دبلوم الأمن السيبراني الشامل من الصفر للمرحلة المتقدمة والعمل

مع المدرب سيف مخارزة

فهرس المحتوى	
مميزات الدورات	2
طريقة التدريب والنجاح في الدورات	3
تفاصيل الدورات	20-4
الأسئلة الشائعة والشهادات	21

مميزات جميع الدورات

- وصول مدى الحياة لمحتوى الدورة
- تحديث دوري للمحتوى حسب:
  - طلب الطلاب
  - ما يقتضيه المجال من تطورات
- امتحان تدريبي عملي
- إعادة الامتحان مجانا
- نضمن لك الوظيفة بعد الدورة ونساعدك في تخطي مقابلة العمل
- استراحات أثناء الدورة (أفلام عن الهاكرز، ورش عمل دورية، مجموعة للطلاب)
- الدورة مسجلة بالكامل
- دعم فني مباشر مع المدرب سيف مخارزة (يستمر بعد الدورة)
- ضمان مساعدتك على الحصول على احد الشهادات العالمية المذكورة بالأعلى (إن أحببت)
- تدريب مختلف وعملي يراعي فروقات المستوى
- حل CTF بشكل مستمر
- طرق لتطوير نفسك بعد الدورة
- لا حاجة ل لغة انجليزية (التدريب بالعربي مع التحفظ على المصطلحات الإنجليزية)
- لا حاجة لتعلم البرمجة بالبداية
- لا حاجة لأي خبرات مسبقة
- سيعرض لك المدرب قضايا واقعية وأسلوبه في جذب العملاء لخدماته لتحصل على بعض الإلهام في خطة عملك الخاصة

طريقة التدريب والنجاح
في كل الدورات

1
منصة خاصة بك كطالب تفاعلية
وتعطيك كل التحكم بالفيديوهات

2
الدورات عبارة عن فيديوهات
مسجلة تشاهدها في أي وقت تريده

3
دعم فني مباشر مع المدرب سيف مخارزة
مباشرة لأي سؤال أو مساعدة

4
مرحلة الأساسيات للمبتدئ مهما كان
مستواه تأخذ من أسبوع-12 يوم

5
الأساسيات تقدم في دوراتنا بالإضافة
لمصادر خارجية (مجانية بالكامل)

6
تصل المرحلة المتقدمة وتتدرب
بشكل عملي ممتع

7
الامتحان في نهاية الدورات عملي
سيطلب منك - على سبيل المثال
وحسب الدورة - القيام بعملية اختراق
شاملة على مختبر مجهز بثغرات عن
عمد، أو تقديم تقارير
عن منظمات اجرامية وتتبع عملياتهم
في الانترنت المظلم ... إلخ

8
انت أمير وقتك في الدورات
تستطيع أخذ الامتحان وقتما تشاء

9
إذا لم تنجح بالامتحان من المرة الأولى
فبإمكانك إعادته بعد 3 أيام مجانا

10
تحصل على الشهادة !
مبروووووك!

ستبقى الدورات ملكا لك
نحدث محتواها باستمرار وسيصلك كل تحديث مجانا

الدورة الأولى : اختبار اختراق الشبكات والسيرفرات

تقوم هذه الدورة بتحضيرك من الصفر وتعليمك مجال الأمن السيبراني الهجومي وتحديدا اختبار لإختراق بشكل عملي بحت، وتعتمد الدورة على المعايير العالمية في هذه الطريقة بحيث:

- سنقوم بتدريبك بشكل عملي باستخدام مختبرات تحاكي مواقع الشركات أو المنظمات، سيرفرات الجامعات أو البنوك، شبكات داخلية لمنظمات...إلخ ، بحيث تحتك بعملية الاختراق بشكل واقعي وعملي وممتع

- نهتم بالمبتدئين كما نهتم بأصحاب الخبرة التقنية فالدورة مصممة بحيث تناسب جميع الفئات، تحصل على الأساسيات وشرح مبسط كمبتدئ وحين تصبح جاهزا (في فترة قصيرة لا تزيد عن 10 ايام) تبدأ بالمحتوى المتقدم، وإذا كنت خبيرا فنحن نقوم بتقديم معلومات متقدمة ومختبرات ممتعة تشبع نهم التعلم للمجال

- تعتبر الدورة تدريبا كاملا وإضافيا لمن يريد الحصول على الشهادات العالمية التالية
CEH > ECSA > LPT – OSCP – PSCP – eCPPTv2

- تهتم الدورة تحديدا بمحتوى شهادة OSCP ونضيف عليه الكثير من الأساليب والطرق الجديدة في الاختراق

- نحضرك بعد الدورة لسوق العمل بحيث نساعدك في عمل الCV الخاص بك وندلك كيف تحصل على وظيفة في المجال

- نقدر في Secstien Security مبدأ العمل الحر والدخل الجيد لصاحب الخبرة الجيدة ومن هذا المنطلق سنقوم بتعليمك كيف تبني عملك الحر والخاص في المجال كمختبر اختراق وكيف تجذب العملاء لتحقيق دخل أفضل من الوظيفة

Syllabus - المحتوى

الدورة الأولى : اختبار اختراق الشبكات والسيرفرات

1 Introductions and Basics - المقدمة والأساسيات

1.1 Introduction - مقدمة الدورة
1.2 Kali Linux Walkthrough - كالي لينكس
1.3 Command Line Fun - أساسيات التعامل مع الأوامر
1.4 Network Basics for hackers - أساسيات الشبكات للهاكرز
1.5 Pentesting Stages - مراحل اختبار الاختراق
1.6 Business Needs Vs Security Needs - احتياجات العمل ضد احتياجات الأمان
1.7 Red Team Vs Blue Team - الفرق بين الأمن السيبراني الهجومي والدفاعي
1.8 Linux File Sys and Kali Prep - خوارزمية ملفات لينكس وتحضير النظام
1.9 Break and Quiz 1 - الاستراحة والاختبار الأول

2 Practical Tools - تدرب على بعض الأدوات

2.1 Netcat
2.2 Metasploit
2.3 Metasploitable Walkthrough
2.4 Wireshark Snack

3 PowerShell & Active Directory

3.1 PowerShell snack
3.2 Active Directory P1
3.3 Active Directory P2
3.4 Active Directory P3
3.5 Active Directory - Authentication P4

Syllabus - المحتوى

الدورة الأولى : اختبار اختراق الشبكات والسيرفرات

4 OSINT - جمع المعلومات مفتوحة المصدر

4.1 OSINT - Introduction - مقدمة القسم
4.2 OSINT - Website Recon P1 - جمع المعلومات عن المواقع
4.3 OSINT - Website Recon P2 - جمع المعلومات عن المواقع
4.4 OSINT - USERS Recon - جمع المعلومات عن المستخدمين
4.5 OSINT - GHBD - الاختراق عن طريق جوجل دوركس
4.6 OSINT - Shodan and Cynsys
4.7 OSINT - Internet Archive - أرشيف الانترنت

5 Real Pentesting - الاختراق العملي على مختبرات محلية

5.1 Real Pentesting - Local Lab 1
5.2 Real Pentesting - Local Lab 2
5.3 Real Pentesting - Local Lab 3
5.4 Real Pentesting - Local Lab 4

6 Real Pentesting (Cloud) - الاختراق العملي

6.1 Introduction - المقدمة
6.1.1 NOTICE - ملاحظة مهمة
6.2 Real Pentesting Lab 1
6.3 Real Pentesting Lab 2
6.4 Real Pentesting Lab 3
6.5 Real Pentesting Lab 4
6.6 Real Pentesting Lab 5
6.7 Real Pentesting Lab 6
6.8 Real Pentesting Lab 7
6.9 Real Pentesting Lab 8
6.10 Real Pentesting - The Exam - الامتحان

Syllabus - المحتوى

الدورة الأولى : اختبار اختراق الشبكات والسيرفرات

7 - Social Engineering - الهندسة الاجتماعية

7.1 Social Engineering - Intro - المقدمة

7.2 Social Engineering - The 4 - أهم 4 طرق للخداع

7.3 Social Engineering - Social Media Hacking P1 - اختراق حسابات التواصل الاجتماعي

7.4 Social Engineering - Social Media Hacking P2 - اختراق حسابات التواصل الاجتماعي

8 Web Application Attacks and Vulnerabilities - ثغرات وهجمات تطبيقات الويب

8.1 BurpSuite P1

8.2 BurpSuite P2

8.3 THE Basics - الأساسيات

8.4 Browser Tools - الاختراق بالمتصفح

8.5 Cross Site Scripting - Reflected

8.6 Cross Site Scripting - Stored

8.7 Sql Injection

8.8 File Inclusion

9 Reporting & Exam - المراجعة والامتحان

9.1 Course Walkthrough - مراجعة الدورة

9.2 Port Redirection and Tunneling

9.3 Pentesting Report Walkthrough - عمل تقرير اختبار اختراق

9.4 The Final Exam - الامتحان

10 Plus - الإضافات

10.1 How to get a job in Cyber Security - احصل على وظيفة

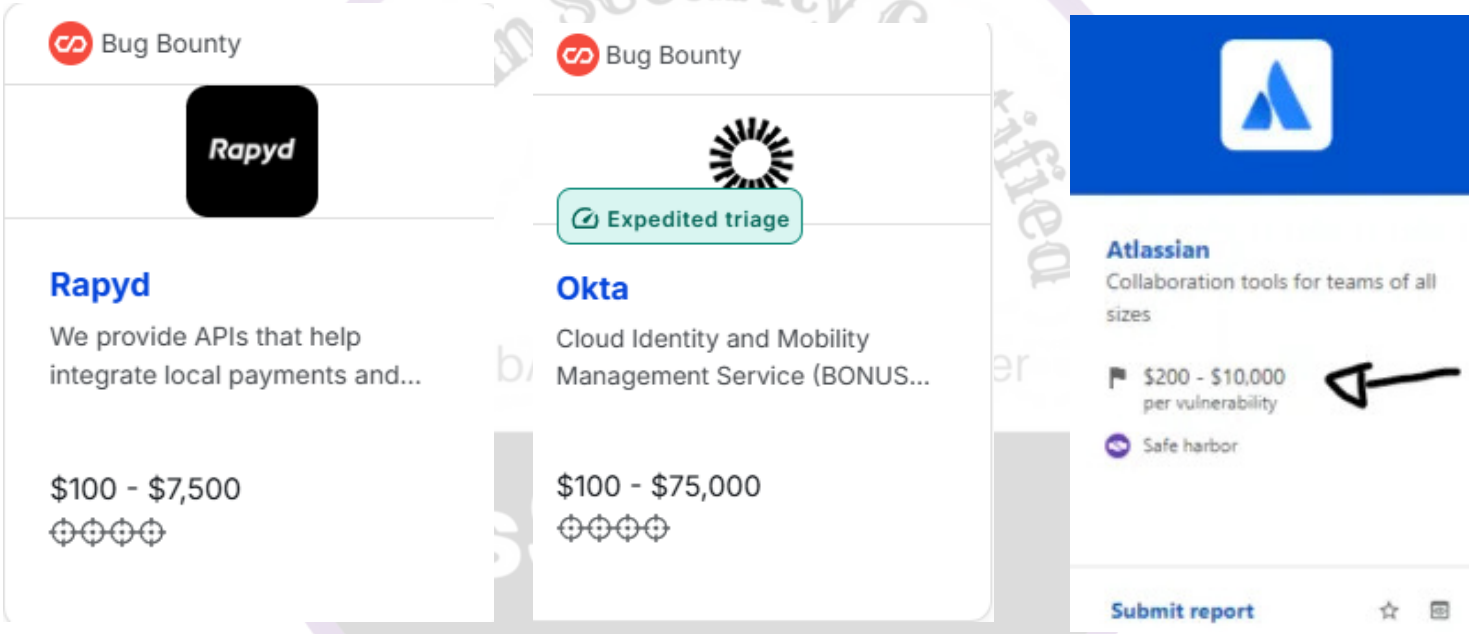
10.2 Job Interview Bypassing - تخطي مقابلة العمل

10.3 Pentester as a free-lancer - ابني عملك الحر كمختبر اختراق

الدورة الثانية: اختبار اختراق تطبيقات الويب (المواقع)

وهي دورة تؤهلك لتصبح قادرا على اختبار اختراق تطبيقات الويب والمواقع، وتؤهلك للعمل على منصات تقديم المكافئات مقابل اكتشاف الثغرات مثل:
منصة اكتشاف الثغرات السعودية، Intigriti، BugCrowd، HackerOne

- صور دلالية توضح لك حجم المكافآت التي ستحصل عليها عند اكتشاف ثغرات في مواقع مختلفة (على سبيل المثال)



ما هو مجال اكتشاف الثغرات؟

- هو مجال يهدف إلى تشجيع الخبراء الأمنيين والقراصنة ومختبرين الاختراق على الإفصاح عن الثغرات التي يجدونها في المواقع بدلًا من استغلالها لسرقة المعلومات أو ببيعها لجهات خارجية، ويتم هذا التشجيع عن طريق مكافآت مالية تدفعها الشركات إلى الباحثين الأمنيين عن طريق طرف ثالث يحفظ حق الشركات عن طريق التحقق من فاعلية الثغرات وحق صائدي الثغرات في الحصول على مكافآتهم حسب خطورة وتأثير الثغرة المبلغ عنها

ماذا سوف أتعلم في الدورة؟

- أساسيات الأمن السيبراني واختبار الاختراق والويب
- اكتشاف الثغرات في تطبيقات الويب والسيرفرات
- برنامج بورب سويت لاكتشاف الثغرات وكيفية التعامل معه واستخدامه في تطبيق الهجمات والفحص
- التعامل مع نظام كالي لينكس وإتقانه
- مفاهيم ومصطلحات خاطئة في مجال اكتشاف الثغرات
- حل المشاكل التي قد تواجهك في عملية اصطياد الثغرات
- أسس جمع المعلومات والريكون للكشف عن الثغرات بالشكل الصحيح
- كيفية التبليغ عن الثغرات المكتشفة
- كيفية استغلال الثغرات المكتشفة وعرض تأثيرها للفريق المسؤول عن التقييم
- استغلال أكثر من ثغرة معا لزيادة خطورة الثغرة المكتشفة
- تكنيكات لزيادة قيمة المكافآة بعد التلبيغ عن الثغرات
- تعلم الـ Methodology وهو بروتوكولك الخاص في تفقد وفحص الموقع لاكتشاف الثغرات بحيث تختصر الوقت والأماكن التي بحث فيها غيرك من مكتشفي الثغرات

Syllabus - المحتوى

الدورة الثانية: اختبار اختراق تطبيقات الويب (المواقع)

1.0 Introduction - المقدمة والمتطلبات والأساسيات

0.0 NOTICE - ملاحظة مهمة

1.1 Why Get Hacked and Assessment Methodologies - طرق تقييم المخاطر الأمنية

1.2 Interception proxies - طرق اعتراض الطلبات بينك وبين الموقع

1.3 OSINT p1 - جمع المعلومات

1.4 OSINT p2 - جمع المعلومات ج2

1.5 OSINT p3 - جمع المعلومات ج3

1.6 HTTP & SSL

1.7 Hashing vs encryption - الفرق بين التشفير والهاش

Section 2 (Burp and Advanced Req) - برنامج بيربسويت والمتطلبات المتقدمة

2.1 BurpSuite p1

2.2 BurpSuite p2

2.3 WAF, Domain, Subdomain, ...etc - مصطلحات مهمة

Section 3 (Vulnerabilities Walkthrough P1/2) - اكتشاف مجموعة الثغرات الأولى بشكل عملي

3.1 XSS p1

3.2 XSS p2

3.3 XSS p3

3.4 CSRF p1

3.5 CSRF p2

3.6 CSRF p3

3.7 CSRF p4

3.8 Broken Access Control p1

3.9 Broken Access Control p2

3.10 Broken Access Control p3

3.11 XML external entity XXE p1

3.12 XML external entity XXE p2

3.13 XML external entity XXE p3

3.14 SQL Injection p1

3.15 SQL Injection p2

3.16 SQL Injection p3

Syllabus - المحتوى

الدورة الثانية: اختبار اختراق تطبيقات الويب (المواقع)

Section 4 (Practical Training P1/2) - تطبيق اختراق عملي مشابه للواقع

4.1 Browser Tools - اكتشاف الثغرات بأدوات المتصفح

4.2 Content Discovery - تفقد المحتوى

4.3 OWASP TOP 10 - أخطر 10 ثغرات حسب تصنيف أواسب

4.4 Juicy Details Forensics on Hacked WebApp - تحقيق رقمي في موقع مخترق

Section 5 (Vulnerabilities Walkthrough P2/2) - اكتشاف مجموعة الثغرات الثانية بشكل عملي

5.1 File Upload Vulnerability

5.2 File Upload Vulnerability p2

5.3 Path Traversal LFI

5.4 Server Side Request Forgery SSRF

5.5 Server Side Request Forgery SSRF p2

5.6 Server Side Template Injection SSTI

5.7 OS Command Injection

5.8 Insecure Deserialization p1

5.9 Insecure Deserialization p2

5.10 JSON Web Token JWT

5.11 Authentication Vulnerabilities p1

5.12 Authentication Vulnerabilities p2

5.13 Information Disclosure

5.14 Clickjacking Vulnerabilities

Section 6 (Practical Training P2/2) - تطبيق الاختراق بشكل مشابه للواقع

6.1 Report Writing - كتابة التقارير

6.3 Practical Real Case 2 Priv Esc and MORE - تطبيق عملي واقعي

6.4 Practical Real Case 3 Web Server hacking and PrivEsc - تطبيق عملي واقعي

6.5 Practical Real Case 4 Priv Esc - تطبيق عملي واقعي

6.6 Practical Real Case 5 web servers hacking and PrivEsc - تطبيق عملي واقعي

6.7 Practical Real Case 6 Local Server and Communications hacking - تطبيق عملي واقعي

الدورة الثالثة: دورة الاختراق والاستخبارات مفتوحة المصدر

وهي دورة جديدة من نوعها على مستوى العالم تمكنك من فهم طبيعة عمل العاملين في المؤسسات الحكومية الأمنية (المخابرات المتقدمة، الأمن الوطني، وحدة الجرائم الإلكترونية)، وتقدم لك كافة المهارات التقنية التي تحتاجها للعمل مع هذه الجهات أو للعمل كمحقق خاص أو مستشار أمني في قضايا الجرائم الإلكترونية والابتزاز الإلكتروني والتجسس، لتصبح قادرًا على الإمساك بالمجرمين وجلب المعلومات عنهم وتتبع مواقعهم ومعرفة كيف يخترقون حسابات التواصل الاجتماعي الخاصة بالضحايا.

- الهدف من الدورة هو جعلك مستشار أمني للأفراد بحيث يأتيك العميل لتقوم بفحص جواله وحساباته في وسائل التواصل الاجتماعي وإذا تبين أنه قد تعرض للاختراق فبإمكانك تتبع موقع المخترق له وتقديم معلوماته في تقرير رسمي، بالإضافة لتأمين حساباته وجواله وشبكة بيته له.
- لتعلم ما ستتعلمه بشكل رسمي فأنت ستتقن في هذه الدورة الكثير من مهارات مهندس عمليات الأمن السيبراني بحيث تعرف كيف تراقب الانترنت المظلم بحثا عن اي تهديدات تخص الشركة أو الدولة أو المؤسسة الرسمية.
- يعتمد عملك كمستشار أمني لدى الأفراد على دورة اختراق الجوال أيضا (والتي سترى تفاصيلها في الدورة رقم 4).

Syllabus - المحتوى

الدورة الثالثة: دورة الاختراق والاستخبارات مفتوحة المصدر

Section 1 Introduction - المقدمة

1.1 Introduction - مقدمة الدورة

0.0 NOTICE - ملاحظة مهمة

Section 2 OSINT

2.1 People Info Gathering part 1 - جمع المعلومات عن الأشخاص ج1

2.2 People Info Gathering part 2 - جمع المعلومات عن الأشخاص ج2

2.3 People Info Gathering part 3 - جمع المعلومات عن الأشخاص ج3

2.4 Phone Numbers OSINT - جمع المعلومات عن أرقام الهواتف

2.5 OS OSINT and Exploitation p1 - جمع المعلومات عن الأنظمة واختراقها ج1

2.6 OS OSINT & Exploitation p2 - جمع المعلومات عن الأنظمة واختراقها ج2

2.7 OS OSINT & Exploitation p3 - جمع المعلومات عن الأنظمة واختراقها ج3

Section 3 Recon and Dark Web Analysis - جمع المعلومات والانترنت المظلم

3.1 Networks Information Gathering - جمع المعلومات عن الشبكات

3.2 Dark Web Sources News and Leaks P1 - الانترنت المظلم منتديات وأخبار ومراقبة

3.3 Dark Web Sources News and Leaks P2 - الانترنت المظلم منتديات وأخبار ومراقبة ج2

3.4 Data Analysis P1 - تحليل البيانات

3.5 Exercise - Data Analysis P2 - اختبار

3.6 Google Hacking Databases - الاختراق باستخدام جوجل

Section 4 Tracking and Phishing - التتبع والتصيد

4.1 Social Media Tracking - تتبع حسابات وسائل التواصل الاجتماعي

4.2 Tracking using Leaks - التتبع باستخدام التسريبات

4.3 GSM Tracking - تتبع الاتصالات اللاسلكية

4.4 Phishing - Fake Pages - اختراق حسابات التواصل الاجتماعي بالصفحات المزورة

4.5 Cam Hacking - اختراق كاميرات المراقبة العامة

4.6 IDN Homograph Attack - اختراق حسابات التواصل الاجتماعي هجمة اي دي ان

4.7 Port Tunneling and browsers hacking - الاحتراق الخارجي

4.8 WhatsApp 2FA Phishing - اختراق الواتساب

Syllabus - المحتوى

الدورة الثالثة: دورة الاختراق والاستخبارات مفتوحة المصدر

Section 5 Forensics and Hidden Services - تتبع اتصالات وكيفية كشفها

5.1 VPN Forensics P1 - كشف اتصالات في بي ان

5.2 VPN Forensics P2 - كشف اتصالات في بي ان ج2

5.3 Honeypots - مصائد المخترقين

5.4 Private Chat Dark Web - التخفي على الانترنت المظلم

5.5 The Exam - الامتحان العملي

الدورة الرابعة: دورة اختراق الجوالات

هي دورة يتم إطلاقها للمرة الأولى في الوطن العربي، تتعلم في هذه الدورة كيف يتم اختراق أنظمة الهواتف وكيف يتم جمع المعلومات عنها بكثير من الطرق، منها ما يعمل على الأجهزة الغير محدثة، ومنها ما يعمل باستغلال مستخدم الجهاز، ومنها ما يتم عبر اختراق جيميل أو آي كلاود

- الهدف من الدورة هو جعلك مستشار أمني للأفراد بحيث يأتيك العميل لتقوم بفحص جواله وحساباته في وسائل التواصل الاجتماعي وإذا تبين أنه قد تعرض للاختراق فبإمكانك تتبع موقع المخترق له وتقديم معلوماته في تقرير رسمي، بالإضافة لتأمين حساباته وجواله وشبكة بيته له.
- **لا يوجد دورة أو شخص في العالم يمكن أن يجعلك تخترق أي جوال تريده، أنظمة الجوالات الحديثة متينة الحماية ومن يستطيع اختراق أي جوال يريده هذا يعني أنه يملك ثغرة في هذا النظام، للعلم شركة Apple تقدم مكافئة ما يصل إلى مليون دولار مقابل هكذا ثغرات**
  - هذا يعني أن من يدعي عليك هذا الكلام هو شخص محتال صريح، فكيف ستتعلم معي مجال اختراق الجوالات؟
  - نحن نقدم لك هذه الدورة لتمكنك من اختراق الجوال باستغلال الهدف (الاختراق عن طريق رابط، أو اختراق الجيميل أو الآي كلاود وبالتالي اتمام الاختراق) والكثير من الطرق طبعا بهدف اخلاقي وهو ما ذكر في البند الأول

Syllabus - المحتوى

الدورة الرابعة: دورة اختراق أنظمة الجوالات

Section 1 : Intro and Lab Setup - المقدمة وتنزيل المختبرات

1.1 Introduction - المقدمة

0.0 Notice - ملاحظة مهمة

1.2 Kali Installation - تنزيل كالي لينكس

Section 2: Kali Basics - أساسيات كالي لينكس (تستطيع تخطيها)

2.1 Kali File System - نظام ملفات كالي لينكس

2.2 Kali Managing Process - إدارة العمليات

2.3 Kali Managing Services - إدارة الخدمات

2.4 Kali Monitoring - مراقبة العمليات

Section 3: Payload and Hacking Process - الاختراق والبايلود

3.1 Intro-Android vs IOS - مقدمة في أنظمة الجوالات

3.2 Payload & Tunneling Services - البايلود والاختراق خارج الشبكة

3.3 APK Process - عمل البايلود المناسب لاندرويد

3.4 Listening for Connections - التنصت على اتصالات الاختراق

3.5 Signing Process - توثيق البايلود ليصبح معتمدا

3.6 Hacking phone and Auto Sign الاختراق العملي

Syllabus - المحتوى

الدورة الرابعة: دورة اختراق أنظمة الجوالات

Section 101 : Rooting, Jailbreaking, and More

101.1 Making PDF Payload & Public Exploitation

101.2 Facebook leaks - تسريبات معلومات فيسبوك

101.3 Introduction to Root & Jailbreak - مقدمة في الروت والجلبريك

101.4 What is Rooting & Jailbreaking - تعريف الروت والجلبريك

101.5 Rooting Android - عمل روت اندرويد

101.6 Jailbreaking IOS - عمل روت آي او اس

Section 4 : IOS Hacking - اختراق اي او اس (الآيفون)

4.1 Port Forwarding - الاختراق الخارجي

4.2 IOS Payload Making - عمل البايلود

4.3 IOS Hacking - الاختراق

4.4 IOS Payload Delivering - توصيل البايلود

4.5 IOS Digital Forensics - التحقيق في هاتف ايفون مخترق

Section 5: More Hacking Ways

5.1 Web Browser Hacking (Gmail, iCloud) - الاختراق باستغلال رابط

5.2 Web Browser Hacking 2

5.3 Web Hacking With Port Tunneling - الاختراق الخارجي برابط

5.4 The Exam - الامتحان

الدورة الخامسة: دورة التحقيق في جرائم الانترنت والانترنت المظلم

وهي دورة جديدة من نوعها تهدف إلى تدريبك على جميع المهارات التقنية التي تحتاجها كصحفي أو محقق في عملية جمع المعلومات عبر الانترنت والانترنت المظلم بالإضافة للتحقيق في جرائم الانترنت وحماية نفسك عبر الانترنت من الاختراق، ومن التنصت ومن كشف هويتك أو كشف تحقيقك الأمني أو الصحفي، هذه الدورة مصممة بشكل جديد وفيها جميع المهارات التي ستحتاجها، قم بجولة على جدول التدريب أو شاهد فيديو المقدمة المجاني لمعرفة تفاصيل أكثر

Syllabus - المحتوى

الدورة الخامسة: دورة التحقيق في جرائم الانترنت والانترنت المظلم

Section 1 : Introduction

1.1 Introduction - المقدمة
1.2 Legal Board - الحدود القانونية
1.3/4 Dark Web Vs. Surface Web - الإنترنت المظلم ضد الانترنت العادي
1.5 Osint & Dark Web Lap Setup - تحضير مختبر التحري والانترنت المظلم
1.6 Private Investigator Job Demonstration - شرح وظيفة المحقق الخاص

Section 2 : Dark Web

2.1 How to Access Dark web ? - كيف تدخل للإنترنت المظلم
2.2 Morals & Ethics & Roles - أخلاقيات العمل
2.3 Dark Web Markets & Forums - أسواق ومنتديات الانترنت المظلم
2.3 Dark Web Forums p2 - منتديات الانترنت المظلم
2.4 Dark Web Search Engines - محركات بحث الانترنت المظلم
2.5 Untraceable Dark Web Chatting - محادثات الانترنت المظلم الغير قابلة للتتبع
2.6/7 Dark Web Sharing Files & Hosting Website - مشاركة الملفات عبر الدارك ويب
2.8 OSINT Practical Lab - تطبيق عملي للتحري على الانترنت المظلم
2.9 Is Dark Web Untraceable ? (Student Side) - هل يمكن التتبع عبر الداركويب
2.10 Dark Web Monitoring Services - مراقبة وتتبع الانترنت المظلم
2.11 Telegram Cybercriminals & Groups - مجرمو ومجموعات التلغرام
2.12 Telegram Osint & Monitoring - تتبع وجمع المعلومات عبر التلغرام

Section 3 : Journalists Private Investigations & Protection - الصحفيين

3.1 Morals and Ethics and Legal Board - الأخلاقيات
3.2 News Tracking P1 - تتبع مصادر الأخبار ج1
3.2 News Tracking P2 - تتبع مصادر الأخبار ج2
3.3 Leaks Info Gathering - جمع المعلومات عن التسريبات
3.4 People OSINT P1 - جمع المعلومات عن الأشخاص ج1
3.4 People OSINT P2 - جمع المعلومات عن الأشخاص ج2
3.5 How to be hidden on the Internet? - التحفي عبر الانترنت

Syllabus - المحتوى

الدورة الخامسة: دورة التحقيق في جرائم الانترنت والانترنت المظلم

3.6 Social Engineering & AI Ideas - الهندسة الاجتماعية والذكاء الاصطناعي
3.7 Social Media Accounts Advanced Protection - الحماية المتقدمة لحساباتك
3.8 How to protect your self from sniffing? - كيف تحمي نفسك من التنصت
3.9 Individuals Incidents Response Protocol - بروتوكول التعامل مع حوادث الأمن السيبراني
3.10 Web Archive - ارشيف الانترنت
3.11 Encrypted Calls, Messages and Emails - المكالمات والايميلات والرسائل المشفرة
3.12 Movies & Stories (Qaisar Files , Snowden) - قصص حقيقية وأفلام

Section 4 : Public OSINT - الاستخبارات مفتوحة المصدر

4.1 Img EXIF Data P1 - استخراج البيانات من الصور ج1
4.2 Img EXIF Data P2 & Hide Data & Messages in Img P2 - استخراج البيانات من الصور ج2
4.3 Hide & Extract info from Audio tracks P1 - اخفاء واستخراج الرسائل السرية من ملفات الصوت ج1
4.3 Hide & Extract info from Audio tracks P2 - اخفاء واستخراج الرسائل السرية من ملفات الصوت ج2
4.4 Maltego (Student Side | Ture Story) - تطبيق واقعي لتتبع مجرم سرق 150 الف دولار
4.5 Usernames Passive OSINT - جمع المعلومات عن اليوزرنيمز
4.6 Permanent Data Deleting - الحذف النهائي للبيانات
4.7 Think Like A Hacker or Cybercriminal - التفكير كهاكر أو كمجرم

Section 5 : Bonus Section - قسم إضافي

5.1 Social Intelligence - الذكاء الاجتماعي
5.2 How to Study Cyber Security?
5.3 More Resources
5.4.1 Journalist Exam - امتحان الصحفيين
5.4.2 Private Investigator Exam - امتحان المحققين الجنائيين

الأسئلة الشائعة

- **الدورات متقدمة، فهل تناسب المبتدئين أيضًا؟**

نعم، نبدأ بتقديم أساسيات مهمة للطالب، تقسم بين أساسيات تؤخذ من خلال الدورة، وأساسيات من مصادر خارجية وذلك لتنمية أهم مهارة عند مختبر الاختراق وهي مهارة البحث.

- **بما أنني سأحصل على الدورات مدى الحياة، هل سيتم تحديثها باستمرار؟**

طبعا، نحن نقوم بتحديث الدورات بالتوافق مع المسار العالمي ومتطلبات السوق في مجالات الأمن السيبراني، بالإضافة لطلبات المتدربين.

- **كيف تساعدني شهاداتكم على العمل في المجال؟**

نقدم لك مع كل شهادة رقم توثيق واعتماد يجعل شهاداتك مصدقة ومعتمدة لدينا، بعد أول دورتين بإمكانك التوقف وإخبار المدرب سيف مخارزة، وقتها سيقوم بعمل الـ CV الخاص بك معك، ويساعدك في التقدم للوظائف التي تناسب خبراتك وبعدها يدربك على مقابلة العمل لتكون جاهزا، طبعا إذا كنت تريد أن تعمل كعمل حر وتكتسف الثغرات وتقدم خدمة اختبار الاختراق للشركات بنفسك سيساعدك المدرب بنفسه .

لأي أسئلة إضافية تواصل مع المدرب سيف مخارزة مباشرة عبر واتساب
00962781523545