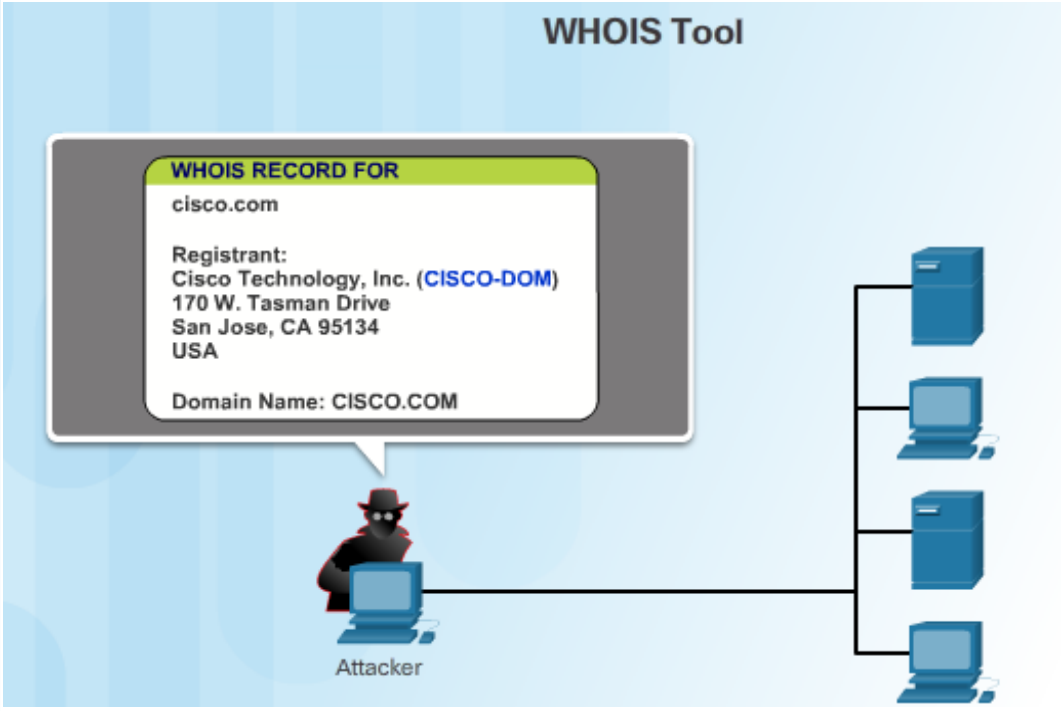
الخطوة الأولى :وفيها يتم جمع اكبر قدر من المعلومات عن الجهاز الضحية .ويتم استخدام اكثر من طريقة في ذلك مثل الهندسة الاجتماعية، أو مسح المنافذ port scanning الخاصة بالأجهزة.

الخطوة الثانية :أي معلومة ولو بسيطة من التي تم جمعها في الخطوة الأولى ممكن أن تكون هي مفتاح الكنز. مثلا اسم نظام التشغيل المستخدم، رقم الإصدار الخاص به. قائمة بالخدمات الجارية على الجهاز.

الخطوة الثالثة :عند معرفة اسم نظام التشغيل وإصداره يبدأ المهاجم في البحث عن الثغرات ونقاط الضعف الخاصة بهذه

سلسلة القتل | مثال





عرض بسيط لكيفية الاستطلاع واستكشاف المنافذ المفتوحة في موقع ويب

سؤال ؟