Hacking for Money - Penetration Testing

Elmar Hoffmann - RedTeam Pentesting
elmar.hoffmann@redteam-pentesting.de
http://www.redteam-pentesting.de/

9. Dezember 2005

Was ist ein Pentest?

- Simulierter Angriff auf ein Netzwerk
- Fragestellung: Wie weit kann ein Angreifer durchdringen?
- Gleiche Methoden wie „die Bösen“
- Nichts kaputt machen
- Vertraulichkeit
- Es wird ein Bericht erstellt
- Besonderheiten bei RedTeam: Kein Test nach Norm

Was ist ein Pentest?

- Simulierter Angriff auf ein Netzwerk
- Fragestellung: Wie weit kann ein Angreifer durchdringen?
- Gleiche Methoden wie „die Bösen“
- Nichts kaputt machen
- Vertraulichkeit
- Es wird ein Bericht erstellt
- Besonderheiten bei RedTeam: Kein Test nach Norm

Was ist ein Pentest?

- Simulierter Angriff auf ein Netzwerk
- Fragestellung: Wie weit kann ein Angreifer durchdringen?
- Gleiche Methoden wie „die Bösen“
- Nichts kaputt machen
- Vertraulichkeit
- Es wird ein Bericht erstellt
- Besonderheiten bei RedTeam: Kein Test nach Norm

Was ist ein Pentest?

- Simulierter Angriff auf ein Netzwerk
- Fragestellung: Wie weit kann ein Angreifer durchdringen?
- Gleiche Methoden wie „die Bösen“
- Nichts kaputt machen
- Vertraulichkeit
- Es wird ein Bericht erstellt
- Besonderheiten bei RedTeam: Kein Test nach Norm

Was ist ein Pentest?

- Simulierter Angriff auf ein Netzwerk
- Fragestellung: Wie weit kann ein Angreifer durchdringen?
- Gleiche Methoden wie „die Bösen“
- Nichts kaputt machen
- Vertraulichkeit
- Es wird ein Bericht erstellt
- Besonderheiten bei RedTeam: Kein Test nach Norm

Was bringt ein Pentest?

- Wie sicher sind wir wirklich?
  - „Betriebsblindheit“
  - Angst vor Industriespionage
  - Kontrollsystem vom Gesetz vorgeschrieben
- Werbung, Imagegewinn

Was bringt ein Pentest?

- Wie sicher sind wir wirklich?
  - „Betriebsblindheit“
  - Angst vor Industriespionage
  - Kontrollsystem vom Gesetz vorgeschrieben
- Werbung, Imagegewinn

Arten von Pentests:

- Black- und Whitebox
- WLAN
- Physikalische Sicherheit
- Phishing/Malware

Arten von Pentests:

- Black- und Whitebox
- WLAN
- Physikalische Sicherheit
- Phishing/Malware

Arten von Pentests:

- Black- und Whitebox
- WLAN
- Physikalische Sicherheit
- Phishing/Malware

Arten von Pentests:

- Black- und Whitebox
- WLAN
- Physikalische Sicherheit
- Phishing/Malware

Aufklärung (Reconnaissance)

- Homepages
- Google
- DNS
- Whois

Aufklärung (Reconnaissance)

- Homepages
- Google
- DNS
- Whois

Aufklärung (Reconnaissance)

- Homepages
- Google
- DNS
- Whois

Aufklärung (Reconnaissance)

- Homepages
- Google
- DNS
- Whois

Enumeration: Finden von Angriffsvektoren

- Port scanning
- (Verwundbare) Versionen von Diensten/Systemen feststellen
  - Nach bekannten Lücken suchen
- Konfigurationsfehler
- Installierte Software auf neue Fehler untersuchen.
- Sonstige kreative Ideen

Enumeration: Finden von Angriffsvektoren

- Port scanning
- (Verwundbare) Versionen von Diensten/Systemen feststellen
  - Nach bekannten Lücken suchen
- Konfigurationsfehler
- Installierte Software auf neue Fehler untersuchen.
- Sonstige kreative Ideen

Enumeration: Finden von Angriffsvektoren

- Port scanning
- (Verwundbare) Versionen von Diensten/Systemen feststellen
  - Nach bekannten Lücken suchen
- Konfigurationsfehler
- Installierte Software auf neue Fehler untersuchen.
- Sonstige kreative Ideen

Enumeration: Finden von Angriffsvektoren

- Port scanning
- (Verwundbare) Versionen von Diensten/Systemen feststellen
  - Nach bekannten Lücken suchen
- Konfigurationsfehler
- Installierte Software auf neue Fehler untersuchen.
- Sonstige kreative Ideen

Enumeration: Finden von Angriffsvektoren

- Port scanning
- (Verwundbare) Versionen von Diensten/Systemen feststellen
  - Nach bekannten Lücken suchen
- Konfigurationsfehler
- Installierte Software auf neue Fehler untersuchen.
- Sonstige kreative Ideen

Exploitation

Ausnutzen von Sicherheitslücken:

- Verifizieren: Haben wir wirklich eine Lücke?
- Was können wir durch Ausnutzen der Lücke erreichen?

Exploitation

Ausnutzen von Sicherheitslücken:

- Verifizieren: Haben wir wirklich eine Lücke?
- Was können wir durch Ausnutzen der Lücke erreichen?

Joker

Was sind Joker, wofür braucht man die?

- Software könnte in Zukunft verwundbar sein
- Ein Angreifer könnte einen eigenen Exploit entwickeln
- Zeit/Geld sparen

Joker

Was sind Joker, wofür braucht man die?

- Software könnte in Zukunft verwundbar sein
- Ein Angreifer könnte einen eigenen Exploit entwickeln
- Zeit/Geld sparen

Joker

Was sind Joker, wofür braucht man die?

- Software könnte in Zukunft verwundbar sein
- Ein Angreifer könnte einen eigenen Exploit entwickeln
- Zeit/Geld sparen

Die üblichen Verdächtigen Teil 1

- Veraltete Software
  - insbesondere Software, die nicht im Online Update des Systems ist.
  - auf Hardware, die nicht geupdated wird
- Schwache Passwörter
- Schwache Konfiguration
  - Admins wird oft nicht genug Zeit gelassen um alles vernünftig zu sichern
- Nur an den Außenrändern des Netzes Firewalls, IDS, etc.
- Zuviele Dienste auf einem Server
- Unnötige Dienste offen

Die üblichen Verdächtigen Teil 1

- Veraltete Software
  - insbesondere Software, die nicht im Online Update des Systems ist.
  - auf Hardware, die nicht geupdated wird
- Schwache Passwörter
- Schwache Konfiguration
  - Admins wird oft nicht genug Zeit gelassen um alles vernünftig zu sichern
- Nur an den Außenrändern des Netzes Firewalls, IDS, etc.
- Zuviele Dienste auf einem Server
- Unnötige Dienste offen

Die üblichen Verdächtigen Teil 1

- Veraltete Software
  - insbesondere Software, die nicht im Online Update des Systems ist.
  - auf Hardware, die nicht geupdated wird
- Schwache Passwörter
- Schwache Konfiguration
  - Admins wird oft nicht genug Zeit gelassen um alles vernünftig zu sichern
- Nur an den Außenrändern des Netzes Firewalls, IDS, etc.
- Zuviele Dienste auf einem Server
- Unnötige Dienste offen

Die üblichen Verdächtigen Teil 1

- Veraltete Software
  - insbesondere Software, die nicht im Online Update des Systems ist.
  - auf Hardware, die nicht geupdated wird
- Schwache Passwörter
- Schwache Konfiguration
  - Admins wird oft nicht genug Zeit gelassen um alles vernünftig zu sichern
- Nur an den Außenrändern des Netzes Firewalls, IDS, etc.
- Zuviele Dienste auf einem Server
- Unnötige Dienste offen

Die üblichen Verdächtigen Teil 1

- Veraltete Software
  - insbesondere Software, die nicht im Online Update des Systems ist.
  - auf Hardware, die nicht geupdated wird
- Schwache Passwörter
- Schwache Konfiguration
  - Admins wird oft nicht genug Zeit gelassen um alles vernünftig zu sichern
- Nur an den Außenrändern des Netzes Firewalls, IDS, etc.
- Zuviele Dienste auf einem Server
- Unnötige Dienste offen

Die üblichen Verdächtigen Teil 1

- Veraltete Software
  - insbesondere Software, die nicht im Online Update des Systems ist.
  - auf Hardware, die nicht geupdated wird
- Schwache Passwörter
- Schwache Konfiguration
  - Admins wird oft nicht genug Zeit gelassen um alles vernünftig zu sichern
- Nur an den Außenrändern des Netzes Firewalls, IDS, etc.
- Zuviele Dienste auf einem Server
- Unnötige Dienste offen

Die üblichen Verdächtigen Teil 2

- Windowsfreigaben im internen Netzwerk für alle les- und schreibbar
  - Bsp.: Userprofiles, man kann Sachen in den Autostart Ordner legen.
- Unsicheres WLAN (gerne auch direkt im Firmennetz)
- Backups für alle lesbar
- Incident Response nicht vorhanden
- Schlechte physikalische Sicherheit

Die üblichen Verdächtigen Teil 2

- Windowsfreigaben im internen Netzwerk für alle les- und schreibbar
  - Bsp.: Userprofiles, man kann Sachen in den Autostart Ordner legen.
- Unsicheres WLAN (gerne auch direkt im Firmennetz)
- Backups für alle lesbar
- Incident Response nicht vorhanden
- Schlechte physikalische Sicherheit

Die üblichen Verdächtigen Teil 2

- Windowsfreigaben im internen Netzwerk für alle les- und schreibbar
  - Bsp.: Userprofiles, man kann Sachen in den Autostart Ordner legen.
- Unsicheres WLAN (gerne auch direkt im Firmennetz)
- Backups für alle lesbar
- Incident Response nicht vorhanden
- Schlechte physikalische Sicherheit

Die üblichen Verdächtigen Teil 2

- Windowsfreigaben im internen Netzwerk für alle les- und schreibbar
  - Bsp.: Userprofiles, man kann Sachen in den Autostart Ordner legen.
- Unsicheres WLAN (gerne auch direkt im Firmennetz)
- Backups für alle lesbar
- Incident Response nicht vorhanden
- Schlechte physikalische Sicherheit

Die üblichen Verdächtigen Teil 2

- Windowsfreigaben im internen Netzwerk für alle les- und schreibbar
  - Bsp.: Userprofiles, man kann Sachen in den Autostart Ordner legen.
- Unsicheres WLAN (gerne auch direkt im Firmennetz)
- Backups für alle lesbar
- Incident Response nicht vorhanden
- Schlechte physikalische Sicherheit

Resultate: Was bringt ein Pentest?

- Zeigt nur punktuelle Schwachstellen
- Was steht im Bericht?
- Wie nutzt man die Ergebnisse des Pentests?

Resultate: Was bringt ein Pentest?

- Zeigt nur punktuelle Schwachstellen
- Was steht im Bericht?
- Wie nutzt man die Ergebnisse des Pentests?

Resultate: Was bringt ein Pentest?

- Zeigt nur punktuelle Schwachstellen
- Was steht im Bericht?
- Wie nutzt man die Ergebnisse des Pentests?

Fragen?