IT-Sicherheit und Kryptographie in der Praxis
–
Fehler aus dem Alltag

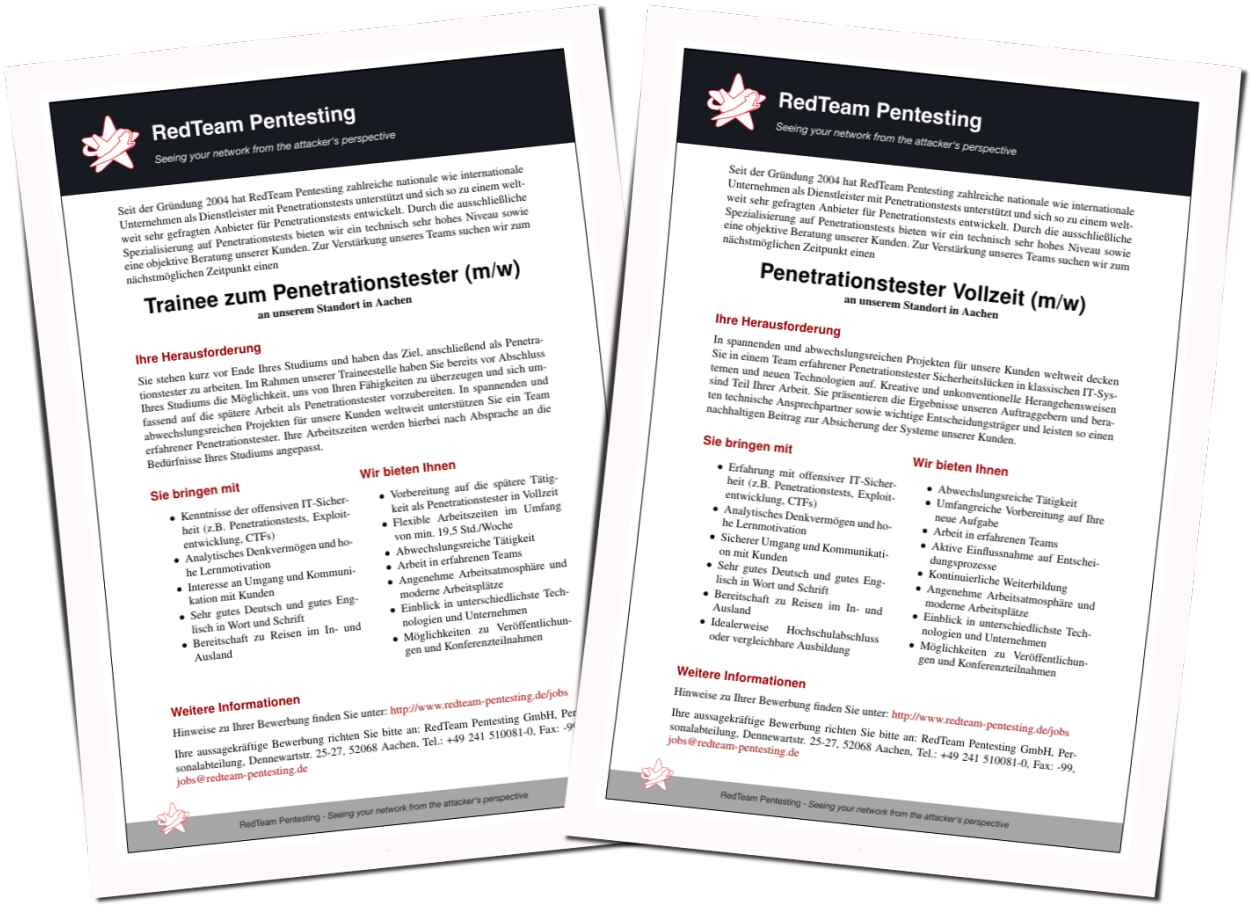
Patrick Hof - RedTeam Pentesting GmbH
patrick.hof@redteam-pentesting.de
http://www.redteam-pentesting.de

Cryptoparty Fachschaft Mathematik/Physik/Informatik
16. Januar 2014 - RWTH Aachen

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004
- ★ 8 Penetrationstester
- ★ Weltweite Durchführung von Penetrationstests
- ★ Spezialisierung ausschließlich auf Penetrationstests

Wir stellen ein!



RedTeam Pentesting

Seeing your network from the attacker's perspective

Seit der Gründung 2004 hat RedTeam Pentesting zahlreiche nationale wie internationale Unternehmen als Dienstleister mit Penetrationstests unterstützt und sich so zu einem weltweit sehr gefragten Anbieter für Penetrationstests entwickelt. Durch die ausschließliche Spezialisierung auf Penetrationstests bieten wir ein technisch sehr hohes Niveau sowie eine objektive Beratung unserer Kunden. Zur Verstärkung unseres Teams suchen wir zum nächstmöglichen Zeitpunkt einen

Trainee zum Penetrationstester (m/w)

an unserem Standort in Aachen

Ihre Herausforderung

Sie stehen kurz vor Ende Ihres Studiums und haben das Ziel, anschließend als Penetrationstester zu arbeiten. Im Rahmen unserer Traineestelle haben Sie bereits vor Abschluss Ihres Studiums die Möglichkeit, uns von Ihren Fähigkeiten zu überzeugen und sich umfassend auf die spätere Arbeit als Penetrationstester vorzubereiten. In spannenden und abwechslungsreichen Projekten für unsere Kunden weltweit unterstützen Sie ein Team erfahrener Penetrationstester. Ihre Arbeitszeiten werden hierbei nach Absprache an die Bedürfnisse Ihres Studiums angepasst.

Sie bringen mit

- Kenntnisse der offensiven IT-Sicherheit (z.B. Penetrationstests, Exploitentwicklung, CTFs)
- Analytisches Denkvermögen und hohe Lernmotivation
- Interesse an Umgang und Kommunikation mit Kunden
- Sehr gutes Deutsch und gutes Englisch in Wort und Schrift
- Bereitschaft zu Reisen im In- und Ausland

Wir bieten Ihnen

- Vorbereitung auf die spätere Tätigkeit als Penetrationstester in Vollzeit
- Flexible Arbeitszeiten im Umfang von min. 19,5 Std./Woche
- Abwechslungsreiche Tätigkeit
- Arbeit in erfahrenen Teams
- Angenehme Arbeitsatmosphäre und moderne Arbeitsplätze
- Einblick in unterschiedlichste Technologien und Unternehmen
- Möglichkeiten zu Veröffentlichungen und Konferenzteilnahmen

Weitere Informationen

Hinweise zu Ihrer Bewerbung finden Sie unter: http://www.redteam-pentesting.de/jobs

Ihre aussagekräftige Bewerbung richten Sie bitte an: RedTeam Pentesting GmbH, Personalabteilung, Dennewartstr. 25-27, 52068 Aachen, Tel.: +49 241 510081-0, Fax: -99, jobs@redteam-pentesting.de

RedTeam Pentesting - Seeing your network from the attacker's perspective

RedTeam Pentesting

Seeing your network from the attacker's perspective

Seit der Gründung 2004 hat RedTeam Pentesting zahlreiche nationale wie internationale Unternehmen als Dienstleister mit Penetrationstests unterstützt und sich so zu einem weltweit sehr gefragten Anbieter für Penetrationstests entwickelt. Durch die ausschließliche Spezialisierung auf Penetrationstests bieten wir ein technisch sehr hohes Niveau sowie eine objektive Beratung unserer Kunden. Zur Verstärkung unseres Teams suchen wir zum nächstmöglichen Zeitpunkt einen

Penetrationstester Vollzeit (m/w)

an unserem Standort in Aachen

Ihre Herausforderung

In spannenden und abwechslungsreichen Projekten für unsere Kunden weltweit decken Sie in einem Team erfahrener Penetrationstester Sicherheitslücken in klassischen IT-Systemen und neuen Technologien auf. Kreative und unkonventionelle Herangehensweisen sind Teil Ihrer Arbeit. Sie präsentieren die Ergebnisse unseren Auftraggebern und beraten technische Ansprechpartner sowie wichtige Entscheidungsträger und leisten so einen nachhaltigen Beitrag zur Absicherung der Systeme unserer Kunden.

Sie bringen mit

- Erfahrung mit offensiver IT-Sicherheit (z.B. Penetrationstests, Exploitentwicklung, CTFs)
- Analytisches Denkvermögen und hohe Lernmotivation
- Sicherer Umgang und Kommunikation mit Kunden
- Sehr gutes Deutsch und gutes Englisch in Wort und Schrift
- Bereitschaft zu Reisen im In- und Ausland
- Idealerweise Hochschulabschluss oder vergleichbare Ausbildung

Wir bieten Ihnen

- Abwechslungsreiche Tätigkeit
- Umfangreiche Vorbereitung auf Ihre neue Aufgabe
- Arbeit in erfahrenen Teams
- Aktive Einflussnahme auf Entscheidungsprozesse
- Kontinuierliche Weiterbildung
- Angenehme Arbeitsatmosphäre und moderne Arbeitsplätze
- Einblick in unterschiedlichste Technologien und Unternehmen
- Möglichkeiten zu Veröffentlichungen und Konferenzteilnahmen

Weitere Informationen

Hinweise zu Ihrer Bewerbung finden Sie unter: http://www.redteam-pentesting.de/jobs

Ihre aussagekräftige Bewerbung richten Sie bitte an: RedTeam Pentesting GmbH, Personalabteilung, Dennewartstr. 25-27, 52068 Aachen, Tel.: +49 241 510081-0, Fax: -99, jobs@redteam-pentesting.de

RedTeam Pentesting - Seeing your network from the attacker's perspective

⇒ `https://www.redteam-pentesting.de/jobs`

Verschlüsselung? Ja also, prinzipiell...

Viele Kommunikationskanäle sind immer noch unverschlüsselt

Netzwerk: HTTP, FTP, POP3/IMAP, SMTP, VoIP

Wireless: DECT, RFID, Wireless-Tastaturen

E-Mail: PGP/GPG, S/MIME? Benutzt niemand (richtig)

Best-Practice-Ansätze (im Aufbau): `https://bettercrypto.org`

Zufall oder Kreativ? Session-IDs

Zufällige IDs in einem Web-Portal.

1. `TvWjLeJjGhPvAhJjNgBuPiFkRqJmHOL`

Zufall oder Kreativ? Session-IDs

Zufällige IDs in einem Web-Portal. Oder?

1. `TvWjLeJjGhPvAhJjNgBuPiFkRqJmHOL`
2. `TvWjLeJjGhPvAhJjNgBuPiFkRrJmHOL`
3. `TvWjLeJjGhPvAhJjNgBuPiFkRsJmHOL`

Zufall oder Kreativ? Session-IDs

Zufällige IDs in einem Web-Portal. Oder?

1. TvWjLeJjGhPvAhJjNgBuPiFkRqJmHOL
2. TvWjLeJjGhPvAhJjNgBuPiFkRrJmHOL
3. TvWjLeJjGhPvAhJjNgBuPiFkRsJmHOL

Jedes zweite Zeichen ist großgeschrieben

Zufall oder Kreativ? Session-IDs

Zufällige IDs in einem Web-Portal. Oder?

1. `TvWjLeJjGhPvAhJjNgBuPiFkRqJmHOL`
2. `TvWjLeJjGhPvAhJjNgBuPiFkRrJmHOL`
3. `TvWjLeJjGhPvAhJjNgBuPiFkRsJmHOL`

Nur ein Zeichen ändert sich bei drei Session-IDs

Zufall oder Kreativ? Session IDs

Anfragen von verschiedenen IP-Adressen

Von 192.168.1.23:

`TvWjLeJjGhPvAhJjNgBuPiFkRsJmHOL`

Von 10.100.1.42:

`TvWjLdBhGbHvAhJlMgBuPiFkRtJmHOL`

Zufall oder Kreativ? Session IDs

"Geheimer" Schlüssel: dahfbhvagjhk

```
192.168.1.23 = 192168001023

dahfbhvagjhk
192168001023
------------
ejjghpvahjjn = eJjGhPvAhJjN
```

TvWjLeJjGhPvAhJjNgBuPiFkRsJmHOL

Zufall oder Kreativ? Session IDs

"Geheimer" Schlüssel: dahfbhvagjhk

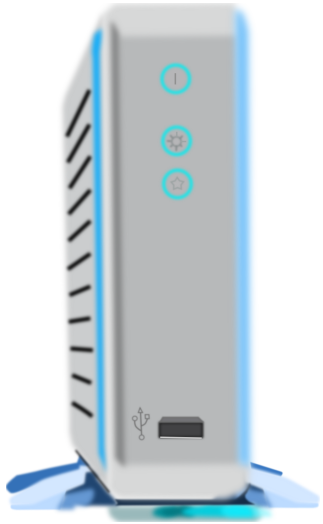
```
192.168.1.23 = 192168001023

dahfbhvagjhk
192168001023
------------
ejjghpvahjjn = eJjGhPvAhJjN
```

TvWjLeJjGhPvAhJjNgBuPiFkRsJmHOL

⇒ Krypto nicht selbst erfinden!

Hardware Hacking

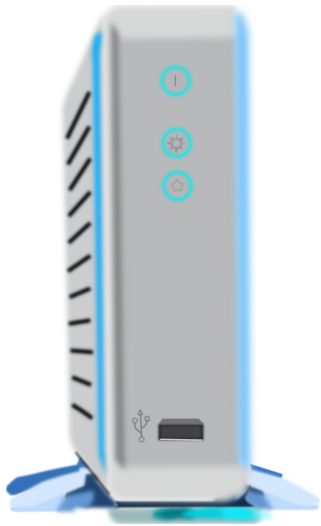
- ★ Storage-Gerät mit Festplatte
- ★ Krypto-Modul im Gerät macht "Hardware"-Verschlüsselung
- ★ Das Krypto-Modul wird beim Booten des Systems, welches das Storage-Gerät benutzt, freigeschaltet
- ★ Wie kommt man an die Daten?



Hardware Hacking

Lösung:

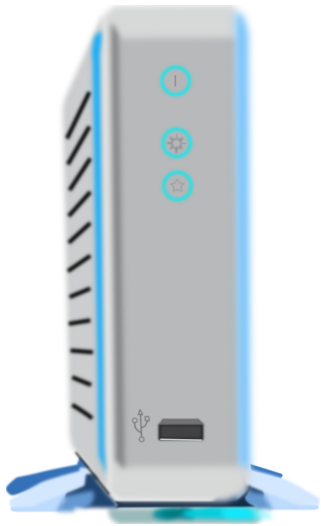
- ★ Das Krypto-Modul ist direkt mit der Festplatte verbunden
- ★ Man startet das System und lässt es das Krypto-Modul freischalten
- ★ Ohne die Stromversorgung zu unterbrechen, verbindet man die Festplatte mit dem Kryptomodul mit einem anderen Rechner



Hardware Hacking

Lösung:

- ★ Das Krypto-Modul ist direkt mit der Festplatte verbunden
- ★ Man startet das System und lässt es das Krypto-Modul freischalten
- ★ Ohne die Stromversorgung zu unterbrechen, verbindet man die Festplatte mit dem Kryptomodul mit einem anderen Rechner



⇒ Auch Hardware-Design ist wichtig!

Layered Security . . . by Obscurity

- ★ Windows-basiertes Netzwerkgerät mit proprietärer Applikation
- ★ Verschlüsselte Festplatten, verschlüsselte Netzwerkkommunikation. AES256.
- ★ Gerät bootet und funktioniert ohne Benutzerinteraktion

Layered Security . . . by Obscurity

- ★ Windows-basiertes Netzwerkgerät mit proprietärer Applikation
- ★ Verschlüsselte Festplatten, verschlüsselte Netzwerkkommunikation. AES256.
- ★ Gerät bootet und funktioniert ohne Benutzerinteraktion

Frage: Wo sind die Krypto-Schlüssel?

Layered Security . . . by Obscurity

Der Boot-Vorgang:

- ★ Windows fährt hoch, startet `run1.exe`

Layered Security . . . by Obscurity

Der Boot-Vorgang:

- ★ Windows fährt hoch, startet `run1.exe`
- ★ Kopiert diverse verschleierte Dateien in das Verzeichnis `\cache`

Layered Security . . . by Obscurity

Der Boot-Vorgang:

- ★ Windows fährt hoch, startet `run1.exe`
- ★ Kopiert diverse verschleierte Dateien in das Verzeichnis `\cache`
- ★ Und führt das Programm `reg.dat` mehrfach aus

Layered Security . . . by Obscurity

Der Boot-Vorgang:

- ★ Windows fährt hoch, startet `run1.exe`
- ★ Kopiert diverse verschleierte Dateien in das Verzeichnis `\cache`
- ★ Und führt das Programm `reg.dat` mehrfach aus
- ★ Welches in Wirklichkeit TrueCrypt ist

Layered Security . . . by Obscurity

Der Boot-Vorgang:

- ★ Windows fährt hoch, startet `run1.exe`
- ★ Kopiert diverse verschleierte Dateien in das Verzeichnis `\cache`
- ★ Und führt das Programm `reg.dat` mehrfach aus
- ★ Welches in Wirklichkeit TrueCrypt ist
- ★ Welches andere verschleierte Dateien entschlüsselt (`8zui72rec.dat`, `8zui72tas.dat`, . . .) mit 50 Zeichen langen Passwörtern, übergeben über die Kommandozeile

Layered Security . . . by Obscurity

Der Boot-Vorgang:

- ★ Windows fährt hoch, startet `run1.exe`
- ★ Kopiert diverse verschleierte Dateien in das Verzeichnis `\cache`
- ★ Und führt das Programm `reg.dat` mehrfach aus
- ★ Welches in Wirklichkeit TrueCrypt ist
- ★ Welches andere verschleierte Dateien entschlüsselt (`8zui72rec.dat`, `8zui72tas.dat`, . . .) mit 50 Zeichen langen Passwörtern, übergeben über die Kommandozeile
- ★ Welche die Anwendung in verschleierten Verzeichnissen enthalten (`\.private\OS\Win32\bin\.plugins\lib\...`)

Layered Security . . . by Obscurity

Der Boot-Vorgang:

- ★ Windows fährt hoch, startet `run1.exe`
- ★ Kopiert diverse verschleierte Dateien in das Verzeichnis `\cache`
- ★ Und führt das Programm `reg.dat` mehrfach aus
- ★ Welches in Wirklichkeit TrueCrypt ist
- ★ Welches andere verschleierte Dateien entschlüsselt (`8zui72rec.dat`, `8zui72tas.dat`, . . .) mit 50 Zeichen langen Passwörtern, übergeben über die Kommandozeile
- ★ Welche die Anwendung in verschleierten Verzeichnissen enthalten (`\.private\OS\Win32\bin\.plugins\lib\. . .`)
- ★ Welche die Krypto-Schlüssel für die Netzwerkkommunikation in einer verschleierten Datei enthalten

Layered Security . . . by Obscurity

Ergebnis:

- ★ Krypto-Schlüssel können ausgelesen werden
- ★ Einzige Arbeit ist das Nachvollziehen des Boot-Prozesses
- ★ Applikation ist insgesamt fehleranfälliger

Layered Security . . . by Obscurity

Ergebnis:

- ★ Krypto-Schlüssel können ausgelesen werden
- ★ Einzige Arbeit ist das Nachvollziehen des Boot-Prozesses
- ★ Applikation ist insgesamt fehleranfälliger

⇒ Verschleiern bedeutet nur unnötige Komplexität und keinen echten Sicherheitsgewinn

Zeit für Ihre Fragen!

Vielen Dank für Ihre Aufmerksamkeit.