RedTeam Pentesting

Physical Security
–
Wenn Türen zu Firewalls werden

Jens Liebchen (jens.liebchen@redteam-pentesting.de)
RedTeam Pentesting GmbH
https://www.redteam-pentesting.de

Lehrstuhl für IT-Sicherheitsinfrastrukturen
Universität Erlangen-Nürnberg
7. Februar 2023, Erlangen

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Firmensitz in Aachen, weltweite Durchführung von Pentetrationstests
- ★ Forschung im IT-Sicherheitsbereich

RedTeam Pentesting

Wir stellen ein!

INTERESSIERT? WERDE EINE*R VON UNS!

https://jobs.redteam-pentesting.de

RedTeam Pentesting GmbH
Alter Posthof 1
52062 Aachen
Deutschland

Warum Physical Security?

- Phyical Security muss Teil der IT-Sicherheits-Stategie sein
- Risiken kann nur begegnet werden, wenn diese auch bekannt sind
- $\Rightarrow$ **Awareness**

Warum Physical Security?

- Phyical Security muss Teil der IT-Sicherheits-Stategie sein
- Risiken kann nur begegnet werden, wenn diese auch bekannt sind
- $\Rightarrow$ **Awareness**
- Sie sparen mindestens 100 Euro für den Schlüsseldienst, wenn Sie Ihren Schlüssel beim nächsten Mal drinnen liegen lassen :-)

Penetrationstests und Physical Security

Penetrationstests

Penetrationstests sind individuelle realitätsnahe Angriffe auf Netzwerke und Produkte im Auftrag des Eigentümers.

- ★ Security-Audits/Checklisten sind im Allgemeinen keine Penetrationstests
- ★ „Testen sie mal unsere Firewall...“ meistens auch nicht
- ★ Stattdessen: Was macht ein Angreifer in der Praxis?

Penetrationstests und Physical Security

Penetrationstests

Penetrationstests sind individuelle realitätsnahe Angriffe auf Netzwerke und Produkte im Auftrag des Eigentümers.

- ★ Security-Audits/Checklisten sind im Allgemeinen keine Penetrationstests
- ★ „Testen sie mal unsere Firewall...“ meistens auch nicht
- ★ Stattdessen: Was macht ein Angreifer in der Praxis?

Penetrationstests testen hauptsächlich Angriffe direkt auf die IT, in letzter Zeit wird aber immer mehr auch die physische Sicherheit in die Tests integriert.

Beschaffung von Werkzeugen/Rechtliches

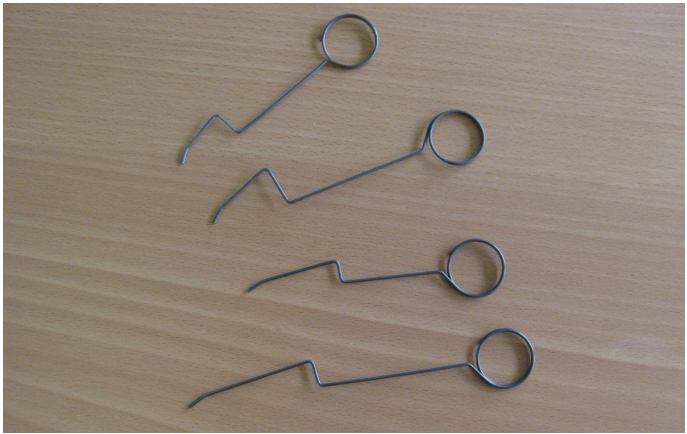
- Baumarkt!
- Großhandel/Fachhändler für Schlüsseldienste
- Normale Werkzeuge sind im Allgemeinen bezahlbar
- Werkzeuge sind frei verkäuflich
- Transport z.B. im Flugzeug ist unproblematisch
- Vorsicht beim Üben an wichtigen Türen $\Rightarrow$ Spuren und Problematik der Unterscheidung von echten Einbrüchen

RedTeam Pentesting

Klassisches Lockpicking

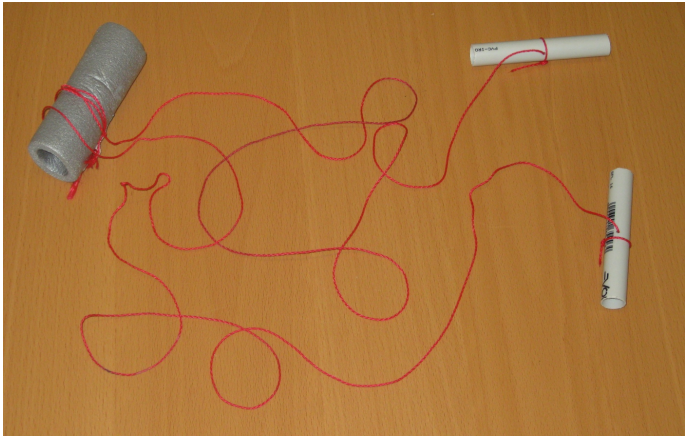
Werkzeuge: Keilformgleiter

Werkzeuge: Türfallennadeln



Werkzeuge: Türklinkenangel

Werkzeuge: Kippfenster/-Türöffnung



Was möchte ein Angreifer?

- ★ Diebstahl von Hardware (nicht IT-spezifisch)

Was möchte ein Angreifer?

- ★ Diebstahl von Hardware (nicht IT-spezifisch)
- ★ Zugriff auf Daten (evtl. auch durch Diebstahl)

Was möchte ein Angreifer?

- ★ Diebstahl von Hardware (nicht IT-spezifisch)
- ★ Zugriff auf Daten (evtl. auch durch Diebstahl)
- ★ Datenmanipulation / Sabotage

Was möchte ein Angreifer?

- Diebstahl von Hardware (nicht IT-spezifisch)
- Zugriff auf Daten (evtl. auch durch Diebstahl)
- Datenmanipulation / Sabotage
- Zugriff auf Netzwerk

Was möchte ein Angreifer?

- ★ Diebstahl von Hardware (nicht IT-spezifisch)
- ★ Zugriff auf Daten (evtl. auch durch Diebstahl)
- ★ Datenmanipulation / Sabotage
- ★ Zugriff auf Netzwerk
- ★ Manifestierung im Netzwerk

Der klassische Irrtum: Abgeschlossene Türen

„Meine Türen sind doch abgeschlossen!“

- ★ Grundsatz in Pentests: Alles hinterfragen
- ★ Viele „abgeschlossene“ Türen sind nicht abgeschlossen

Der klassische Irrtum: Abgeschlossene Türen

„Meine Türen sind doch abgeschlossen!“

- Grundsatz in Pentests: Alles hinterfragen
- Viele „abgeschlossene“ Türen sind nicht abgeschlossen
- „Aber *meine* Türen sind doch abgeschlossen...“
  $\Rightarrow$ **Wetten, dass nicht?**

Eingangs- und Zwischentüren

- Eingangstüren mit Summer

Eingangs- und Zwischentüren

- Eingangstüren mit Summer
- Zwischentüren mit Chipkarten/Fingerprint/Code sind meistens nicht abgeschlossen

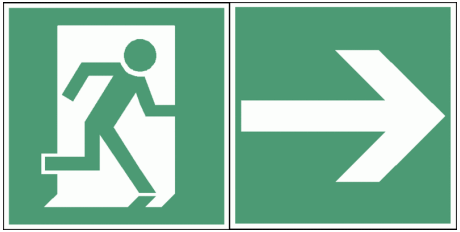
Eingangs- und Zwischentüren

- Eingangstüren mit Summer
- Zwischentüren mit Chipkarten/Fingerprint/Code sind meistens nicht abgeschlossen

Aus einem Penetrationstest

Glaszwischentüre, Chipkarten gesichert, von innen live videoüberwacht. Angriff mit Türfallennadeln: Kurzes Vortäuschen einer Chipkarte, dann Türöffnung in 1-2 Sekunden per Nadel. Auf dem Video ist der Angriff kaum zu erkennen.

Fluchtwege und Türen



Fluchttüren

Fluchttüren müssen, um Panikfallen zu vermeiden, einfach (mit einer Hand) in Fluchtrichtung zu öffnen sein.

Fluchtwege und Türen

- Fluchttüren können durchaus abgeschlossen sein
- Die einfache Betätigung der Türklinke oder z.B. einer Querstange zieht in diesem Fall auch den Riegel zurück.

Fluchtwege und Türen

- Fluchttüren können durchaus abgeschlossen sein
- Die einfache Betätigung der Türklinke oder z.B. einer Querstange zieht in diesem Fall auch den Riegel zurück.
- Öffnung von außen: Meistens mit Hilfe der Türklinkenangel
- Bei wenig Platz unterhalb der Türe: Türe z.B. mit pneumatischem Hebekisten leicht anheben.
- Angreifer können Fluchtwegen „rückwärts“ folgen...

Serverräume

- ★ Interessantes Ziel für Angreifer
- ★ In der Praxis: Lokalisierung für Angreifer meistens einfach

Serverräume

- ★ Interessantes Ziel für Angreifer
- ★ In der Praxis: Lokalisierung für Angreifer meistens einfach
- ★ Oft mit Gaslöschanlagen ausgestattet
- ★ Gaslöschanlagen $\Rightarrow$ Fluchttüren müssen vorhanden sein, da Personen bei Auslösung der Löschanlage den Raum verlassen müssen

Gekippte Fenster == Offene Fenster

Wenn die Fenster nicht alarmgesichert sind, existieren in großen Gebäuden immer Fenster, die nachts offen bleiben. Wie kommt der Angreifer an Fenster in oberen Etagen?

- ★ Leiter (trivial, wird aber häufig übersehen)
- ★ Abseilen von oben

Gekippte Fenster == Offene Fenster

Wenn die Fenster nicht alarmgesichert sind, existieren in großen Gebäuden immer Fenster, die nachts offen bleiben. Wie kommt der Angreifer an Fenster in oberen Etagen?

- ★ Leiter (trivial, wird aber häufig übersehen)
- ★ Abseilen von oben

Zitat aus einem Penetrationstest:

„Haben sie bedacht, dass ein Angreifer sich hier evtl. abseilt?“ — „Das hatten wir schon...“ (und zwar nicht im Rahmen eines Penetrationstests)

Mobile IT-Hardware

Der Angreifer ist nicht auf Ihr Gebäude beschränkt. Ihre Nutzer tragen die Daten aus dem Unternehmen.

Mobile IT-Hardware

Der Angreifer ist nicht auf Ihr Gebäude beschränkt. Ihre Nutzer tragen die Daten aus dem Unternehmen.

Hoteltüren

- Die meisten Hoteltüren sind nicht sicher abschließbar
- Zutritt mit den vorgestellten Werkzeugen ist fast immer möglich

Hoteltüren

- Die meisten Hoteltüren sind nicht sicher abschließbar
- Zutritt mit den vorgestellten Werkzeugen ist fast immer möglich
- Über Hotelsafes könnte man eigene Vorträge halten

Hoteltüren

- Die meisten Hoteltüren sind nicht sicher abschließbar
- Zutritt mit den vorgestellten Werkzeugen ist fast immer möglich
- Über Hotelsafes könnte man eigene Vorträge halten
- $\Rightarrow$ Hotels sind kein guter Ort, um wichtige Daten zu lagern!

Hoteltüren

Manchmal funktioniert es sogar noch einfacher:

Hoteltüren

Manchmal funktioniert es sogar noch einfacher:

Allgemein

- Rein kommt ein Angreifer fast immer, ohne etwas zu beschädigen
- Das Entdeckungsrisiko ist zumindest in großen Gebäuden gering
- Personen in Gebäuden werden nur sehr selten hinterfragt

Allgemein

- Rein kommt ein Angreifer fast immer, ohne etwas zu beschädigen
- Das Entdeckungsrisiko ist zumindest in großen Gebäuden gering
- Personen in Gebäuden werden nur sehr selten hinterfragt
- Passwörter „hacken“ geht auch per Teleobjektiv (Passwörter werden immer noch aufgeschrieben)

Allgemein

- Rein kommt ein Angreifer fast immer, ohne etwas zu beschädigen
- Das Entdeckungsrisiko ist zumindest in großen Gebäuden gering
- Personen in Gebäuden werden nur sehr selten hinterfragt
- Passwörter „hacken“ geht auch per Teleobjektiv (Passwörter werden immer noch aufgeschrieben)
- Die gefühlte Aufregung ist selbst während eines Penetrationstests relativ hoch

Beispiel: Netzwerkzugriff

- In fast allen Räumen finden sich gepatchte Netzwerkdosen
- Oft reicht das Überwinden einer einzigen Türe, um Zugriff auf das interne Netzwerk zu erhalten
- Bodentanks öffnen: Es finden sich häufig Netzwerkdosen, die den Verantwortlichen nicht bewusst sind

Beispiel: Netzwerkzugriff

- In fast allen Räumen finden sich gepatchte Netzwerkdosen
- Oft reicht das Überwinden einer einzigen Türe, um Zugriff auf das interne Netzwerk zu erhalten
- Bodentanks öffnen: Es finden sich häufig Netzwerkdosen, die den Verantwortlichen nicht bewusst sind
- VoIP-Netzwerke
  - Zugriff in einem relativ unwichtigen Raum kann zu einer Kompromittierung aller Telefongespräche führen
  - Telefone können Überwachungbilder anzeigen, weitere Türen öffnen etc.

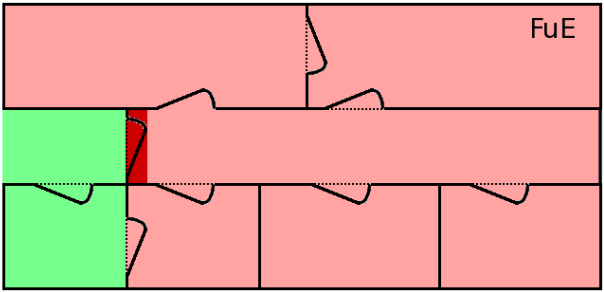
Beispiel: Serverraum

- Um bis in den Serverraum vorzudringen sind häufig verschiedene Sicherheitsbereiche zu überwinden
- Das Entdeckungsrisiko in Serverräumen ist oft geringer als in Büros
- Bei einer Entdeckung ist der Angriff dafür aber meistens komplett aufgeflogen, da eine Tarnung hier nicht möglich ist

Beispiel: Serverraum

- Um bis in den Serverraum vorzudringen sind häufig verschiedene Sicherheitsbereiche zu überwinden
- Das Entdeckungsrisiko in Serverräumen ist oft geringer als in Büros
- Bei einer Entdeckung ist der Angriff dafür aber meistens komplett aufgeflogen, da eine Tarnung hier nicht möglich ist
- Durch einen unauffällig installierten Hardwarekeylogger z.B. an lokalen Terminals werden schnell Passwörter erlangt

Beispiel: Bauliche Besonderheiten



Beispiel: Einbruchmeldeanlagen

- Einbruchmeldeanlagen sind nur sinnvoll, falls auch eine Alarmverfolgung stattfindet

Beispiel: Einbruchmeldeanlagen

- ★ Einbruchmeldeanlagen sind nur sinnvoll, falls auch eine Alarmverfolgung stattfindet
- ★ Problem: Fehlalarme kosten Geld und werden irgendwann nur noch halbherzig oder gar nicht mehr verfolgt

Beispiel: Einbruchmeldeanlagen

- Einbruchmeldeanlagen sind nur sinnvoll, falls auch eine Alarmverfolgung stattfindet
- Problem: Fehlalarme kosten Geld und werden irgendwann nur noch halbherzig oder gar nicht mehr verfolgt
- Also: Solange auslösen, bis Sicherheitsdienst nicht mehr erscheint

Aufgefallen, und dann?

- Klassisches Social Engineering hilft weiter, wenn ein Angreifer „entdeckt“ wird
- Selbst professionelle Mitarbeiter des Objektschutzes im Hochsicherheitsbereich verhalten sich bei gut gewählten Erklärungen falsch

Aufgefallen, und dann?

- ★ Klassisches Social Engineering hilft weiter, wenn ein Angreifer „entdeckt“ wird
- ★ Selbst professionelle Mitarbeiter des Objektschutzes im Hochsicherheitsbereich verhalten sich bei gut gewählten Erklärungen falsch

Beispiel:

„Wir führen hier gerade eine Sicherheitsüberprüfung durch. Ich notiere Ihren Namen, damit ich sie lobend erwähnen kann. Bitte behalten sie über die Prüfung Stillschweigen, damit wir weiter testen können.“

Positives

- ★ Gut geschulte Mitarbeiter, die Fremde direkt ansprechen
- ★ Auslösung des Alarms und Eintreffen der Security in weniger als 10 Sekunden
- ★ Mitarbeiter, die bei Geräuschen an der Türe von innen (durch die geschlossene Türe) fragen, ob sie weiterhelfen können

Wie kann man sich schützen?

- Vertrauen sie nicht darauf, dass ein Angreifer nicht ins Gebäude bzw. in bestimmte Räume kommt
- Rechnen Sie immer damit, dass ein Angreifer Zugriff auf Ihr Netzwerk und einzelne Komponenten erlangen kann

Wie kann man sich schützen?

- Vertrauen sie nicht darauf, dass ein Angreifer nicht ins Gebäude bzw. in bestimmte Räume kommt
- Rechnen Sie immer damit, dass ein Angreifer Zugriff auf Ihr Netzwerk und einzelne Komponenten erlangen kann
- Informieren Sie Ihre Benutzer, und stellen Sie genaue Regeln für unbekannte Personen auf
- Insbesondere für Bereichen mit nur wenigen Besuchern ist dies relativ einfach

Wie kann man sich schützen?

- Vertrauen sie nicht darauf, dass ein Angreifer nicht ins Gebäude bzw. in bestimmte Räume kommt
- Rechnen Sie immer damit, dass ein Angreifer Zugriff auf Ihr Netzwerk und einzelne Komponenten erlangen kann
- Informieren Sie Ihre Benutzer, und stellen Sie genaue Regeln für unbekannte Personen auf
- Insbesondere für Bereichen mit nur wenigen Besuchern ist dies relativ einfach
- Treffen Sie Vorkehrungen für den Fall, dass Hardware gestohlen wird (äquivalent zu mobiler Hardware)

(Flucht-)Türen und Fenster

- Tagsüber können meistens nur einzelne Türen alarmüberwacht werden
- Oft reicht hier eine akustische Alarmierung in Verbindung mit geschulten Mitarbeitern

(Flucht-)Türen und Fenster

(Flucht-)Türen und Fenster

(Flucht-)Türen und Fenster

- Tagsüber können meistens nur einzelne Türen alarmüberwacht werden
- Oft reicht hier eine akustische Alarmierung in Verbindung mit geschulten Mitarbeitern
- (Flucht-)Türen dürfen teilweise nachts abgeschlossen werden $\Rightarrow$ Sprechen Sie mit Ihrer Feuerwehr

Einbruchmeldeanlagen

- Stellen Sie fest, wenn Unbefugte Ihre Räume betreten haben
- $\Rightarrow$ Einbruchmeldeanlage und Alarmverfolgung

Einbruchmeldeanlagen

- Stellen Sie fest, wenn Unbefugte Ihre Räume betreten haben
- $\Rightarrow$ Einbruchmeldeanlage und Alarmverfolgung
- Testen Sie die Effektivität Ihrer Alarmverfolgung. Wird das Gebäude überhaupt genauer untersucht, wenn keine Türen beschädigt sind?

Diskussion?

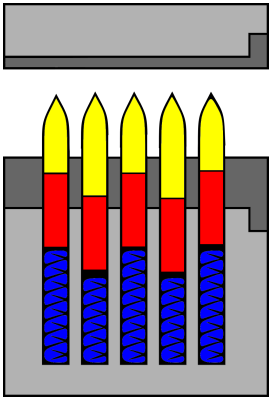
Vielen Dank

RedTeam Pentesting

Übung: Lockpicking

RedTeam Pentesting

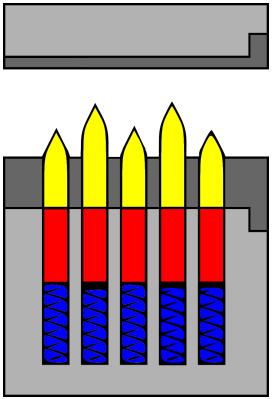
Übung: Lockpicking



Bildquelle: basierend auf Wikipedia/Gree `http://de.wikipedia.org/w/index.php?title=Datei:Schloss-zu.png`

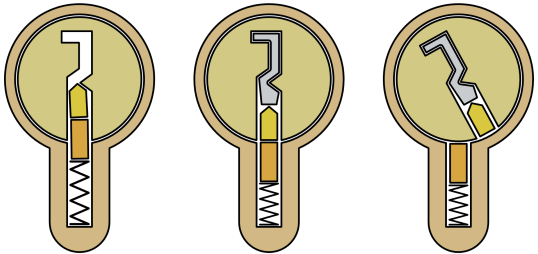
RedTeam Pentesting

Übung: Lockpicking



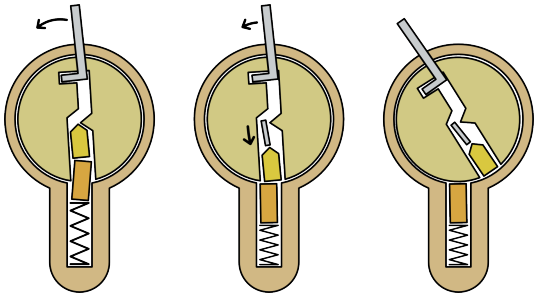
Bildquelle: basierend auf Wikipedia/Gree http://de.wikipedia.org/w/index.php?title=Datei:Schloss-auf.png

Übung: Lockpicking



Bildquelle: basierend auf Wikipedia/Kalkühl `http://de.wikipedia.org/wiki/Datei:CylinderLock-Cut-HotToOpen.svg`

Übung: Lockpicking



Bildquelle: basierend auf Wikipedia/Kalkühl `http://de.wikipedia.org/wiki/Datei:CylinderLock-Cut-HotToOpen.svg`