ZERTIFIKAT

SySS THE PENTEST EXPERTS.

Angela Baruth

hat erfolgreich am Workshop

Hack3: Angriffe gegen Windows-basierte Netzwerke

vom 06. bis zum 08.12.2022 in Tübingen teilgenommen.

Windows-basierte Netze liegen oft im Fokus von Hackern. Um solche Angriffe besser nachvollziehen und sich besser dagegen wappnen zu können, gewährt dieser Workshop einen tieferen Einblick in die Vorgehensweise der Angreifer. Dabei werden Schwachstellen erläutert, Werkzeuge vorgestellt, mögliche Schutzmaßnahmen besprochen, theoretische Konzepte und kryptografische Verfahren beleuchtet sowie erlernte Angriffsvektoren anhand von praxisbezogenen Übungen erprobt.

Behandelte Themengebiete

- Windows-basierte Netzwerke
- Angriffe auf Einzelsysteme und Netzwerkprotokolle
- Rechteausweitung/Ausbreitung
- Einsatz geeigneter Tools
- „Best Practice"-Schutzmaßnahmen

Daniel Isern
(Senior IT Security Consultant)

ZERTIFIKAT

THE PENTEST EXPERTS.

Angela Baruth

hat erfolgreich am Workshop

Secu7: Phishing Awareness

am 28.07.2020 über Zoom teilgenommen.

Phishing-E-Mails sind sowohl im beruflichen als auch im privaten Umfeld tägliche Begleiter geworden. Anhand von Praxisbeispielen und einer Live-Demo wird in dieser Schulung gezeigt, wie sich unterschiedliche Varianten von Phishing-Mails und deren Anhänge auswirken können. Die Teilnehmer lernen, an welchen typischen Merkmalen Phishing-Mails zu erkennen sind und wie sie sich verhalten müssen, wenn sie eine solche Mail erhalten. Durchgeführt wird die Schulung durch das eigene Red Team der SySS.

Behandelte Themengebiete

- **Vorstellung der verschiedenen Phishing-Varianten**
- **Erkennungsmerkmale: Worauf ist zu achten?**
- **Live-Demo**
- **Beispiele aus der jüngsten Vergangenheit**
- **Richtiger Umgang mit einem Phishing-Vorfall**
- **Zusätzliche Sicherheitsmaßnahmen (SMiShing, Vishing)**

Referent:
Christoph Ritter
(Senior IT Security Consultant)

ZERTIFIKAT

THE PENTEST EXPERTS.

Angela Baruth

hat erfolgreich am Workshop

Hack5: Exploit Development

vom 14. bis zum 15. Juli 2020 in Tübingen teilgenommen.

Dieser Workshop befasst sich mit den theoretischen und praktischen Grundlagen der Funktionsweise und Entwicklung von Exploits. Hierbei werden diverse Aspekte von gängigen Schwachstellentypen betrachtet und diese ausgenutzt.

Behandelte Themengebiete:

- **Besonderheiten verschiedener Zielplattformen**
- **Verschiedene Formen der Schwachstellenanalyse**
- **Tools of Trade: Wichtige Werkzeuge für die Exploit-Entwicklung**
- **Ausnutzung verschiedener Schwachstellentypen**
- **Schutzmaßnahmen und Umgehungsmöglichkeiten**

Matthias Deeg
(Senior Expert IT-Security Consultant)

ZERTIFIKAT

SySS
THE PENTEST EXPERTS.

Angela Baruth
hat erfolgreich am Workshop

Secu3: IPv6-Security

Am 12.09.2019 in Tübingen teilgenommen.

Die Tage des Internetprotokolls in Version 4 (IPv4) sind bald gezählt. Daher setzen viele Bereiche schon heute das Internetprotokoll in der Version 6 (IPv6) ein. Aktuelle Betriebssysteme unterstützen dieses Protokoll meist schon von sich aus, ohne dass eine Interaktion des Benutzers notwendig wird. Dieser Umstand birgt die Gefahr, dass hier Sicherheitslücken entstehen können, von denen IT-Sicherheitsbeauftragte oft nichts wissen, da sie mit der Technologie nicht vertraut sind. Aus diesem Grund ist es ratsam, den IPv6-Datenverkehr in gleicher Weise zu sichern wie den mit IPv4.

Behandelte Themengebiete:

- **Kurze Einführung in IPv6**
- **Firewalls und IPv6**
- **Schwächen im internen Netzwerk**
- **Schwächen in Sicherheitsmechanismen**
- **(Remote) Host-Discovery**
- **Sicherheitsmaßnahmen**

Kien-Van Quang
(IT-Security Consultant)

THE PENTEST EXPERTS.

ZERTIFIKAT

Angela Baruth

hat erfolgreich am Workshop

Hack4: Angriffe gegen VoIP-Infrastrukturen

vom 10.02. bis zum 11.02.2016 in Tübingen teilgenommen.

Um die eigene Infrastruktur einheitlich und kostengünstig nutzen zu können, setzen viele Unternehmen das Protokoll VoIP ein. Dadurch erhöht sich der Schutzbedarf der übermittelten Daten, da ihre Trennung nicht mehr physikalisch, sondern logisch per VLAN erfolgt. Hieraus ergeben sich neue Ziele für Angreifer. Denn wenn es ihnen gelingt, im internen Unternehmensnetzwerk auf VLANs zuzugreifen, so sind sie mitunter in der Lage, vertrauliche Telefonate mitzuschneiden.

Technische Grundlagen

- Einführung in Techniken
- VoIP-Terminologie und -Aufbau
- Passive und aktive Traffic-Analyse
- VLAN-Terminologie und -Aufbau

VoIP-Angriffsverfahren

- Netzbasierte Angriffe gegen VoIP-Phones und -Anlagen

Angriffe gegen Authentisierungsmechanismen

- Boot-Angriffe und weitere physische Angriffsmöglichkeiten
- Angriffe gegen die Vertraulichkeit von Daten

VLAN-Angriffsverfahren

- Trunking-Angriffe
- Inter-VLAN-Routing
- Angriffe gegen Authentisierungsmechanismen

Sven Freund
(Senior IT-Security Consultant)

Ludwig Stage
(IT-Security Consultant)

THE PENTEST EXPERTS.

Zertifikat

Angela Baruth

hat erfolgreich am Workshop

„Hack8: WLAN-Hacking und WLAN-Security"

vom 08.12. bis zum 09.12.2015 in Tübingen teilgenommen.

Um eigene Drahtlosnetzwerke abzusichern, benötigt ein Systemadministrator fundierte Grundkenntnisse im Bereich der Funktionsweise und des „Hackings" moderner Drahtlosnetzwerke. Nur so wird er in der Lage sein, potenzielle Gefahren rechtzeitig zu identifizieren und grundlegende Probleme von vornherein auszuschließen.

Im Rahmen des Workshops wurden folgende Themen behandelt:

Grundlagen der WLAN-Technologie

- Standards, Begriffe

Aufbau einer WLAN-Umgebung

- Unter Linux (Adhoc, Infastruktur)

WLAN-*Sniffing*

- Ausspähen ungesicherter Drahtlosnetzwerke

Sicherheitsansätze des 802.11-Standards

- SSID-/MAC-basierte Filter, WEP
- Schwächen

Erweiterungen des 802.11-Standards

- WPA, WPA2, 802.11i, 802.11w

Authentifizierung und Schlüsselmanagement in 802.11i

- 802.1x, EAP, Schlüsselhierarchien, *Handshaking*

Funktionsweise der Verschlüsselungsmechanismen

- WEP, TKIP, CCMP

WLAN-Hacking

- DoS-Angriffe, WEP-Cracking, Angriffe gegen WPA/WPA2-PSK
- *MAC Address Spoofing* & *Man-in-the-Middle*-Angriffe
- Hacking von vorkonfigurierten *AccessPoints*, WPS Hacking

G. Klostermeier

Gerhard Klostermeier
(IT-Security Consultant)

SySS GmbH
Wohlboldstraße 8
72072 Tübingen
www.syss.de

THE PENTEST EXPERTS.

Zertifikat

Angela Baruth

hat erfolgreich am Workshop

„Secu4: IT-Recht und Datenschutz für IT-Verantwortliche"

am 16.11.2015 in Tübingen teilgenommen.

Administratoren und IT-Sicherheitsverantwortliche müssen täglich Entscheidungen treffen, ohne sich der rechtlichen Tragweite stets im Klaren zu sein. Um daher ein ausgereiftes Sicherheitskonzept im eigenen Verantwortungsbereich etablieren zu können, bedarf es der erfolgreichen Synchronisation von technischen und juristisch-organisatorischen Komponenten, der Kenntnis über die aktuelle Rechtslage im weiten Feld der IT-Compliance, Informationssicherheit und Datenschutz sowie der Fähigkeit, kritische Situationen richtig einschätzen zu können.

Im Rahmen des Workshops wurden folgende Themen behandelt:

Software-Lizenz-Audits; KRITIS

Big Data, SIEM, etc.

Wirtschaftsspionage und Geheimnisverrat – NSA-Affäre

Mobile Computing + BYOD; Cloud Computing

Einsatz sozialer Netzwerke, Social Media Richtlinien; Online-Werbung

Gestaltung und Dokumentation von IT-Compliance

Archivierungspflicht, neue GoBD, elektronisches Rechnungswesen

Hacking und Penetration

Vermeidung von Haftungsrisiken für IT-Verantwortliche und Datenschutzbeauftragte

Horst Speichert
(Rechtsanwalt)

SySS GmbH
Wohlboldstraße 8
72072 Tübingen
www.syss.de

THE PENTEST EXPERTS.

Zertifikat

Angela Baruth

hat erfolgreich am Workshop

„Secu5: Planung und Durchführung von Penetrationstests"

am 30.10.2015 in Tübingen teilgenommen.

Eine starke IT-Sicherheit ist das Fundament einer optimal funktionierenden IT-Landschaft eines Unternehmens. IT-Infrastrukturen und Applikationen sind meist hochwertig und robust konzipiert, sodass sie für Anwender und Administratoren sicher erscheinen. Dennoch können sie Lücken aufweisen. Oftmals sind es kleine, unscheinbare Fehler, die gefährliche Löcher in IT-Netze reißen. Der Penetrationstest ist ein geeignetes Kontrollinstrument, um Sicherheitsschwächen auf die Spur zu kommen und die IT-Sicherheit von Unternehmen nachhaltig zu stärken.

Im Rahmen dieses Workshops wurden folgende Themen behandelt:

Gründe für die Durchführung von Penetrationstests

Gegenstand der Prüfungen

- Perimeter, LAN, WLAN, Webapplikationen, etc.

Diverse Gestaltungsmöglichkeiten

Kosten-/Nutzenverhältnis

Vorgehensweise und Projektmanagement

Nachverfolgung von Schwachstellen

Politische Folgen innerhalb des Unternehmens

Ethische Aspekte

Sebastian Schreiber
(IT-Security Consultant)

SySS GmbH
Wohlboldstraße 8
72072 Tübingen
www.syss.de

Zertifikat

Frau Angela Baruth

hat erfolgreich am Workshop
„Hack6: Mobile Device Hacking“
vom 14.04. – 15.04.2015 in Tübingen teilgenommen.

Smartphones und iPhones sind aus unserer Welt nicht mehr wegzudenken. Immer mehr Menschen nutzen diese äußerst geschickten Geräte geschäftlich und privat, um auch von unterwegs Zugriff auf den eigenen Kalender, E-Mails und das Internet zu haben. Mit zunehmender Popularität steigt auch die Gefahr durch Angriffe auf Mobile Devices, sodass es für Administratoren und Entwickler eminent wichtig ist, Kenntnisse von möglichen Angriffsszenarien zu haben.

Im Rahmen des Workshops wurden folgende Themen behandelt:

- **Allgemeine Informationen**
  Eigenschaften und Verwaltung von Mobilgeräten
- **Angriffstechniken**
  Physischer Zugriff; Hardware Hacks; Mitschnitt des Datenverkehrs
  Man-in-the-Middle-Angriffe
- **Apple iOS**
  Sicherheitskonzept; Mobile Device Management-Lösungen
  Jailbreak; Forensik von A4-Geräten; Angriffe auf Apps zur Laufzeit und Reverse Engineering
- **Google Android**
  Sicherheitskonzept; Angriffe auf diverse Android-Versionen
  Emulation eines Smartphones; was Google über Android-User weiß
- **Windows Phone, Blackberry, etc.**
  Ausnutzung aktueller Schwachstellen; Sicherheitskonzept; Schutzmechanismen

Philipp Buchegger
(IT-Security Consultant)

SySS GmbH
Wohlboldstraße 8
D-72072 Tübingen
http://www.syss.de

Zertifikat

Frau Angela Baruth

hat erfolgreich am Workshop
„Praktische IT-Security: Hackertechniken beherrschen (Teil 2)“
vom 19.03. – 20.03.2014 in Tübingen teilgenommen.

Um das eigene Netzwerk abzusichern, benötigt ein Systemadministrator fundierte Grundkenntnisse im Bereich des „Hackings“. Die in Teil 1 erworbenen Fähigkeiten werden um weitere Themengebiete erweitert.

Im Rahmen des Workshops wurden folgende Themen behandelt:

- Verwendung von Rootkits
- Metasploit Framework
- Sicherheit in Windows-Netzen
- Security-Scanner
- Tunneling
- Grundlegende Schwächen in Webanwendungen

Jennifer Bornholt
(IT-Security Consultant)

SySS GmbH
Wohlboldstraße 8
D-72072 Tübingen
http://www.syss.de

Zertifikat

Frau Angela Baruth

hat erfolgreich am Workshop
„Praktische IT-Security: Hackertechniken beherrschen (Teil 1)“
vom 17.03. – 18.03.2014 in Tübingen teilgenommen.

Um das eigene Netzwerk abzusichern, benötigt ein Systemadministrator fundierte Grundkenntnisse im Bereich des „Hackings“. Nur so wird er in der Lage sein, potentielle Gefahren rechtzeitig zu identifizieren und grundlegende Probleme von vornherein auszuschließen.

Im Rahmen des Workshops wurden folgende Themen behandelt:

- Internet-Footprinting – Information Gathering
- Sniffing
- Man-in-the-Middle-Angriffe
- Port-Scanning – Identifizieren von Diensten
- Passwort-Cracking
- Exploit-Grundlagen
- Trojaner

Jennifer Bornholt
(IT-Security Consultant)

SySS GmbH
Wohlboldstraße 8
D-72072 Tübingen
http://www.syss.de

Zertifikat

Frau Angela Baruth

hat erfolgreich am Workshop
„Sicherheit bei Web-Applikationen“
vom 20.11. – 21.11.2013 in Tübingen teilgenommen.

Web-Applikationen sind für Hacker beliebte Ziele. Dort finden sie oftmals Schwachstellen, die ihnen ermöglichen, vertrauliche Daten zu entwenden und in das darunterliegende System vorzudringen. Dabei finden sie auch häufig den Weg in Unternehmensnetzwerke. Um solchen Angriffen begegnen zu können, benötigen Web-Developer und Mitarbeiter fundierte Grundkenntnisse über die beliebtesten Angriffsszenarien.
Im Rahmen des Workshops wurden folgende Themen behandelt:

- **Cross-Site Scripting**
  Angriffe auf Sitzungsinformationen, Phishing, Defacing
- **Cross-Site Request Forgery (XSRF)**
  Wie Angreifer Applikationsnutzer dazu bringen, das zu tun, was sie wollen
- **SQL-Injection**
  Unberechtigtes Auslesen von Daten aus einer Datenbank
- **OS Command Injection**
  Einschleusen von eigenen Betriebssystemkommandos in eine Web-Applikation
- **Local/Remote File Inclusion (LFI/RFI)**
  Ausführung des eigenen Programmcodes auf angegriffenem Server
- **Session-Hijacking**
  Übernahme von fremden Sitzungen
- **Cookies**
  Besonderheiten bei Generierung und Verwendung von Cookies

M. Mangold

Marcel Mangold
(IT-Security Consultant)

SySS GmbH
Wohlboldstraße 8
D-72072 Tübingen
http://www.syss.de