

A large, semi-transparent white triangle is positioned on the left side of the image, pointing towards the right. Inside this triangle is a stylized logo of a building with three stars above it, resting on an open book. To the right of the triangle is a vertical blue bar. On the blue bar, the same logo is displayed again, along with the text "مركز الأكاديمية" (Academy Center) and "الإسكندنافية للتدريب" (Scandinavian Training).

Banking

DATA

downloading 70%

25%

Mobile | 00966536473335 : Mobile | 00966112695229 : Phone : 00966552365295

info@scandinavianacademy.co : Email | <https://scandinavianacademy.co> : Web site

المملكة العربية السعودية - الرياض - حي الخليج - شارع الشيخ عبد العزيز بن عبد الرحمن بن بشر - 13223 - مكتب رقم 5 P.O.BOX : 13224



دورة: الأساليب الاحتيالية في اختراق شبكات البنوك وكيفية الوقاية منها

ال코드	المدينة	الفندق	نهاية التدريب	بداية التدريب	نهاية الدورة - الساعات	السعر	لغة الدورة
BIC-910	الرياض	فندق فندقية	2026-06-21	2026-06-25	25	SR 8950	العربية -

الأهداف من الدورة التدريبية

- الحفاظ على أمن وسرية معلومات وبيانات حسابات العملاء داخل البنوك وبما يكفل تحقيق الاستقرار والسلامة لجميع أعمال قطاعات البنك وبمختلف إداراته من خلال الكشف على أهم الأساليب الاحتيالية التي يقوم بها المحتالون في اختراق المواقع والشبكات المصرفية المختلفة.

المستهدفون من الدورة التدريبية

- جميع الموظفين الذين يعملون في قطاع البنوك بمختلف إداراته وفروعه وبكافأة خدماته المصرفية الإلكترونية والتقليدية.
- إداريو أمن ونظم المعلومات ممن لديهم الرغبة في تطوير مهاراتهم الأمنية، والتعرف على الأدوات الأمنية اللازمة لحماية الشبكة الخاصة بمؤسساتهم.
- مدراء الأمن التقني الراغبون بالاطلاع على كيفية توفير أفضل مستويات الحصانة الأمنية لمؤسساتهم ضد مخترقي الشبكات.

محفوبيات الدورة التدريبية

- من هم القرادنة؟ وكيفية تصنيفهم ونشأتهم ودوافعهم.
- ما المقصود بعملية اختراق وقرادنة بيانات وحسابات عملاء البنوك داخل الأجهزة والشبكات.
- طرق معرفة القرادنة لأنواع أنظمة المواقع المستهدفة داخل البنوك ومحفوبياتها وإخراج معلوماتها .
- كيفية استخدام القرادنة لمحركات البحث الشهيرة (Ex. Google) في البحث عن البنك الضحية لاختراقه.



- أنواع موقع البنوك الإلكترونية (eBanking) واستراتيجية اختراقها من خلال القرصنة .
- استراتيجية اختيار القرصنة للجهاز الذي يود اختراقه وأهم الأشياء التي يبحث عنها داخل البنك.
- الأدوات التي تساعد القرصنة على اختراق الأجهزة والخوادم داخل البنك وطريقة تتبعها والتعرف عليها للوقاية منها.
- طرق خداع القرصنة لمستخدمي الأجهزة داخل البنك ليصاب بملفات التجسس Spyware وأحصنة طروادة Trojan والفيروسات Viruses لتسهيل عملية الاختراق.
- كيفية استغلال القرصنة لمبدأ تنمية العلاقات الاجتماعية والاختلاط داخل البنك في تنظيم عمليات الاختراق والتجسس (Social Engineering Attack).
- ما المقصود بـ Phishing (اصطياد عملاء البنك) وطرق تصميمها واستخدامها من قبل القرصنة.
- أشهر برامج القرصنة وتصنيف تأثيرها وقوتها.
- ما هو الشيل (Shell) وكيفية استعماله ورفعه؟
- شرح أهم أوامر صلاحيات وتصاريح الدخول داخل أنظمة اليونيكس Unix واللينكس Linux والتي يستخدمها القرصنة في الاختراق داخل البنك.
- كيفية استخدام الـ Sniffing من قبل القرصنة لمعرفة جميع الثغرات والمنفذ داخل شبكة البنك الداخلية والخارجية.
- طرق اخراج وإستغلال القرصنة لأغلب الثغرات الأمنية والمنفذ داخل البنك وكيفية إغلاقها.
- طرق استخدام القرصنة لاختراق كلمات السر الرئيسية والعبور عن طريق الـ Brute Force.
- طرق استخدام القرصنة لتفصيل Encryption وفك تشفير Decryption كلمات السر لاختراق الخوادم الرئيسية والأجهزة داخل البنك من خلال أخذ ورفع الصلاحيات .
- طرق القرصنة الاحتياطية في تخفيص صلاحيات المستخدم ورفعها للاختراق.
- شرح استغلال ثغرات Command Execution + Remote File Disclosure + SQL Injection
- كيفية استخدام القرصنة للباكتور (Backdoor) لاختراق أجهزة وخوادم البنك.
- كيفية قيام القرصنة بالتعديل على قاعدة البيانات لتغيير معلومات المشرف الرئيسي Admin لرفع الصلاحيات وتغيير الفهرسة Index من لوحة التحكم.



- كيفية استغلال القراءنة للـ FTP والـ Telnet في الدخول على الأجهزة والتعديل على قاعدة بياناتها.
- طرق استغلال القراءنة لـ Remote Desktop في اختراق الأجهزة والخوادم الرئيسية داخل البنوك.
- طرق استغلال القراءنة لثغرات SQL لتركيب سكريبت خاص Script على أجهزة وخوادم البنك الرئيسية لتسهيل عملية اختراقها وقرصنة بياناتها.
- تتبع آثار دخول القراءنة على الأجهزة والخوادم الرئيسية داخل البنوك ودراسة طرقوهم في مسح آثارهم عند الخروج.
- أهم الاحتياطات الأمنية والإجراءات الوقائية التي يجب اتخاذها داخل البنوك للحماية من القراءنة .
- أشهر الطرق للكشف عن ملفات التجسس والاختراق داخل البنوك.



مركز الأكاديمية الإسكندنافية للتدريب يعتمد على أحدث الأساليب العلمية والمهنية في مجالات التدريب وتنمية الموارد البشرية، بهدف رفع كفاءة الأفراد والمؤسسات. يتم تنفيذ البرامج التدريبية وفق منهجية متكاملة تشمل:

- المحاضرات النظرية المدعومة بعروض تقديمية (PowerPoint) ومقاطع مرئية (فيديوهات وأفلام قصيرة).
- التقييم العلمي للمتدربين قبل وبعد البرنامج لقياس مدى التطور والتحصيل العلمي.
- جلسات العصف الذهني وتطبيقات عملية للأدوار من خلال تمثيل المواقف العملية.
- دراسة حالات عملية مصممة خصيصاً لتلائم المادة العلمية وطبيعة عمل المشاركين.
- اختبارات تقييمية تُجرى في نهاية الدورة لتحديد مدى تحقيق الأهداف التدريبية.

يحصل كل مشارك على المادة العلمية والعملية للبرنامج مطبوعة ومحفوظة على CD أو فلاش ميموري، مع تقديم تقارير مفصلة تشمل الحضور والنتائج النهائية مع التقييم العام للبرنامج.

يتم إعداد المادة العلمية للبرامج التدريبية بطريقة احترافية على يد نخبة من الخبراء والمتخصصين في مختلف المجالات والتخصصات. في ختام البرنامج، يحصل المشاركون على شهادة حضور مهنية موقعة ومعتمدة من مركز الأكاديمية الإسكندنافية للتدريب.

أوقات البرامج التدريبية :

- من الساعة 9:00 صباحاً حتى 2:00 ظهراً

البرامج التدريبية تتضمن :

- بوفيه يومي يقدم أثناء المحاضرات لضمان راحة المشاركين.
- جميع الأسعار لا تتضمن 15 % ضريبة القيمة المضافة



Scandinavian Academy

Training Center



00966112695229



info@scandinavianacademy.co



المملكة العربية السعودية - الرياض - حي الخليج - شارع الشيخ عبد العزيز بن عبد الرحمن بن بشر - 13223 - مكتب رقم 5
Riyadh - Al Khaleej District - Sheikh Abdul Aziz Bin Abdul Rahman Bin Bishr Street - 13223 - Office No. 5

Mobile | 00966536473335 : Mobile | 00966112695229 : Phone : 00966552365295

info@scandinavianacademy.co : Email | <https://scandinavianacademy.co> : Web site

المملكة العربية السعودية - الرياض - حي الخليج - شارع الشيخ عبد العزيز بن عبد الرحمن بن بشر - 13223 - مكتب رقم 5
P.O.BOX : 13224 | 5