SCHULUNGSBROSCHÜRE

ERNST & YOUNG

eXtreme Hacking – Defending Your Site

Frankfurt am Main / Eschborn
26. – 30. April 2004

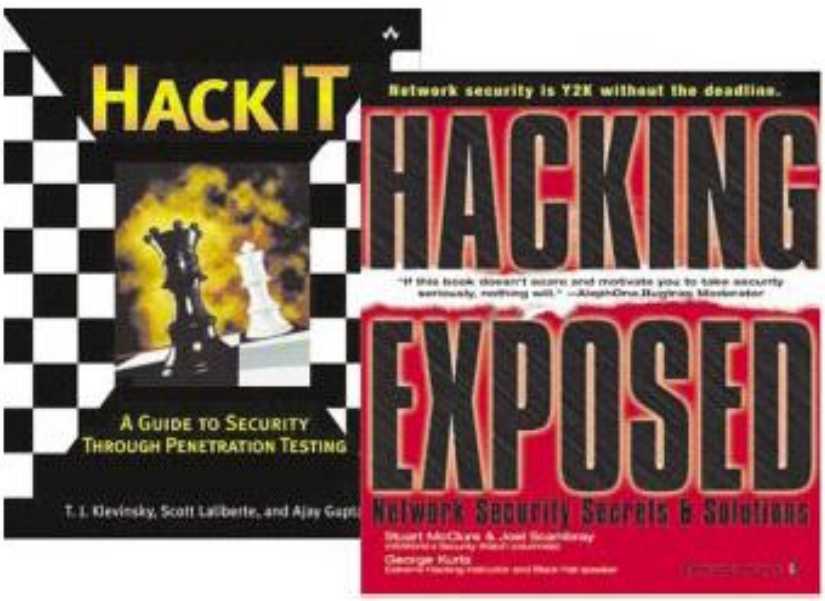
eXtreme hacking
Defending Your Site

Warum Ernst & Young?

Häufig ist nicht bewußt, welchen Gefahren Unternehmen durch Hacking-Attacken ausgesetzt sind. Die „Chicago Tribune" bezeugte einen beauftragten „Ethical Hack" eines Finanzinstitutes durch Ernst & Young. Nach lediglich 2 Stunden wurde das gesamte Netzwerk identifiziert und alle Kreditkartennummern kopiert. Nach 23 Stunden hatten wir alle Mitarbeiterpasswörter ermittelt. Der Mandant hatte hiervon nichts bemerkt!

Attack & Penetration: Methodologie und Vorgehensweise

Basis für aktuelle und effiziente Vorgehensweisen sind offen und intensiv kommunizierende Mitarbeiter – ohne Grenzen. Weltweit haben wir mehr als 2.000 ITSicherheitsberater, deren kontinuierlicher Austausch von Vorgehensweisen, aktuellen Schwachstellen, Tools, etc. dazu beiträgt, dass wir ein global einheitliches Dienstleistungsangebot auf dem neuesten Stand anbieten können – überall mit den gleichen Qualitätsmaßstäben.



Die offene Kommunikationskultur bei Ernst & Young führt dazu, dass wir unsere internen Vorgehensweisen auch unseren Mandanten als Training anbieten. Ernst & Young investiert intensiv in die Entwicklung eigener Methodenkompetenzen. Dadurch hat sich unsere Vorgehensweise als Standard etabliert. Zum Beispiel wurde das bekannte Buch „Hacking Exposed" sowie das kürzlich erschienene Buch „HackIT" von Ernst & Young Mitarbeitern geschrieben und wird kontinuierlich erweitert, so z.B. auch durch einen „Global Hacking Cup Contest".

Wir erweitern unsere Methodenkompetenz fortlaufend um aktuelle Themengebiete, wie z. B. zum Thema „Mobile Security": War-Driving, WEP / WLAN-Hacking, etc.

Ernst & Young hat in die besten Tool-Programme investiert und diese weltweit lizensiert. Neben diesen „state-of-the-art" Tools hat Ernst & Young zusätzlich eigene entwickelt.

eXtreme hacking
Defending Your Site

Agenda

Beginn der Schulung:
Montag, den 26. April um 10:00 Uhr.

Ende der Schulung:
Freitag, den 30. April um 16:00 Uhr.

Tagesablauf:
Die Schulung beginnt täglich um 9.00 Uhr und endet um 17.00 Uhr mit der Option, sich auch nach 17.00 Uhr noch mit den Übungen zu beschäftigen (open end). Am Tag der gemeinsamen Abendveranstaltung endet der Schulungstag pünktlich um 17.00 Uhr.

Tag 1: Discovery / Scanning
Target acquisition, Host discovery, TCP Fingerprinting, Port scanning, Banner retrieval, Intrusive Techniques, Custom Tools, Automated Scanners, War Dialing, Putting it all together – Hnds on Eercise

Tag 2: Profile Windows NT/2000/XP
Target Identification, Information Gathering, Enumerating NT Information, Brute Force Authentication (Tools, Methods, Pros and Cons), Passwords, Password Cracking, Password Sniffing, User Access, Privilege Escalation, Admin Access, „Twenty Things To Do After You've Hacked Admin“, Backdoors, Trojans, Hijacks, Further Exploits, Routing over non-routable protocols, Bypassing router filtering, Intrusion Exercise, Countermeasures

Tag 3: Profile Unix
Discovery/Scanning, Target Acquisition, Remote Information Gathering, Vulnerability Mapping, Remote Access, Local Privilege Escalation, Local Information Gathering, Further Exploits, Hacking the Next Hop, Intrusion Exercise, Countermeasures

Tag 4: Web Anwendungen/ Firewalls
Web Server Discovery/Scanning, Web Server Exploits, Web Application Exploits, Web Server/Application Countermeasures, Firewall Footprinting, Attacking the Firewall, Known Firewall Weaknesses, Firewall Countermeasures

Tag 5: Mainframes/ Datenbanken/ Advanced Techniques
Netware, Mainframe, Databases, Dial-in, Social Engineering, Port Redirection, Backdoors, Tunneling, Sniffing, Eavesdropping, Keystroke Capturing, Session Hijacking, GUI Hijacking, DNS & IP Spoofing, Multi-Host Multi-OS Hack That Will Challenge Even The Most Ardent Hackers, Knowledge Resources

Referenten

Wir setzen ausschließlich speziell geschulte und erfahrene Ernst & Young eXtreme Hacking Class Trainer ein. Alle unsere eXtreme Hacking Class Trainer haben umfangreiche mehrjährige Erfahrung in Attack & Penetration Projekten gesammelt und sind durch kontinuierliche Weiterbildung stets auf dem neuesten Stand der Technik und Methodik.

Marcus Rubenschuh

Marcus Rubenschuh ist Bereichsleiter Information Security der Ernst & Young AG. Er ist zertifizierter eXtreme Hacking Trainer und verfügt über mehrjährige Erfahrungen in den Bereichen Penetration Testing, Anti-Hacking Maßnahmen, Sicherheitskonzepte, etc.

Krisztian Piller

Krisztian Piller ist als Senior Advisor Information Security bei Ernst & Young tätig. Er ist ebenfalls zertifizierter eXtreme Hacking Trainer und hat umfangreiche internationale Erfahrung im Penetration Testing sowie in Anti-Hacking Maßnahmen.

eXtreme hacking
Defending Your Site

Teilnahmebedingungen

Folgende Voraussetzungen gelten für die Teilnahme an unserer eXtreme Hacking Schulung:

Sprache:
Die Schulung wird in deutscher Sprache gehalten. Unterlagen gibt es wahlweise in deutscher oder englischer Sprache.

Technisches Verständnis:
Fundiertes Verständnis von TCP/IP und ein gewohnter Umgang mit den Betriebssystemen Microsoft Windows NT/ 2000/ XP und Unix/Linux Varianten sind hilfreich. Für beide Betriebssysteme sollten die folgenden Tätigkeiten den Teilnehmern geläufig sein: Benutzerkonten erstellen, Services installieren und benutzen, Patches installieren, Modifikation von Systemdateien, Erstellen und Ausführen von Shell-Skripts, TCP/IP Ports für gängige Services identifizieren sowie ein Verständnis der verschiedenen Authentifizierungsmechanismen von Betriebssystemen.

Ethische Grundeinstellung:
Das im Rahmen dieser Veranstaltung vermittelte Wissen ist hochsensibel in der Hinsicht, dass es ohne ethisch verantwortungsvollen Umgang ein hohes Gefährdungspotenzial darstellt. Daher müssen vor der Schulungsteilnahme alle Teilnehmer schriftlich einem selbstverpflichtenden, ethischen Kodex zustimmen.

Non-compete Agreement:
Unsere Mandanten bekundeten vermehrt den Wunsch einer Schulung zu diesem Thema. Daher bieten wir diese Art von Schulungen ausschließlich im Interesse unserer Mandanten an. Alle Teilnehmer müssen sich in Form eines non-compete Agreements dazu verpflichten, das erworbene Wissen nicht zum Zwecke des Wettbewerbs gegen Ernst & Young zu benutzen.

eXtreme hacking
Defending Your Site

Ort

Die Schulung findet in den eigenen Schulungsräumen von Ernst & Young statt. Die Adresse lautet:

Ernst & Young AG
Konferenzraum 3
Düsseldorfer Straße 40
65760 Eschborn
Tel. (06196) 996 24781
Fax (06196) 996 23746

Gebühren

Die Teilnahmegebühr für die eXtreme Hacking Schulung beträgt h 4.990,- zzgl. 16 % MwSt. Bei zwei oder mehreren Teilnehmern der gleichen Firma gewähren wir einen Rabatt von 10 % pro Teilnehmer. Frühbucher erhalten bei Anmeldungen bis zu acht Wochen vor der Schulung zusätzlich 10 % Rabatt.

Zahlungsbedingungen: Eine garantierte Schulungsplatzzuteilung kann von unserer Seite erst nach Bestätigung der Anmeldung erfolgen.

Rücktrittsrecht: Anspruch auf eine komplette Rückerstattung der Schulungsgebühren besteht nur bei einer schriftlichen Stornierung mindestens 21 Tage vor Schulungsbeginn. Ein Austausch des Schulungsteilnehmers kann unter Vorbehalt unserer Zustimmung vor Schulungsbeginn (nur schriftlich) vorgenommen werden. Für Stornierungen nach 21 Tagen vor Schulungsbeginn können wir leider keine Gebühren zurückerstatten. Eine Anrechnung auf einen späteren Kurstermin ist jedoch zu 75 % möglich.

Ernst & Young behält sich das Recht vor, die Schulungstermine aus wichtigem Grund zu verschieben, zu streichen bzw. Teilnehmer abzulehnen. Eine Schulung findet nur bei mindestens 10 Teilnehmern statt. Sollte eine Terminverschiebung unvermeidbar sein, so werden die Kursteilnehmer spätestens 7 Tage vor Schulungsbeginn per E-Mail/Telefon von uns benachrichtigt.

Inklusivleistungen

Die Teilnahmegebühr beinhaltet folgende Leistungen:

- Teilnahme an der Schulung inkl. der Benutzung eines Schulungs-Computers pro Teilnehmer, alle notwendigen Programme, gemeinsame Nutzung einer 2Mbit Anbindung an das Internet sowie einem Zertifikat über die erfolgreiche Teilnahme.
- Schulungsordner und CD mit Hacking- Tools.
- Täglich Erfrischungen und Mittagessen.
- Eine gemeinsame Abendveranstaltung.
- Ein eXtreme Hacking Polo-Shirt.

eXtreme hacking
Defending Your Site

Anreise

Die Anreise erfolgt auf eigene Kosten des Teilnehmers.

Mit dem Auto: Am Nordwestkreuz nehmen Sie bitte die A66 Richtung Wiesbaden bis zum Dreieck Eschborn und nehmen dort die Ausfahrt Eschborn/Kronberg. Biegen Sie an der ersten Ampel-Kreuzung rechts in die Frankfurter Straße ab und fahren die erste Möglichkeit rechts in die Mannheimer Straße und dann links in die Düsseldorfer Straße. Besucherparkplätze stehen Ihnen dort zur Verfügung.

Mit dem Taxi: Transferzeit vom – Hauptbahnhof ca. 20 Min. - Flughafen ca. 25 Min. (abhängig von der Verkehrslage).

Mit der Bahn: Vom Frankfurter Hauptbahnhof mit der S-Bahn S3 Richtung Bad Soden oder der S4 Richtung Kronberg bis zur Haltestelle Eschborn-Süd. Ca. 10 Min. Fußweg bis zu den Büros.

Service Hotline

Haben Sie noch Fragen? Rufen Sie uns an! Wir helfen Ihnen gerne.

Anmeldung/Kundenservice:

Frau Miriam Hellhund
Ernst & Young AG WPG
Mergenthalerallee 10-12
D-65760 Eschborn / Frankfurt am Main
Tel. (06196) 996 24781
Fax (06196) 996 23746
E-Mail: miriam.hellhund@de.ey.com

Schulungsinhalt:

Herr Marcus Rubenschuh
Ernst & Young AG WPG
Mergenthalerallee 10-12
D-65760 Eschborn / Frankfurt am Main
Tel. (06196) 996 27664
Fax (06196) 996 23746
E-Mail: marcus.rubenschuh@de.ey.com

Unterkunft

Für Teilnehmer, die eine Unterkunft in Frankfurt benötigen, steht im Mercure-Hotel ein begrenztes Zimmerkontingent zu einem Preis von Euro 104,00 pro Nacht zur Verfügung.
Bitte buchen Sie direkt im Hotel unter Angabe des Buchungscodes „eXtreme Hacking“.
Die Hotelkosten werden von den Teilnehmern selbst getragen.

Mercure Hotel Eschborn
Frankfurter Str. 71-75, 65760 Eschborn
Tel. (06196) 7790-0
Fax (06196) 7790-500

Anmeldung

Anmeldung bitte per FAX an Frau Hellhund: 06196-99623746

Sie erhalten nach Anmeldung eine Bestätigung durch Ernst & Young. Die Anmeldungen werden nach der Reihenfolge der Eingänge berücksichtigt.

Hiermit melde ich mich für die Teilnahme an der Ernst & Young „eXtreme Hacking“ Schulung vom 26. April bis zum 30. April 2004 an. Die Teilnahmebedingungen sind mir bekannt und werden von mir akzeptiert. (Für die Anmeldung von mehreren Mitarbeitern einer Firma, bitte diese Seite für jeden Teilnehmer kopieren und ausfüllen.)

Titel

Nachname Vorname

Position

Firma

Strasse

PLZ Ort

Telefon Telefax

E-Mail

Staatsbürgerschaft

Ort / Datum Unterschrift

Hiermit bestätigen wir, dass der Teilnehmer bei uns beschäftigt ist, und wir die Schulungskosten des genannten Teilnehmers übernehmen.

Ort / Datum

Rechtsverbindliche Unterschrift

Stempel der Firma

Alle Teilnehmer müssen sich vor Beginn der Schulung ausweisen können! Bitte bringen Sie daher Ihren Personalausweis oder ein anderes identifizierendes Dokument mit.

Polo-Shirt Größe (bitte ankreuzen) ¨ M ¨ L ¨ XL ¨ XXL

Welchen Nutzen wird die Teilnahme an diesem Kurs Ihnen bzw. Ihrer Firma bringen?

Gibt es Themengebiete, für die Sie sich in dieser Schulung besonders interessieren?

Referenzen

„Die neutrale Betrachtung, Organisation, das Engagement der Teilnehmer und Trainer, sowie die Open End Sessions haben mir sehr gut gefallen. “

Christian Thor – Microsoft Deutschland GmbH

„ Sehr gut strukturiert. Klare Vorgehensweise. Angenehme Teilnehmerzahl. “

Stephan Gerhager – Audi AG

„Bootcamp for the Pros: Why Ernst & Young Will Lead Security Auditing Standards“ TechnologyEvaluation.com, January 19, 2002 (http://www.technologyevaluation.com/ViewArticle.asp?id=25.2002.01.19.1503)

„Execs become hackers to learn how to stop snoopers $5000 course teaches latest sneaky techniques“, USA Today, June 1, 2001 (http://www.usatoday.com/life/cyber/tech/2001-06-19-execs-become-hackers.htm)

„The black arts of ‘white hat’ hackers“ Financial Times Survey-Corporate Security, April 10, 2001

„Cracking the Code“ TIME Magazine, March 22, 1999 (http://www.time.com/time - search the archive for „Cracking the Code“)