Penetration Testing mit Metasploit

M. Heckel, H. W. Mark

26. Juni 2020

Inhalt

Disclaimer

“Im Rahmen dieser Veranstaltung können und werden Dinge kaputt gehen. Führen Sie solche Angriffe nur an Ihren eigenen Systemen oder nach schriftlicher Genehmigung durch den entspechenden Eigentümer durch.”

Vorteile von Penetrationtests

Vorteile von Penetrationtests

- Realistisches Bild der Sicherheitslage aus Sicht eines Angreifers

Vorteile von Penetrationtests

- Realistisches Bild der Sicherheitslage aus Sicht eines Angreifers
- Häufig Bewertung der Sicherheit unabhängig von Mitarbeitern

Vorteile von Penetrationtests

- Realistisches Bild der Sicherheitslage aus Sicht eines Angreifers
- Häufig Bewertung der Sicherheit unabhängig von Mitarbeitern
- Erhöhen der Sicherheit durch Beheben der gefundenen Schwachstellen

Nachteile von Penetrationtests

Nachteile von Penetrationtests

- Test geht in die Tiefe, nicht in die Breite

Nachteile von Penetrationtests

- Test geht in die Tiefe, nicht in die Breite
- Keine generelle Lösung, nur Teil eines Sicherheitskonzepts

Nachteile von Penetrationtests

- Test geht in die Tiefe, nicht in die Breite
- Keine generelle Lösung, nur Teil eines Sicherheitskonzepts
- **Sicherheit ist kein Zustand sondern ein Prozess.**

Veröffentlichung

Veröffentlichung

- Full disclosure

Veröffentlichung

- Full disclosure
- Responsible disclosure

Veröffentlichung

- Full disclosure
- Responsible disclosure
- No disclosure

Hardware

Hardware

(a) Rubber Ducky

Hardware

(a) Rubber Ducky

(b) Keylogger

Hardware

(a) Rubber Ducky

(b) Keylogger

(c) Logitech Empfänger

Metasploit

Metasploit

- Werkzeug zur Entwicklung und Ausführung von Exploits gegen verteilte Zielrechner

Metasploit

- Werkzeug zur Entwicklung und Ausführung von Exploits gegen verteilte Zielrechner
- Modularer Aufbau

Metasploit

- Werkzeug zur Entwicklung und Ausführung von Exploits gegen verteilte Zielrechner
- Modularer Aufbau
- 2003 von H. D. Moore entwickelt

Metasploit

- Werkzeug zur Entwicklung und Ausführung von Exploits gegen verteilte Zielrechner
- Modularer Aufbau
- 2003 von H. D. Moore entwickelt
- seit 21. Oktober 2009 von Rapid7 weiterentwickelt

Metasploit

- Werkzeug zur Entwicklung und Ausführung von Exploits gegen verteilte Zielrechner
- Modularer Aufbau
- 2003 von H. D. Moore entwickelt
- seit 21. Oktober 2009 von Rapid7 weiterentwickelt
- Aktuelle Version: 5.0.92

Quellen

- https://cdn.shopify.com/s/files/1/0068/2142/products/rubber_ducky_2000x.jpg?v=1590788897
- https://www.keelog.com/imageset/keylogger_13m/keylogger_13m_14.jpg
- https://upload.wikimedia.org/wikipedia/commons/thumb/2/2e/Logitech_Unifying_Receiver_USB.jpg/220px-Logitech_Unifying_Receiver_USB.jpg
- https://www.linkedin.com/in/hdmoore