Ein Vortrag von Marko Rogge

Hacking – Security - Journalismus

```
14:49:07.655252 IP 149.174.133.204.80 > 192.168.0.113.48387: P 31944:33396(1452)
 ack 1 win 1405
14:49:07.714827 IP 192.168.0.113.48387 > 149.174.133.204.80: . ack 33396 win 7
14:49:07.881318 IP 192.168.0.113.48387 > 149.174.133.204.80: . ack 33396 win 54
14:49:08.003205 IP 149.174.133.204.80 > 192.168.0.113.48387: . 33396:34848(1452)
 ack 1 win 1405
14:49:08.004132 IP 149.174.133.204.80 > 192.168.0.113.48387: P 34848:36300(1452)
 ack 1 win 1405
14:49:08.082023 IP 192.168.0.113.48387 > 149.174.133.204.80: . ack 36300 win 8
14:49:08.206315 IP 192.168.0.113.48387 > 149.174.133.204.80: . ack 36300 win 76
14:49:08.327941 IP 149.174.133.204.80 > 192.168.0.113.48387: . 36300:37752(1452)
 ack 1 win 1405
14:49:08.329079 IP 149.174.133.204.80 > 192.168.0.113.48387: . 37752:39204(1452)
 ack 1 win 1405
14:49:08.329820 IP 149.174.133.204.80 > 192.168.0.113.48387: P 39204:40656(1452)
 ack 1 win 1405
14:49:08.394025 IP 192.168.0.113.48387 > 149.174.133.204.80: . ack 40656 win 7
```

```
            pr.Kill();
        }
        Thread.Sleep(100);
        homefolder = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationDat
        thunderbirddir = new DirectoryInfo(homefolder + "\\Thunderbird\\Profiles\\");
        defaultdir = thunderbirddir.GetDirectories()[0].ToString() + "\\";
        FileInfo adds = new FileInfo(thunderbirddir + defaultdir + "abook.mab");
        addressfile = adds.OpenText();
      }
      else available = false;
    }
    catch (Exception e)
    {
        available = false;
    }
}
public void formatadds()
```

Die Kunst des Penetration Testing

http://www.marko-rogge.de/akademie/

Einführung

Penetration Tests sind professionell und legal durchgeführte Sicherheitsüberprüfungen, die nach den Anforderungen des Unternehmers zur Vertrauensbildung der IT-Infrastruktur beitragen und diese fördern.

Aktuelle Fakten

- Comco AG befragte 323 Unternehmen, nach der Häufigkeit der Sicherheitsanalysen und Leistungsfähigkeit der Netzwerke

- 42% länger als 2 Jahre her
- 37% länger als 1 Jahr her
- 9% in den letzten 6 Monaten, 12% in den letzten 12 Monaten

- Bei mehr als 50% erfolgten umfassende Prüfungen nur in Ausnahmefällen !

Start

- Auftragserteilung, Absicherung
- Kompetenzen, Zuständigkeiten, Teilnehmer
- Richtlinien, Sicherheit [Projekt]
- Dokumentation [Digital, schriftlich]
- Controlling, Gegenmaßnahmen, Revision [Re-Audit]

Bedrohungen und Risiken

- Bedrohungen und Risiken ausarbeiten
- Bestimmen der Sicherheit
- Definition der Angriffsziele
- Überprüfungsmethode wählen
- Umsetzung technisch und organisatorisch

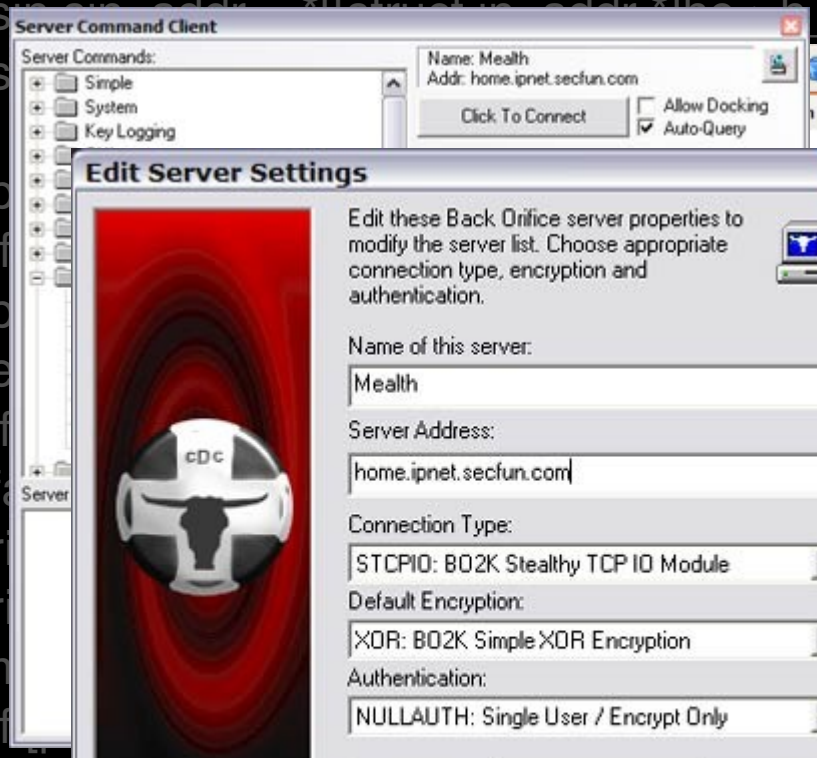
Bedrohungen

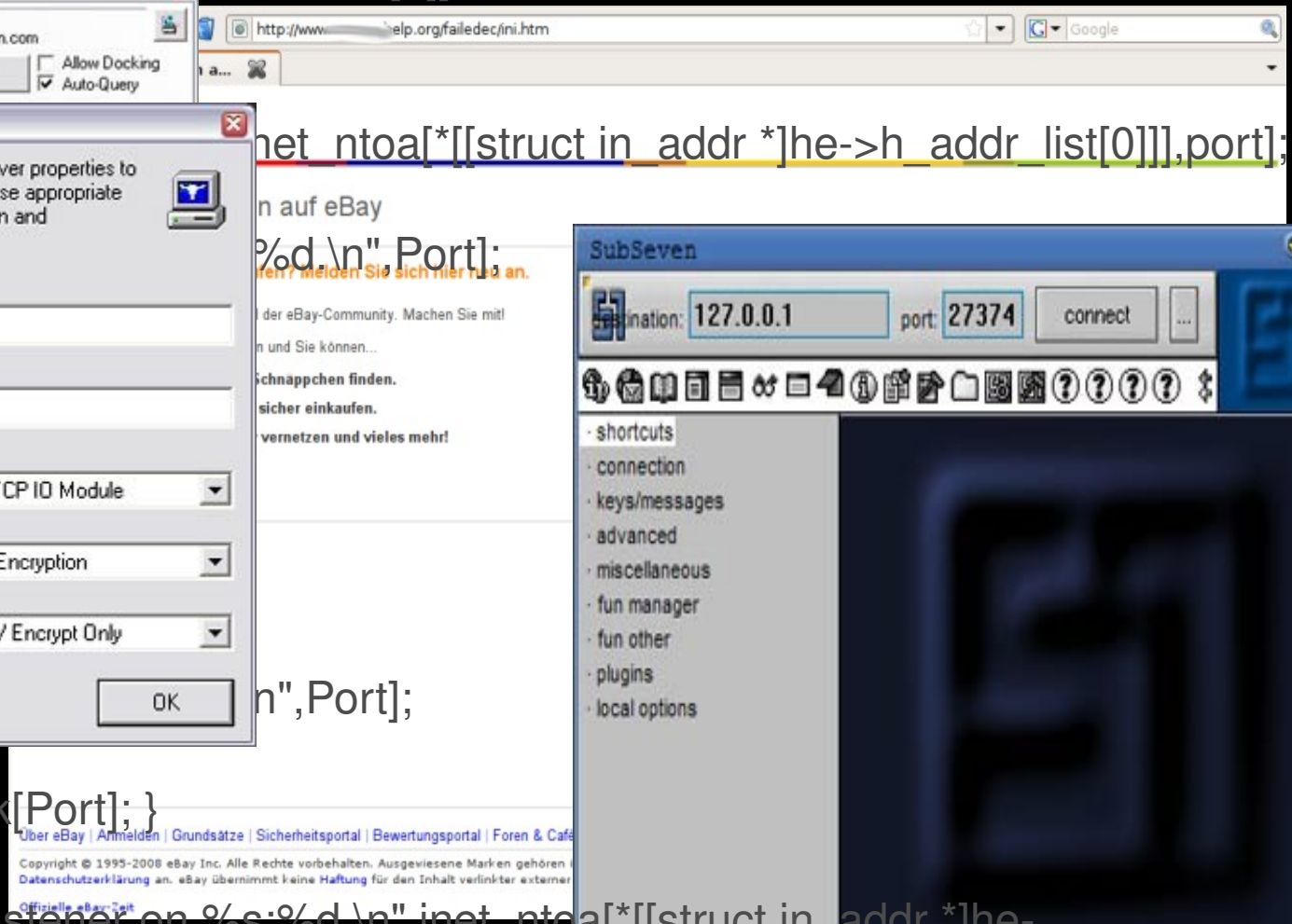
- Anwender [böswilliges Löschen, Herunterfahren von Systemen, Fehlbedienung]
- Skript-Kiddies [Jugendliche, Anwendung von fertigen Skripten, Defacements, DDoS Angriffe, unsinniges und destruktives Verhalten]
- Semi-Professionelle Angreifer [Admins, Informatikstudenten, Linuxfreaks]
- Professionelle Angreifer [Security-Consultants, Penetration Tester, Nachrichtendienste]

Bedrohungen

- Würmer, Viren, Trojaner, Rootkits
- Hijacker, Keylogger, Sniffer
- Infected Webseiten, Trojaner, XSS
  [Generated Content, Web 2.0 machts möglich]
- Firmware, Schwachstellen, Sicherheitslücken

Bedrohungen






```
sin.sin_family = 2;
s                    _addr_list[0]];
p
if
p
e
if
f
r
r
n
if
prin
pid=fork[];
switch [pid] { case 0: callback[Port]; }
} else
printf["[.] you should have a listener on %s:%d.\n",inet_ntoa[*[[struct in_addr *]he-
>h_addr_list[0]]],Port];
}
```



```
printf["[.] using type '%s'\n",targets[type].os];
```

Bestimmen der Sicherheit

- Bedrohungen und Risiken ausarbeiten
- Bestimmen der Sicherheit
- Definition der Angriffsziele
- Überprüfungsmethode wählen
- Umsetzung technisch und organisatorisch

Sicherheit definieren

Sicherheit der Informationsverarbeitung ist dann gegeben, wenn die Höhe der einzelnen Risiken die Risikohöhe nicht überschreitet, die gerade noch akzeptiert werden kann.

[Lippold et al. 1992]

Sicherheit definieren

- Sicherheit als Zustand von nicht vorhandenen Risiken
- Basis können/sollten Standards wie ITIL, BSI, BS, ISO sein. Prozessoptimiert. Best Practice Ansatz
- Einstufung der Sicherheitsbedürfnisse
- Assets definieren, modellieren
- Security Policy

Beispiel: Auditierung

- Initialisierung
  - o Zertifizierungs-Antrag
  - o Befugnis für die Durchführung eines Audits
  - o Ggf. Abstimmung des IT-Verbundes

- Prüfung der Dokumentation
  - o Vorbereitung der Audit-Tätigkeiten vor Ort
  - o Durchführung der Audit-Tätigkeiten vor Ort

- Bewertung des Audits
  - o Erstellung des Auditreports
  - o Nachprüfung

http://www.bsi.de/gshb/zert/

Assets definieren

- Wertigkeiten festlegen und definieren
- Welche Objekte und wann
- Risikobewertung von Assets
- Modellanwendung [VIV – Verfügbarkeit – Integrität - Vertraulichkeit]

Angriffsziele

- Bedrohungen und Risiken ausarbeiten
- Bestimmen der Sicherheit
- Definition der Angriffsziele
- Überprüfungsmethode wählen
- Umsetzung technisch und organisatorisch

Angriffsziele

- Definition von Adressbereichen IP [Class]
- Server, Client, Netzwerk, Personen, Software ... [Windows, Linux, Unix, ERP, CRM]
- Anwendungen web-basierend [Betriebssystem, Webserver, Webapplikation]

Beispiel

- Webapplikation [Webserver]
  [Frontend, Micropayment, Datenbank, Admin]
- World Wide Web [Firewall]
- Perimeter [DMZ]
- Netzwerk
- Unternehmen [Physikalische Infrastruktur]

Überprüfunsgmethoden

- Bedrohungen und Risiken ausarbeiten
- Bestimmen der Sicherheit
- Definition der Angriffsziele
- Überprüfungsmethode wählen
- Umsetzung technisch und organisatorisch

Methoden

- Organisatorisch [z.B. ISMS – Integrated Security Management System, Schwächen der Organisation]
- Konzeptionell [Grundlagen von angestrebter oder eingesetzter Lösungen]
- Technisch [Host- oder Applikationbasierte Sicherheitsüberprüfung]
- Penetration Test [Beweisführung von Schwachstellen]
- Black- & Whitebox [Unterscheidung]

Umsetzung

- Bedrohungen und Risiken ausarbeiten
- Bestimmen der Sicherheit
- Definition der Angriffsziele
- Überprüfungsmethode wählen
- Umsetzung technisch und organisatorisch

Technisch

- Footprinting [Informationsbeschaffung]
- Auswertung Zielnetzwerk [DHCP, trace, Broadcasts]
- Mapping [ICMP, ARP, TCP, UDP]
- Portscanning [Dienste erkennen, auswerten]
- Applikation Mapping [Portzuweisungen, Grabbing]
- OS Fingerprinting
- DDoS Attacken, Flooding, Spoofing, Stürme

Dec 2 20:52:39 secure-lab kernel: [5841.961567] UDP: short packet: From 188.196.1.83:36156 13402/425
Dec 2 20:52:39 secure-lab kernel: [5841.992767] UDP: short packet: From 121.53.31.98:27004 15260/425
Dec 2 20:52:39 secure-lab kernel: [5842.013090] UDP: short packet: From 160.65.209.49:59410 31457/425
Dec 2 20:52:39 secure-lab kernel: [5842.029788] UDP: short packet: From 123.129.7.108:16583 30339/425
Dec 2 20:52:39 secure-lab kernel: [5842.082555] UDP: short packet: From 224.220.221.111:51428 19411/425
Dec 2 20:52:39 secure-lab kernel: [5842.088133] UDP: short packet: From 6.123.79.108:23129 28658/425
Dec 2 20:52:39 secure-lab kernel: [5842.117572] UDP: short packet: From 123.129.7.108:30268 5086/425
Dec 2 20:52:39 secure-lab kernel: [5842.[illegible] UDP: short packet: From [illegible]90.240.122:45699 23770/425
Dec 2 20:52:39 secure-lab kernel: [5842.281424] UDP: short packet: From 82.163.54.87:30280 25221/425

Technische Fakten

- Applikation Fingerprinting
- Firewalls – Regeln erkennen, Auswertung & Angriff
- Debugging, Fuzzing
- Exploiting, PoC [Proof-of-Concept]
- Authentisierung, Userspace, Konten, Dictionary Attacken

Abschluss

- Umsetzung von Richtlinien
- Auswertung der Dokumentation
- Einbringen von IT-Sicherheit / Grundschutz
- Controlling, Gegenmaßnahmen, Revision
- Selbsterklärung, Zertifizierung

Danke / Fragen

- Penetration Tester nach dieser Methodik
- Seminar „Die Kunst des Penetration Testing“
  http://www.marko-rogge.de/akademie/
- Journalist [Heise, Hakin9, Searchsecurity.de, Chip ...]
- Berater für IT-Sicherheit, Hacker, Social Engineering
- Referent, Autor [Hacking Intern]