Abwehr

Technische Security Audits nach OSSTMM

Christoph Baumgartner, Pete Herzog und Martin Rutishauser

Schwierigkeitsgrad

Das Open Source Security Testing Methodology Manual (OSSTMM) von ISECOM (Institute for Security and Open Methodologies) beschreibt eine Methode, wie technische Security Audits geplant, durchgeführt und dokumentiert werden. In diesem Artikel wird anhand eines konkreten Beispiels erklärt, wie ein OSSTMM-konformer Security Audit exklusive Dokumentation durchgeführt wird.

Das im Beispiel genannte Untersuchungsobjekt ist der extern gehostete Webserver der OneConsult GmbH, weil derartige Tests nicht ohne vorherige Genehmigung des Systemeigners und des Systembetreibers durchgeführt werden dürfen. Die Tests erfolgen aus externer Sicht (= vom Internet her gesehen).

Historie und Kurzvorstellung OSSTMM

Das *Open Source Security Testing Methodology Manual* (OSSTMM) beschreibt eine Methode zur Planung, Durchführung und Dokumentation von technischen Sicherheitsüberprüfungen. Die Erstausgabe erfolgte 2000 durch Pete Herzog. Seit 2001 wird das OSSTMM unter der Leitung von Pete Herzog von ISECOM (Institute for Security and Open Methodologies) kontinuierlich weiterentwickelt und erfreut sich einer wachsenden Verbreitung und Beliebtheit – dies nicht zuletzt aufgrund der Konformität zu diversen Normen, Regulatorien und Frameworks, wie beispielsweise ISO/IEC 17799, BASEL II, SOX, IT GSHB und ITIL.

Die Worte *Open Source* im OSSTMM stehen dafür, dass die Methode ohne Lizenzgebühren frei verfügbar und nutzbar ist.

Die zum Zeitpunkt der Artikeleinreichung aktuelle Version 2.2 des OSSTMM umfasst 129 A4-Seiten und besteht aus drei Elementen:

- Methodik;
- RAV-Kalkulation;
- OSSTMM-Templates;

In diesem Artikel erfahren Sie...

- Was das Open Source Security Testing Methodology Manual ist;
- Was Sinn und Nutzen eines Audits nach OSSTMM sind;
- Wie ein OSSTMM-konformer technischer Security Audit durchgeführt wird.

Was Sie vorher wissen/können sollten...

- Dass Sicherheitsüberprüfungen in den meisten Ländern ohne das vorherige Einverständnis von Systemeigner und Systembetreiber strafbar sind;
- Wie man die erwähnten Security Tools unter Linux installiert und konfiguriert.

Die korrekt ausgefüllten *OSSTMM-Templates* bilden zusammen mit dem Action Log des Testers und dem *Netzwerk-Traffic-Dump* die Minimalanforderungen an eine OSSTMM-konforme Dokumentation.

Präambel

Aus Platzgründen wird der Umfang der einzelnen *Module* nicht vollständig wiedergegeben und es werden nicht alle Tasks vollständig abgearbeitet. Das OSSTMM definiert nicht, mit welchen Tools getestet werden soll, fordert aber, dass die Resultate immer mit einem zweiten Tool mit gleicher Funktionalität verifiziert werden. Teilweise wird in den Beispielen auf den Einsatz zweier Tools mit gleicher Funktionalität verzichtet, aber es werden oftmals geeignete Tools namentlich genannt.

Falls möglich, sollten immer die IP-Adressen statt der Systemnamen der zu testenden Systeme verwendet werden, um mögliche Probleme im Zusammenhang mit forwarded Ports, Virtual Hosting und vom DNS zufällig zugeteilten IP-Adressen zu vermeiden. Andernfalls wird die Datenanalyse erschwert. Aus Gründen der leichteren Verständlichkeit wurde in diesem Artikel oneconsult.com in das */etc/hosts-File* für die Adressauflösung aufgenommen.

Vom Einsatz von All-in-One Security Scannern (oft kommerziell) rät das OSSTMM aufgrund der nicht möglichen Verifizierbarkeit des Scanner-Quellcodes und der erschwerten Nachvollziehbarkeit der Tests und der Resultate ab. Dies gilt aber generell für alle technischen Security Audits der Qualitätsstufe Penetration Test. Die in diesem Artikel genannten Tools sind Open Source Tools – aber es kann selbstverständlich auch mit kommerzieller Software gearbeitet werden.

Das OSSTMM in seiner aktuellsten Version (zum Zeitpunkt der Artikeleinreichung V. 2.2.) ist derzeit nur in Englisch verfügbar. Die Version 2.1. ist auch in Spanisch erhältlich. Das OSSTMM kann kostenlos auf der Website http://www.osstmm.org/ heruntergeladen werden.

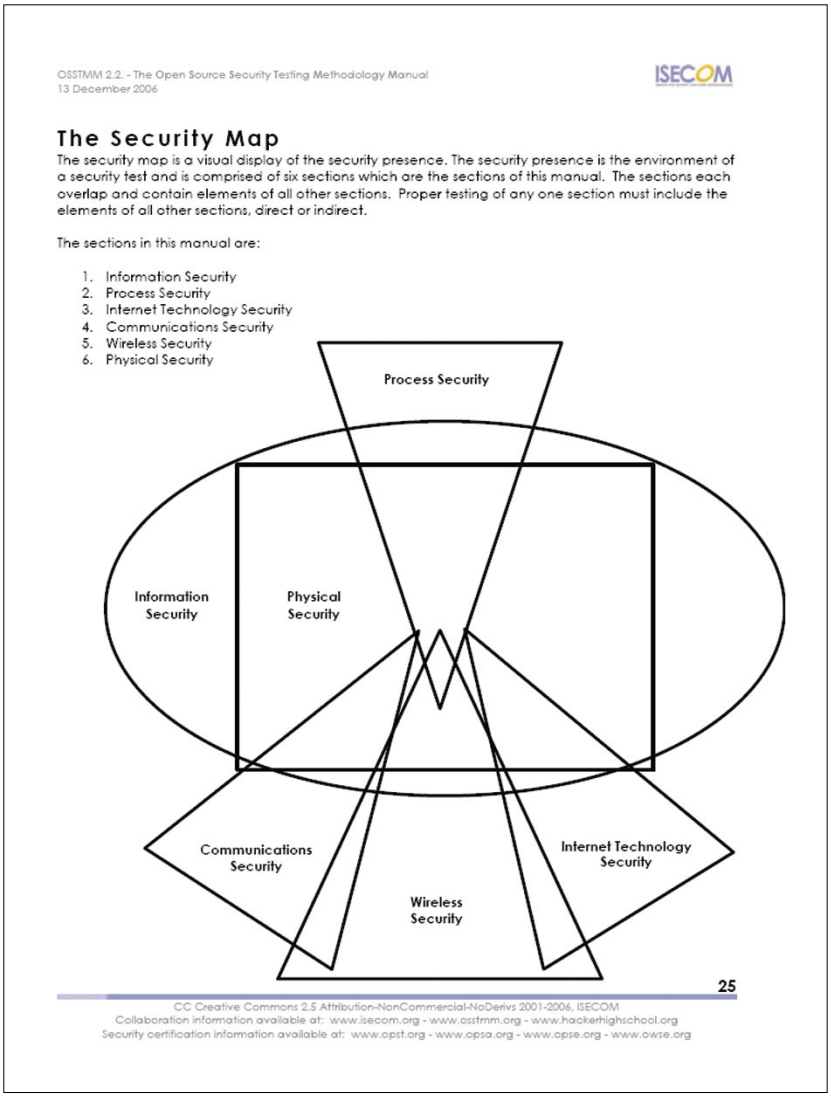


Abbildung 1. *Security Map des OSSTMM*

OSSTMM-konformer Test in Stichworten

Es müssen mindestens folgende Schritte für den Remote-Test eines mit dem Internet verbundenen Systems durchlaufen werden:

- Vorbereitungen treffen:
  - Tester Tools updaten (z. B. Plugins bei Vulnerability Scannern oder neue Releases installieren);
  - Action Log einrichten/führen;
  - Netzwerksniffer: Netzwerktraffic mitschneiden und Netzwerksniffer zur laufenden visuellen Kontrolle während Tests starten;
- IP-Adressen bzw. -Ranges prüfen:
  - Gehören die IP-Ranges wirklich dem Auftraggeber?;
  - Sind sie erreichbar oder was ist im Subnet erreichbar?;
  - Welche Komponententypen belegen welche IPs (Server, Netzwerkkomponente, Clients oder Peripheriegerät)?;
  - Gibt es etwas zu beachten (z.B. instabile Systeme)?;
- Port und Service Scan durchführen:
  - Port Scan;
  - OS Detection;
  - Service Detection;
  - Informationsabflüsse;
- Vulnerability Scan ausführen (zur Tool-gestützten Identifikation von Sicherheitslücken):
  - generelle Vulnerability Scanner;
  - spezifische Vulnerability Scanner für Web Services oder Datenbanken;

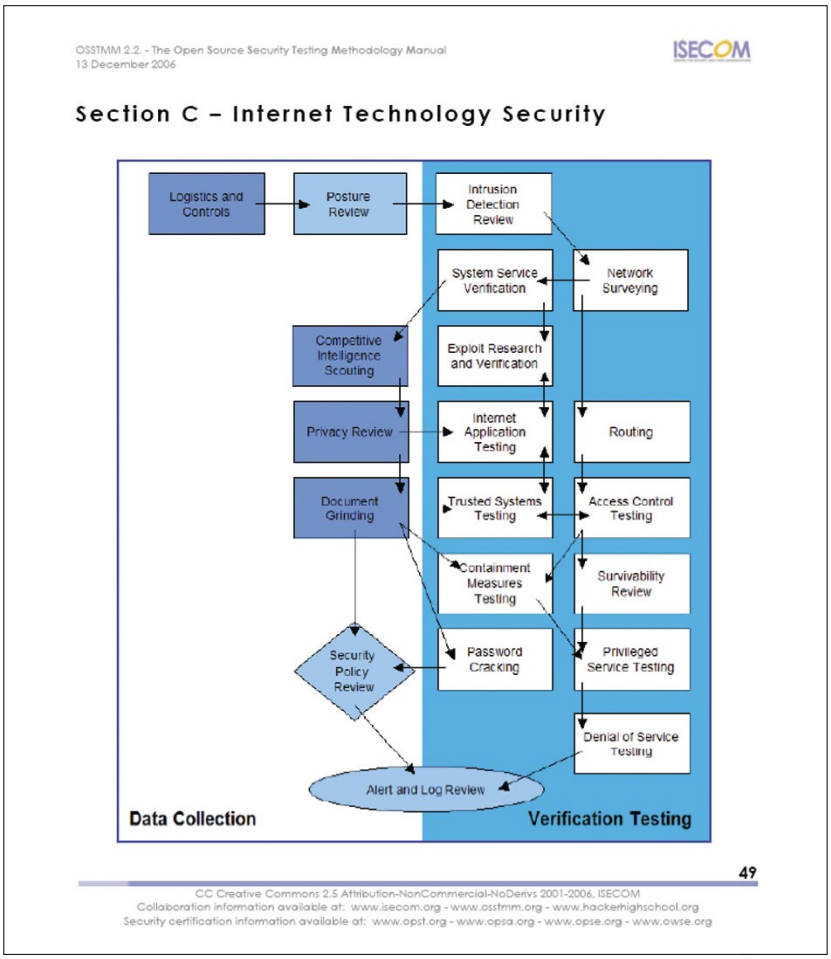


Abbildung 2. *Ablaufschema von Section C des OSSTMM*

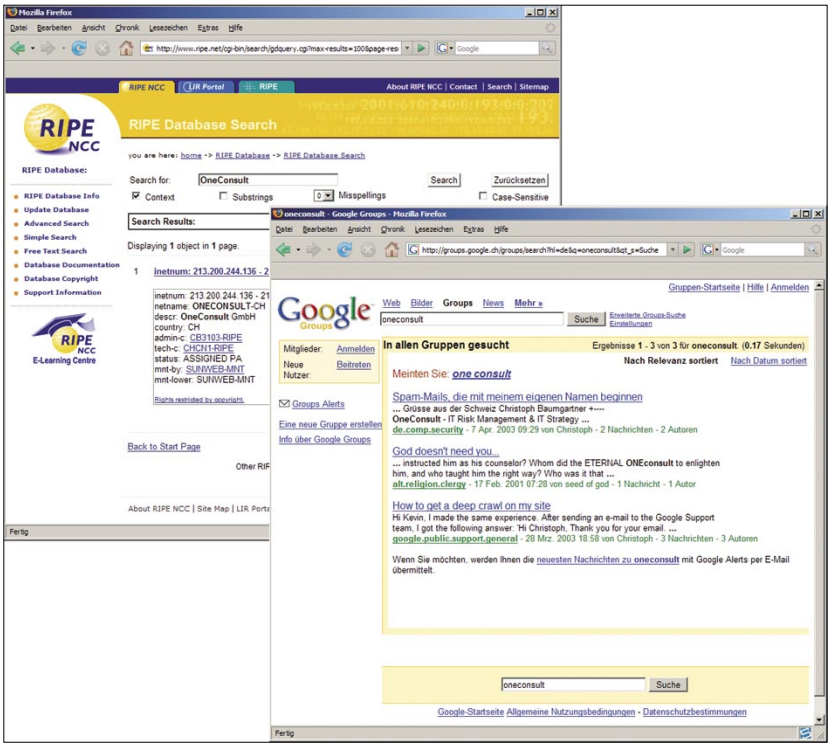


Abbildung 3. *Abfrage der IP-Ranges via http://www.ripe.net/ und der Newsgroup-Beiträge*

- Sicherheitslücken verifizieren:
  - Verifikation der identifizierten Sicherheitslücken beispielsweise mittels Exploiting;
- Resultate:
  - Analysieren (auch auf Plausibilität, Datenintegrität und Vollständigkeit);
  - RAV-Berechnung durchführen;
  - Dokumentieren (Schlussbericht inklusive: RAV und ausgefüllten OSSTMM-Templates, Action Log, Dump des Netzwerktraffics und Rohdaten auf Datenträger);
  - mit den Verantwortlichen besprechen.

Aufbau des OSSTMM

Das OSSTMM ist in verschiedene *Sections* gegliedert, welche die verschiedenen Bereiche der Security Map abdecken.

Die Sections wiederum sind in *Moduls* gegliedert, welche aus einzelnen *Tasks* bestehen, die durchlaufen werden müssen. Für diesen Artikel relevant ist *Section C*, welche sich mit Tests von via Netzwerk erreichbaren Systemen befasst.

Aufgrund der Funktionalität können bestimmte Tools teilweise in verschiedenen OSSTMM-Modulen eingesetzt werden.

Es folgt eine Kurzvorstellung der Module von Section C, wobei die Module die gleiche Nummerierung aufweisen wie im OSSTMM.

Network Surveying (Modul 1)

Im Modul Network Surveying werden Informationen gesammelt, ohne das eigentliche Untersuchungsobjekt mittels intrusiven Tests zu attackieren. Es dient dazu, sich einen Überblick über das Untersuchungsobjekt zu verschaffen. Hierzu wird geprüft, ob die vom Auftraggeber genannten Domains, IP-Adressen oder IP-Ranges tatsächlich ihm gehören – andernfalls könnte der Tester sich in den folgenden Modulen strafbar machen. Ausserdem wird in den DNS-Einträgen nach Servern und in Newsgroups nach Einträgen

gesucht, welche die Domain(s) des Untersuchungsobjekts beinhalten. Für diese Zwecke eignen sich beispielsweise die Tools dig, whois, host und Abfragen via Browser.

Des weiteren kann der Quelltext von Websites auf interne Links zu Applikationen und andere Systeme durchsucht und Mailheader bezüglich Angaben über involvierte Systeme analysiert werden.

Außerdem gilt es sicherzustellen, dass die Testing-Tools sowie die Netzwerkeinstellungen korrekt konfiguriert sind. Dies wird erreicht, indem die tatsächlich zur Verfügung stehende Bandbreite geprüft, die Route zu den Zielsystemen und allfällige Paketverluste eruiert werden. Diese Tests müssen für alle zu testenden Systeme ausgeführt werden, weil andernfalls während der eigentlichen Tests *False Positives* oder *False Negatives* auftreten können.

Aus Platzgründen wird hier auf die Auflistung sämtlicher Teilschritte verzichtet, aber anhand des Tools *traceroute* aufgezeigt, über welche Pfade das Zielsystem erreicht werden kann. Falls bei einem oder nach einem Hop keine Antworten mehr zurückkommen, deutet dies auf eine filternde Komponente (z.B. *Firewall*) hin. Je mehr Hops zwischen dem System des Testers und dem zu testenden System liegen, desto länger dauert der Test.

Listing 1. *Abfrage von DNS-Informationen mit dig*

```
# dig oneconsult.com any
; <<>> DiG 9.3.2 <<>> oneconsult.com any
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17471
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;oneconsult.com.    IN    ANY
;; ANSWER SECTION:
oneconsult.com.    64200    IN    NS    ns2.nameserver.ch.
oneconsult.com.    64200    IN    NS    ns1.nameserver.ch.
;; AUTHORITY SECTION:
oneconsult.com.    64200    IN    NS    ns2.nameserver.ch.
oneconsult.com.    64200    IN    NS    ns1.nameserver.ch.
;; ADDITIONAL SECTION:
ns1.nameserver.ch.    1034    IN    A    217.71.80.188
ns2.nameserver.ch.    909    IN    A    217.71.81.4
;; Query time: 13 msec
;; SERVER: 192.168.60.1#53(192.168.60.1)
;; WHEN: Mon Dec  4 14:07:42 2006
;; MSG SIZE  rcvd: 141
# dig oneconsult.com mx
; <<>> DiG 9.3.2 <<>> oneconsult.com mx
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48932
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4
;; QUESTION SECTION:
;oneconsult.com.    IN    MX
;; ANSWER SECTION:
oneconsult.com.    3600    IN    MX    10 mail.oneconsult.com.
;; AUTHORITY SECTION:
oneconsult.com.    12880    IN    NS    ns1.nameserver.ch.
oneconsult.com.    12880    IN    NS    ns2.nameserver.ch.
;; ADDITIONAL SECTION:
mail.oneconsult.com.    3600    IN    A    195.129.94.130
mail.oneconsult.com.    3600    IN    A    195.129.94.194
ns1.nameserver.ch.    219    IN    A    217.71.80.188
ns2.nameserver.ch.    1560    IN    A    217.71.81.4
;; Query time: 49 msec
;; SERVER: 192.168.50.6#53(192.168.50.6)
;; WHEN: Mon Dec 14 14:08:09 2006
;; MSG SIZE  rcvd: 166
```

Port Scanning (Modul 2)

Dies ist das erste Modul, welches intrusive Tests beinhaltet. Mittels verschiedenartiger Port Scans (SYN-, ACK- , Bounce-Scans, etc.) wird ermittelt, welche Systeme erreichbar sind, welche Protokolle unterstützt werden, wie der Status der 65'536 (inklusive Port 0) TCP und UDP Ports ist und welche Dienste (inklusive Versionen) angeboten werden. Es ist allerdings nicht immer nötig, den gesamten Port Range zu testen. Außerdem wird eine Firewall (falls vorhanden) aktiv getestet um allfällige weitere Systeme zu finden. Tabelle 1 hilft bei der Eruierung der Portstati.

Services Identification (Modul 3)

In diesem Modul wird nach Applikationen gesucht, welche hinter den Diensten lauschen. Es kommt oft vor, dass mehr als eine Applikation hinter einem Dienst existiert, wobei eine Applikation als Listener (Lauscher) agiert und die anderen als deren Komponenten agieren. Ein Beispiel dafür ist PERL, welches als Best andteil einer Web-Applikation installiert wurde. In diesem Fall ist der http-Deamon der Listener und eine seiner Komponenten PERL.

Fingerprinting-Tools liefern generell unzuverlässige Resultate. Aus diesem Grund ist die Verifikation von deren Ergebnissen unumgänglich. System- und Diensttypen können beispielsweise mittels Untersuchung von Headern, 404- und Error-Pages, html-Seiten, initial TTLs, installierten Komponenten und Verwundbarkeiten (welche ausgenutzt werden konnten), verifiziert werden.

Aufgrund von forwarded Ports kann die gleichzeitige Service- und System Identification irreführende Ergebnisse liefern.

Beispiele zur Services Identification finden sich in den Listings 8 ff.

Listing 2. *Abfrage von Domain-spezifischen Informationen mit whois*

```
# whois oneconsult.com
Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net for
                    detailed information.
   Domain Name: ONECONSULT.COM
   Registrar: KEY-SYSTEMS GMBH
   Whois Server: whois.rrpproxy.net
   Referral URL: http://www.key-systems.net
   Name Server: COM1.NAMESERVER.CH
   Name Server: COM2.NAMESERVER.CH
   Status: REGISTRAR-LOCK
   EPP Status: clientTransferProhibited
   Updated Date: 31-Oct-2006
   Creation Date: 22-Sep-2002
   Expiration Date: 22-Sep-2007
>>> Last update of whois database: Mon, 14 Dec 2006 08:08:21 EST <<<
[…]
DOMAIN: ONECONSULT.COM
RSP: domaindiscount24.com
URL: http://www.dd24.net
created-date: 2002-09-23
updated-date: 2006-11-01
registration-expiration-date: 2007-09-23
owner-contact: P-CIB44
owner-organization: OneConsult GmbH
owner-fname: Christoph
owner-lname: Baumgartner
owner-street: Zuercherstrasse 73
owner-city: Thalwil
owner-zip: 8800
owner-country: CH
owner-phone: +41 (0)43 443 52 52
owner-fax: +41 (0)43 443 52 62
owner-email: info@oneconsult.com
[…]
nameserver: com1.nameserver.ch
nameserver: com2.nameserver.ch
…
```

Listing 3. *Traceroute UDP*

```
# traceroute www.oneconsult.com
traceroute: Warning: www.oneconsult.com has multiple addresses; using
                    195.129.94.193
traceroute to 195.129.94.193 (195.129.94.193), 30 hops max, 38 byte packets
 1  192.168.60.1 (192.168.60.1)  0.392 ms  0.286 ms  0.180 ms
 2  zrhth-pe2.cybernet-ag.ch (212.90.192.151)  8.921 ms  9.011 ms  9.110 ms
[…]
 7  212.71.100.18 (212.71.100.18)  14.054 ms  12.435 ms  12.319 ms
 8  * 212.71.100.18 (212.71.100.18)  13.896 ms !X *
```

Listing 4. *Traceroute ICMP*

```
# traceroute -I www.oneconsult.com
traceroute: Warning: www.oneconsult.com has multiple addresses; using
                    195.129.94.193
traceroute to 195.129.94.193 (195.129.94.193), 30 hops max, 38 byte packets
 1  192.168.60.1 (192.168.60.1)  0.256 ms  0.187 ms  0.176 ms
 2  zrhth-pe2.cybernet-ag.ch (212.90.192.151)  9.475 ms  8.272 ms  8.868 ms
[…]
 7  212.71.100.18 (212.71.100.18)  13.294 ms  12.724 ms  13.286 ms
 8  212.71.100.18 (212.71.100.18)  13.890 ms !X
```

System Identification (Modul 4)

In diesem Modul wird mittels OS-Fingerprinting das Betriebssystem inklusive Version ermittelt.
Weitere Tools:

- *scanudp*;
- *dcetest*;
- *rpcinfo*;
- *nbtscan*;
- *smbclient*;
- *snmpwalk*;
- *showmount*;
- *sing*;
- *ike-scan*.

Vulnerability Research and Verification (Modul 5)

In diesem Modul werden Schwachstellen, Konfigurationsfehler und Verwundbarkeiten eines Hosts oder Netzwerkes identifiziert und verifiziert. In den vorhergehenden Modulen wurden mittels technischer und konzeptioneller Mittel Informationen über das Untersuchungsobjekt gesammelt. Jetzt gilt es, die erlangten Informationen entweder manuell oder (teil-)automatisiert (mittels Tools) mit bekannten Sicherheitslücken und Schwachstellen zu vergleichen, welche für die detektierten Dienste des Untersuchungsobjekts bekannt sind.

Identifikation von Sicherheitslücken

Für die Identifikation von Sicherheitslücken werden Online-Datenbanken wie beispielsweise *http://cve.mitre.org/cve/*, *http://secunia.com/* oder *http://osvdb.org/* und spezifische Mailinglists wie *Full Disclosure* oder *Bugtraq* konsultiert.

Unterstützung mittels Tools

Vulnerability Scanner vereinfachen diese Aufgabe und ermöglichen signifikante Zeiteinsparungen im Vergleich zur rein manuellen Vorgehensweise. Die nötige Voraussetzung ist aber der Zugriff auf Datenbanken mit möglichst tagesaktuellen Listen von bekannten Sicherheitslücken und Schwachstellen. Der Security Scanner *nessus* ist eine

gute Hilfe, allerdings verwendet die kostenlose Version nur Plugins (= `Testscripts`), welche älter als eine Woche sind. Alternativ kann die kommerzielle Variante von *nessus* verwendet werden, welche den Zugriff auf die aktuellsten Plugins ermöglicht.

nikto ist speziell für die Analyse von Webservices bestimmt. Auch *nikto* arbeitet mit einer Datenbank von bekannten Sicherheitslücken und vergleicht diese mit der angetroffenen Webserver-Konfiguration.

Verifizierung

Identifizierte Sicherheitslücken und Schwachstellen müssen verifiziert werden um *False Positives* ausschliessen zu können. Dies kann mit einzelnen Exploits oder einem Framework, wie beispielsweise *metasploit,* erfolgen. Dieses Framework enthält diverse konfigurierbare Exploits für bekannte Sicherheitslücken – was den Verifikationsprozess (teil-) automatisiert.

Ansonsten werden in dieser Phase öffentlich verfügbare Exploit-Codes verwendet und die Verifikation manuell durchgeführt.

Internet Application Testing (Modul 6)

Bei der Suche nach Sicherheitslöchern in Internet-Applikationen sind verschiedenartige Techniken erforderlich, welche unterschiedliche Aspekte berücksichtigen. Brute Forcing von Passwörtern, API-Monitoring, Networksniffing, Decompilation, Reverse Engineering and Client Bypassing sind nur einige Beispiele.

Obwohl kein derzeit verfügbares Tool einen manuellen Audit ersetzen kann, bei welchem die gesamte Website auf die lokale Festplatte des Testers geladen wird, um sie anschliessend akribisch zu untersuchen können dennoch Tools die Arbeit des Testers unterstützen.

Web-Applikationen lassen sich beispielsweise mit dem lokal zu installierenden Tool paros proxy auf Sicherheitslücken hin überprüfen. Es handelt sich dabei um einen Man-in-the-Middle-Proxy, womit Anfragen und Antworten zwischen Webserver

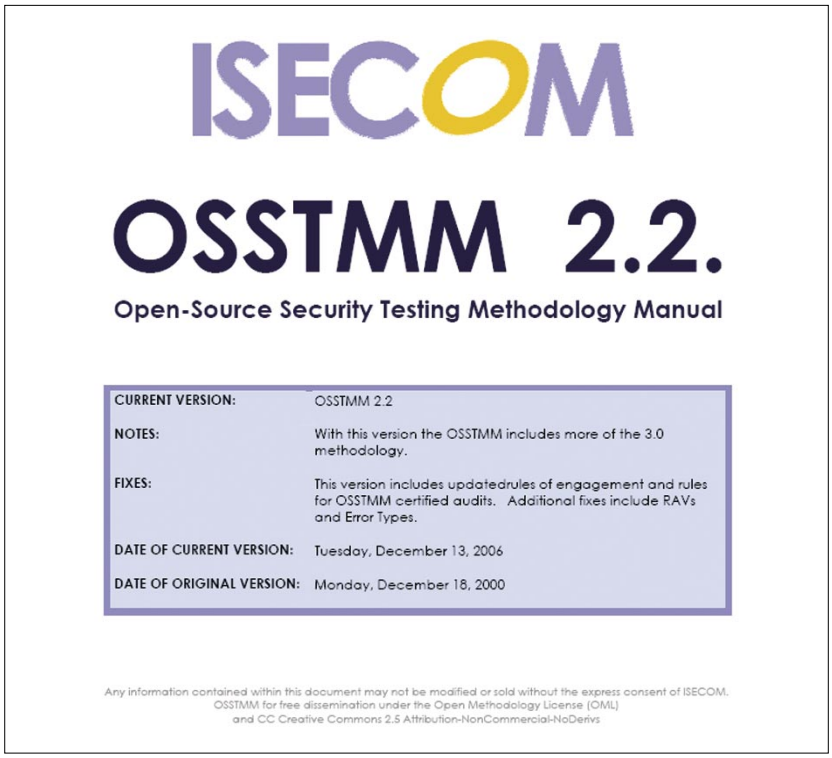


Abbildung 4. *Open-Source Security Testing Methodology Manual*

Listing 5. *Traceroute TCP mit tcptraceroute*

```
# tcptraceroute www.oneconsult.com
Selected device eth0, address 192.168.60.117, port 45919 for outgoing packets
Tracing the path to www.oneconsult.com (195.129.94.193) on TCP port 80
                    (http), 30 hops max
 1  192.168.60.1  0.307 ms  0.182 ms  0.175 ms
 2  zrhth-pe2.cybernet-ag.ch (212.90.192.151)  9.130 ms  8.955 ms  9.487 ms
[…]
 7  212.71.100.18  12.901 ms  14.469 ms  13.008 ms
 8  195.129.94.193 [open]  12.907 ms  12.124 ms  14.428 ms
```

Tabelle 1. *Packet Responses*

State / Protocol	TCP	UDP	ICMP
OPEN	Host/Port SYN/ ACK; Host Service Response	Host Service Response;	Host ICMP packet response; Host Service Response
CLOSED	Host RST;	Host ICMP T03C03;	Host ICMP T03C03;
FILTERED	Any ICMP T03C09,10,13; Any RST	Any ICMP T03C09,10,13; Any ICMP T03C00,01,02	Any ICMP T03C00,01,02;
WILD	Any ICMP T11C0, T09C0, T03C04, T03C05; Host Netbios Hostname Req.	Any ICMP T11C0, T09C0, T03C04, T03C05; Any ICMP T04C0	Any ICMP T11C0, T09C0, T03C02, T03C04, T03C05;

und Client (Browser) abgefangen und modifiziert werden können. *paros* bietet aber auch weiterführende Funktionen wie einen Spider, der die Struktur des Webservers respektive der darauf befindlichen Webseite ermittelt.

Web-Applikationen können auch mittels Fuzzers (= Brute Force Tools, welche das Zielsystem auf Datei- oder Netzwerkebene mit diversen Strings beliefern um via Trial-and-Error Schwachstellen aufzudecken) getestet werden.

Datenbankgestützte Applikationen sollten auf die Anfälligkeit auf SQL Injection (= Einspeisung von SQL-Kommandos via Datenerfassungsmasken) oder generelle Injection überprüft werden. Cookies und das Session Handling sollten ebenfalls geprüft werden.

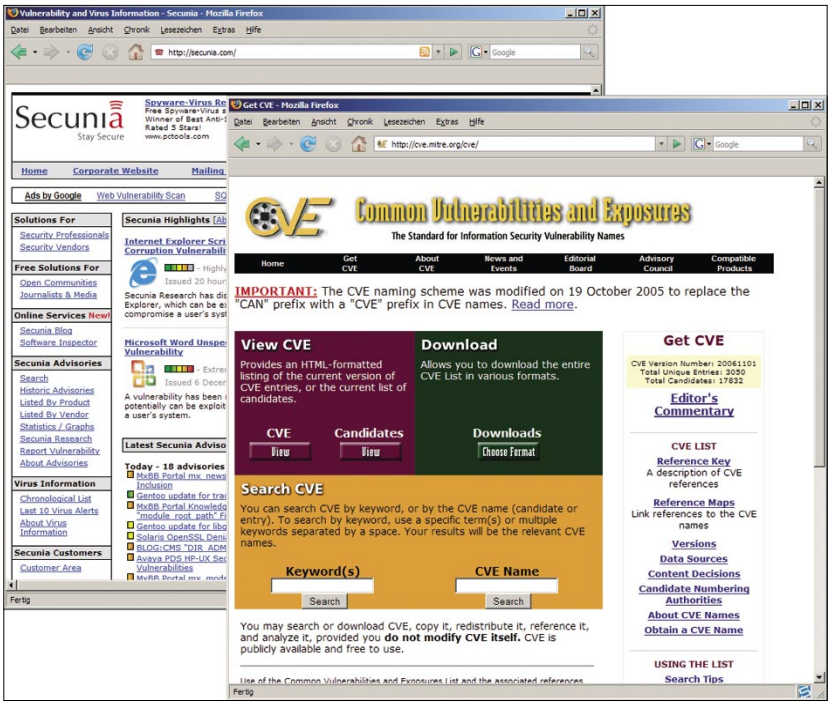


Abbildung 6. *Manuelle Recherche zu bekannten Schwachstellen und Verwundbarkeiten*

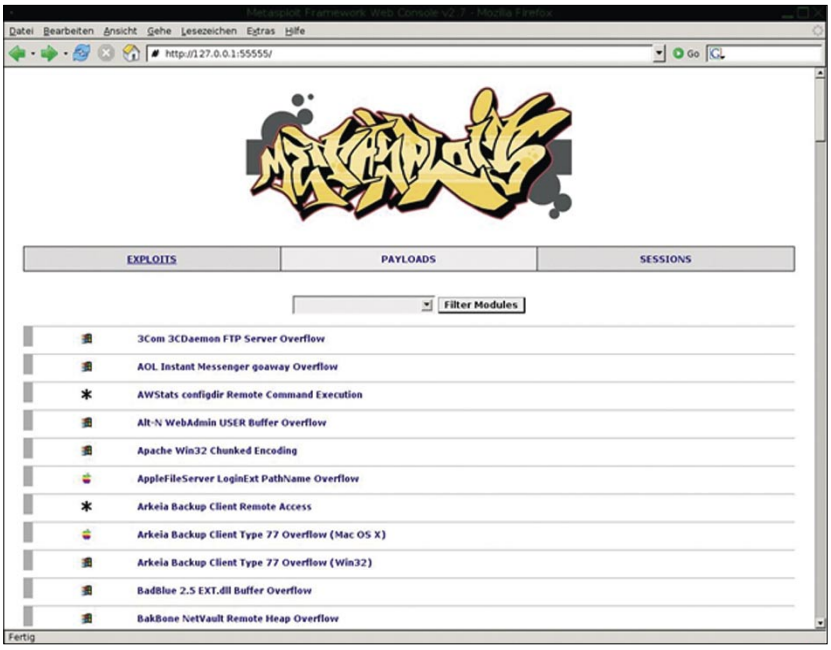


Abbildung 7. *metasploit bietet auch ein Web-Interface*

Router Testing (Modul 7)

Der Border-Router beschränkt manchmal den Netzwerkverkehr zwischen Internet und dem internen Unternehmensnetz. In diesem Modul wird überprüft, ob die Einstellungen der ACLs (Access Control Lists) derart konfiguriert sind, dass nur regulärer Traffic zwischen den (beiden) involvierten Zonen zugelassen wird. Dazu gehören auch DoS-Tests (siehe Modul 13).

Mittels Tools wie *yersinia* oder *ettercap* kann die Anfälligkeit des Untersuchungsobjekts auf Man-in-the-Middle-Attacken und Routing-Angriffe überprüft werden. Der Einsatz derartiger Tools ist nicht sinnvoll bei einem Untersuchungsobjekt, welches Remote getestet werden soll (Layer 2 des OSI-Referenzmodells ist nur im gleichen Subnet ansprechbar).

Bei einem Vor-Ort-Test im LAN können diese Tools jedoch wertvolle Arbeit leisten. Eine Toolalternative ist irpas.

Trusted Systems Testing (Modul 8)

Hierbei wird überprüft, ob Systeme einander ohne vorgängige Authentisierung vertrauen. Dabei werden Systemnamen, IP- oder MAC-Adressen beispielsweise mittels Source Routing gespooft. Wenn das Untersuchungsobjekt dann mit den gespooften Systemen bereitwillig interagiert, ist die Anfälligkeit nachgewiesen.

Für derartige Tests können beispielsweise mit *nmap* ausgeführte IDLE-Scans oder die IP Spoofing-Funktionen von *unicornscan* genutzt werden, indem interne IP-Adressen als Absender vorgetäuscht werden, um zu prüfen, ob sich die getesteten Systeme dadurch täuschen lassen.

Firewall Testing (Modul 9)

In diesem Abschnitt wird die Firewall überprüft. Dies umfasst das Austesten der Erreichbarkeit der DMZ und das Testen der Regeln der Firewall.

Beim Firewalking wird überprüft, ob die Regeln der Firewall es zulassen, dass mit dem dahinter

Listing 6. *Port Scan & Service Identification (TCP & UDP) mit nmap*

```
# nmap -sSU -P0 -nA -vv -p 21-23,25,53,80,110,137,161,443 www.oneconsult.com
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2006-12-14 17:41 MET
Warning: Hostname www.oneconsult.com resolves to 2 IPs. Using 195.129.94.193.
Initiating SYN Stealth Scan against 195.129.94.193 [10 ports] at 17:41
Discovered open port 80/tcp on 195.129.94.193
The SYN Stealth Scan took 1.82s to scan 10 total ports.
Initiating UDP Scan against 195.129.94.193 [10 ports] at 17:41
The UDP Scan took 2.05s to scan 10 total ports.
Initiating service scan against 11 services on 195.129.94.193 at 17:41
Service scan Timing: About 36.36% done; ETC: 17:43 (0:01:28 remaining)
The service scan took 55.77s to scan 11 services on 1 host.
Warning:  OS detection will be MUCH less reliable because we did not find at
                    least 1 open and 1 closed TCP port
For OSScan assuming port 80 is open, 30346 is closed, and neither are firewalled
For OSScan assuming port 80 is open, 33677 is closed, and neither are firewalled
For OSScan assuming port 80 is open, 42372 is closed, and neither are firewalled
Host 195.129.94.193 appears to be up ... good.
Interesting ports on 195.129.94.193:
PORT    STATE    SERVICE    VERSION
21/tcp  filtered   ftp
22/tcp  filtered   ssh
23/tcp  filtered   telnet
25/tcp  filtered   smtp
53/tcp  filtered   domain
80/tcp  open    http    Apache httpd 1.3.33 ((Unix) PHP/4.3.10
110/tcp filtered   pop3
137/tcp filtered   netbios-ns
161/tcp filtered   snmp
443/tcp filtered   https
21/udp  open|filtered ftp
[…]
443/udp open|filtered https
Device type: general purpose|broadband router|router
Running (JUST GUESSING) : Linux 2.4.X|2.6.X|2.5.X (97%), D-Link embedded
                    (93%), Siemens embedded (90%), Cisco IOS 12.X (90%),
                    Conexant embedded (90%), FreeSCO Linux 2.0.X (90%),
                    Apple Mac OS 9.X (88%), HP HP-UX 11.X (88%)
Aggressive OS guesses: Linux 2.4.16 - 2.4.18 (97%), Linux 2.4.18 - 2.4.21
                    (x86) (97%), Linux 2.6.0-test5 x86 (94%), Linux kernel
                    2.6.5 - 2.6.8 (94%), Linux 2.4.0 - 2.5.20 (93%),
                    Linux 2.4.18 - 2.4.20 (93%), Linux 2.4.26 (93%), Linux
                    2.4.27 or D-Link DSL-500T (running linux 2.4) (93%),
                    Siemens Speedstream 2602 DSL/Cable router (90%), Cisco
                    2620 router running IOS 12.2(15) (90%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SInfo(V=4.11%P=i686-pc-linux-gnu%D=12/14%Tm=45817EFC%O=80%C=-1)
TSeq(Class=RI%gcd=1%SI=255D63%IPID=Z%TS=100HZ)
TSeq(Class=RI%gcd=1%SI=2559D0%IPID=Z%TS=100HZ)
TSeq(Class=RI%gcd=1%SI=65C83B%IPID=Z)
T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T2(Resp=Y%DF=Y%W=0%ACK=S%Flags=AR%Ops=)
T3(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T4(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=N)
T6(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=Y%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=N)

TCP Sequence Prediction: Class=random positive increments
   Difficulty=6670395 (Good luck!)
IPID Sequence Generation: All zeros

Nmap finished: 1 IP address (1 host up) scanned in 76.335 seconds
```

liegenden Zielsystem kommuniziert respektive dessen Existenz festgestellt werden kann ohne das mit dem Zielsystem in der DMZ interagiert werden muss. Zu diesem Zweck wird die Time-to-live (TTL) so gesetzt, dass auf der Firewall die TTL noch 1 beträgt und das Paket somit auf dem nächsten Hop (oft das eigentliche Zielsystem in der DMZ) verfällt. Im folgenden Beispiel ist ersichtlich, dass auf dem Zielhost der offene Port 80 erkannt wurde.

Weitere Tools für Firewall-Tests:

- *hping*;
- *ftester.*

ftester ermöglicht mittels einem in PERL implementierten Client-Server-Prinzip, die einzelnen Regeln der Firewall auszuloten. Das Tool schickt Traffic durch die Firewall und schliesst aufgrund der durchgekommenen Pakete auf die implementierten Regeln der Firewall.

Eine eventuelle Anfälligkeit der Firewall auf Loose Source Routing kann beispielsweise mittels des Tools lsrscan überprüft werden.

Intrusion Detection System Testing (Modul 10)

In diesem Modul werden mögliche IDS (Intrusion Detection Systeme) *und/oder* IPS (Intrusion Prevention Systeme) gesucht und untersucht.

Das Tool *http-ips-detect* sucht nach einem *IDS/IPS*, indem es spezialisierte Strings versendet und so versucht, das *IDS/IPS* zu einer Reaktion zu bewegen. *mutate2* kann verwendet werden, um mittels Encoding-Tricks und anderer Methoden Content am *IDS/IPS* vorbeizuschleusen. *fragrouter* versucht dies mittels konfigurierbarer Fragmentierung. Mit den Tools *stick* und *snot* können Rulesets von *snort* verwendet werden, um die Funktionstüchtigkeit des *IDS/IPS* zu verifizieren. Dazu werden die gespooften versendeten snort-Rules mit den aufgetretenen Alarmen in den IDS-Protokollen verglichen.

Containment Measures Testing (Modul 11)

Dieses Unterkapitel beschäftigt sich mit den Eindämmungsmassnahmen des Systemkomplexes Firewall, Mailsystem und Virenschutz. Dabei wird Anfälligkeit auf potentiell gefährliche Dateiendungen (SAP 27), verschiedene Archivtypen inklusive Archivbomben und digitales Ungeziefer wie Viren, Würmer und Trojaner überprüft. Selbstverständlich wird dabei das Untersuchungsobjekt nicht infiziert, es reicht vollends, wenn anhand der Logfiles (Firewall, Antiviren-System und Mailserver) und der Attachment-Namen beim Mailempfänger erkannt wird, welche (bösartigen) Attachments ungehindert den Empfänger erreicht haben. Zu diesem Zweck ist es sinnvoll, für die Dauer der Tests zwei dedizierte interne Mailaccounts nutzen zu können, um sicherzustellen, dass niemand die Testmails unbeabsichtigt öffnet und damit eine Kontamination mit Malware riskiert.

Listing 7. *Port Scan (TCP & UDP) mit unicornscan*

```
# unicornscan -i eth0 www.oneconsult.com:q -pr 100 -p
Added     195.129.94.193 port 80 ttl 57
Open    http[    80]    From 195.129.94.193    ttl 57
# unicornscan -mU -i eth0 www.oneconsult.com:q -pr 100 -p
```

Listing 8. *Service Identification (TCP & UDP) mit amap*

```
# amap -H -v www.oneconsult.com 80
Using trigger file /usr/share/amap/appdefs.trig ... loaded 30 triggers
Using response file /usr/share/amap/appdefs.resp ... loaded 346 responses
Using trigger file /usr/share/amap/appdefs.rpc ... loaded 450 triggers
amap v5.2 (www.thc.org/thc-amap) started at 2006-12-14 14:49:00 - MAPPING
                        mode
Total amount of tasks to perform in plain connect mode: 10
Waiting for timeout on 10 connections ...
Protocol on 195.129.94.193:80/tcp (by trigger http) matches http
Protocol on 195.129.94.193:80/tcp (by trigger http) matches http-apache-1
Protocol on 195.129.94.193:80/tcp (by trigger http) matches http-apache-2
Protocol on 195.129.94.193:80/tcp (by trigger webmin) matches webmin
Unidentified ports: none.
amap v5.2 finished at 2006-12-14 14:49:06
```

Listing 9. *Protocol Scan mit nmap*

```
# nmap -sO -P0 www.oneconsult.com
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2006-12-14 14:05 CET
Warning: Hostname www.oneconsult.com resolves to 2 IPs. Using 195.129.94.193.
Interesting protocols on 195.129.94.193:
Not shown: 255 open|filtered protocols
PROTOCOL STATE    SERVICE
17   filtered udp
Nmap finished: 1 IP address (1 host up) scanned in 52.869 seconds
```

Listing 10. *OS Detection mit xprobe2*

```
# xprobe2 -p tcp:80:open www.oneconsult.com
Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com,
meder@o0o.nu
[+] Target is www.oneconsult.com
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[…]
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 195.129.94.129 Running OS: "Linux Kernel 2.6.3" (Guess probability:
96%)
[+] Other guesses:
[+] Host 195.129.94.129 Running OS: "Linux Kernel 2.4.20" (Guess
probability: 96%)
[…]
[+] Host 195.129.94.129 Running OS: "Linux Kernel 2.6.3" (Guess probability:
96%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

Password Cracking (Modul 12)

Mittels Passwort Cracking wird die Stärke von Passwörtern ganz pragmatisch ermittelt. Dies kann entweder via Wörterlisten (Dictionary, Durchprobieren von thematischen Wortlisten als Passwort), systematischem Pröbeln (Bruteforce: sämtliche möglichen Kombinationen von Zeichen durchprobieren) oder sogenannten *Regenbogentabellen* (Rainbow Tables, Nachschauen von Passwörtern und Teilen davon in Hashtabellen) geschehen. Derartige Mechanismen dienen in diesem Kontext dem Nachweis der Tauglichkeit der technischen Massnahmen zur Erzwingung von bestimmten Anforderungen an die Wahl oder Generierung von Passwörtern mittels Systemvorgaben.

Die Tools *ophcrack* (Windows Passwörter) und *john* (Unix- und Windows-Passwörter) sind gut für derartige Aufgaben geeignet.

Denial of Service Testing (Modul 13)

DoS-Test sind besonders heikel, weil sie im Sinne eines Proof-of-Concept bei Erfolg die Verfügbarkeit des Zielsystems massgeblich einschränken, beziehungsweise gänzlich unterbinden. Aus diesem Grund fordert das OSSTMM, dass DoS-Tests generell

Listing 11. *System Uptime Check mit hping2*

```
# hping -S -p 80 --tcp-timestamp www.oneconsult.com
HPING www.oneconsult.com (eth0 195.129.94.193): S set, 40 headers + 0 data
bytes
len=56 ip=195.129.94.193 ttl=58 DF id=0 sport=80 flags=SA seq=0 win=5792
rtt=11.9 ms
 TCP timestamp: tcpts=14373635
len=56 ip=195.129.94.193 ttl=58 DF id=0 sport=80 flags=SA seq=1 win=5792
rtt=15.9 ms
 TCP timestamp: tcpts=14373741
 HZ seems hz=100
 System uptime seems: 1 days, 15 hours, 55 minutes, 37 seconds
 --- www.oneconsult.com hping statistic ---
3 packets tramitted, 2 packets received, 34% packet loss
round-trip min/avg/max = 11.9/13.9/15.9 ms
```

Listing 12. *Sicherheitslückenidentifikation mit nikto*

```
#  nikto -verbose -generic -host www.oneconsult.com
---------------------------------------------------------------------------
- Nikto 1.35/1.36   -   www.cirt.net
V: - Calling nmap:/usr/bin/nmap  -P0 -oG - -p 80 195.129.94.193
V: - Testing open ports for web servers
V: - Checking for HTTP on port 195.129.94.193:80
+ Target IP:   195.129.94.193
+ Target Hostname: www.oneconsult.com
+ Target Port:   80
+ Start Time:   Mon Dec  4 14:56:02 2006
---------------------------------------------------------------------------
+ Server: Apache/1.3.33 (Unix) PHP/4.3.10 FrontPage/5.0.2.2510
V: - Checking for CGI in: /cgi.cgi/ /cgi-bin/
V: - Server category identified as 'apache', if this is not correct please use
                    -g to force a generic scan.
V: - 4093 server checks loaded
+ /robots.txt - contains 3 'disallow' entries which should be manually viewed
                    (added to mutation file lists) (GET).
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ HTTP method 'TRACE' is typically only used for debugging. It should be
                    disabled. OSVDB-877.
...
```

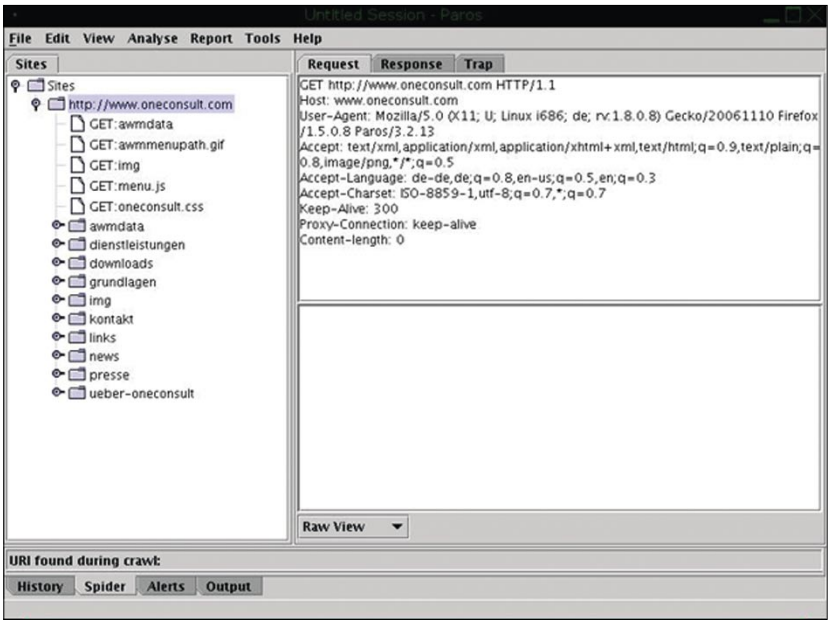


Abbildung 8. *Paros proxy*

nur vor-Ort, also direkt vor dem Untersuchungsobjekt ausgeführt werden. Andernfalls könnten die Knoten zwischen dem System des Testers und der zu testenden System unfreiwillig in Mitleidenschaft gezogen werden.

Für DoS-Tests eignen sich beispielsweise die Tools *datapool* und *spikesh4*.

Security Policy Review (Modul 14)

Dieses Modul befasst sich mit der Aufdeckung von Schwachstellen, Widersprüchen und Abweichungen zwischen definierter (= `geschriebener`) und umgesetzter Sicherheitspolicy. Dafür können sowohl technische Tools als auch konzeptionelle Methoden eingesetzt werden.

Hier endet Section C. Im folgenden Kapitel wird der Begriff und die Berechnung des Risk Assessment Value (RAV) erläutert.

RAV (Risk Assessment Value)-Berechnung

Bei anderen Methoden basiert das Risikomanagement auf dem Schätzen von Eintretenswahrscheinlichkeit und Schadenausmass – nicht so beim OSSTMM.

Der Risk Assessment Value (RAV) beschreibt das angetroffene Sicherheitsniveau in Form eines Zahlenwertes. Die Auswertung der Ergebnisse erfolgt mittels der zusammengetragenen Informationen und verifizierten Resultate, die in das von ISECOM kostenlos erhältliche RAV-Calculation-Sheet eingefüllt werden. An dieser Stelle wird das RAV-Modell 3.0 beschrieben:

Die *Visibility* bezeichnet die Anzahl IP-Adressen, welche während der Tests sichtbar waren. Unter *Access* wird das Total aller Zugriffpunkte eingetragen und bei *Trusts* die ersichtlichen Vertrauensstellungen zwischen den Systemen (*Web -> DNS zum Beispiel*). Die Schwachstellen werden als Risikotypen zusammengezählt: Vulnerability (Verwundbarkeit), Weakness (Schwäche), Concern (Bedenken), Information Leak (Informationsabfluss) und Anomaly (Anomalie). Dabei müssen mindestens

Listing 13. *Firewalking mit firewalk*

```
# firewalk -n -pTCP -s 80 -S 80 -t 1 -d 80 -T 100 212.71.100.18 195.129.94.193
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 80, destination port: 80
Hotfoot through 212.71.100.18 using 195.129.94.193 as a metric.
Ramping Phase:
 1 (TTL  1): expired [192.168.60.1]
 2 (TTL  2): expired [212.90.192.151]
 3 (TTL  3): expired [212.90.192.151]
 4 (TTL  4): expired [213.200.201.232]
 5 (TTL  5): expired [213.200.205.37]
 6 (TTL  6): expired [194.242.34.29]
 7 (TTL  7): expired [212.71.100.18]
Binding host reached.
Scan bound at 8 hops.
Scanning Phase:
port  80: A! open (port listen) [195.129.94.193]
Scan completed successfully.
Total packets sent:   8
Total packet errors:   0
Total packets caught   8
Total packets caught of interest   8
Total ports scanned   1
Total ports open:   1
Total ports unknown:   0
```

66% der identifizierten Schwachstellen verifiziert werden, um das Risiko der Bewertung von False Positives zu reduzieren. Anschliessend werden die zehn *Loss Controls* bewertet – wie viele Dienste des Untersuchungsobjektes verfügen über Mechanismen wie: Authentifizierung, Vertraulichkeit, Datenschutz, Alarmierung, etc.. Nach diesem Verfahren wird der RAV berechnet und kann danach als Massstab für das gemessene Sicherheitsniveau verwendet werden.

Weil der RAV keine Rückschlüsse auf das konkrete Untersuchungsobjekt zulässt, können die erzielten Werte mit anderen Projekten (eigene oder Projekte anderer Unternehmen) verglichen werden – ein echter Mehrwert!

Das Management kann den RAV als Kontrollinstrument nutzen und das Trending der gemessenen Sicherheit über die Zeit aufzeigen.

Zertifizierungsmöglichkeiten der ISECOM hinsichtlich OSSTMM

ISECOM bietet verschiedene Projekt-, Personen- und Anbieter-bezogene Zertifizierungsmöglichkeiten nach OSSTMM an: Projekbezogene Zertifizierungsmöglichkeit.

ISECOM bietet die Möglichkeit, Audits nach OSSTMM hinsichtlich ihrer OSSTMM-Konformität zu prüfen und bei Erfolg zu zertifizieren.

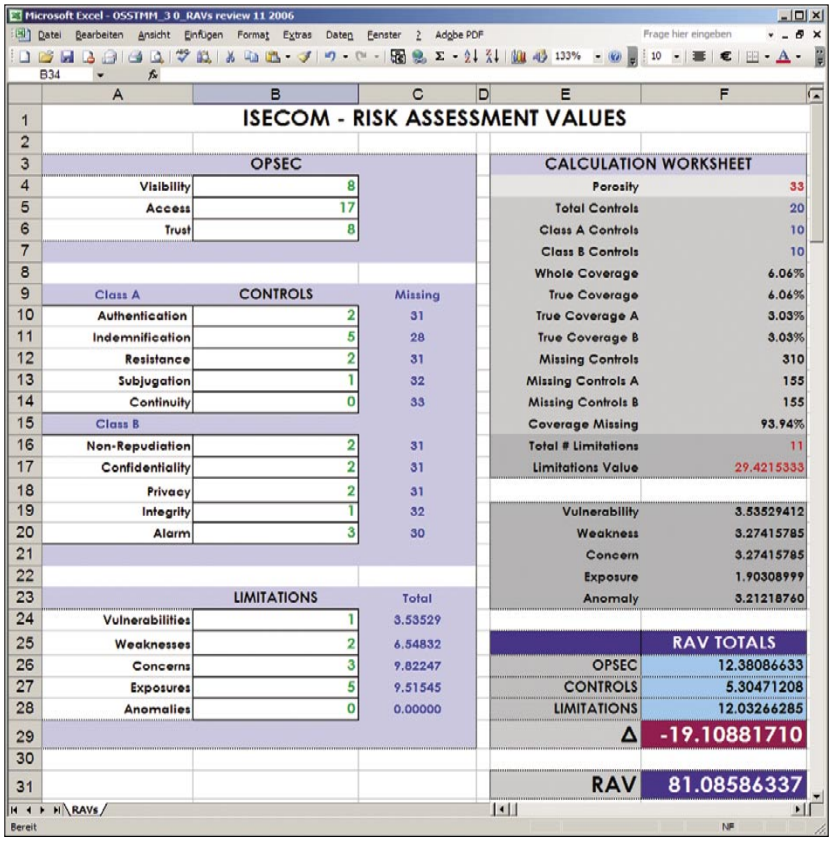


Abbildung 9. *RAV-Calculation Sheet*

Personenbezogene Zertifizierungsmöglichkeiten

ISECOM bietet verschiedene OSSTMM -spezifische Kurse mit anschliessender Zertifizierungsmöglichkeit an:

- *OPSE* (*OSSTMM Professional Security Expert*): belegt, dass der/die Zertifizierte genaue theoretische Kenntnisse des OSSTMMs und bezüglich Projektplanung hat;
- *OPST* (*OSSTMM Professional Security Tester*): belegt, dass der/die Zertifizierte über die nötigen Fähigkeiten verfügt, um als professioneller Security Tester nach OSSTMM zu arbeiten;
- *OWSE* (*OSSTMM Wireless Security Expert*): belegt, dass der/die Zertifizierte über die nötigen Fähigkeiten verfügt, um kabellose Netzwerke nach OSSTMM zu testen;
- *OPSA* (*OSSTMM Professional Security Analyst*): belegt, dass der/die Zertifizierte über die nötigen Fähigkeiten verfügt, Testresultate richtig zu interpretieren, den RAV zu berechnen und Testerteams zu koordinieren.

Über die Autoren

Christoph Baumgartner ist CEO und Inhaber der OneConsult GmbH. Seit 2002 auditiert er nach OSSTMM, ist zertifizierter OSSTMM Professional Security Tester (OPST) und Mitglied des ISECOM Core Teams. *http://www.oneconsult.com/*

Pete Herzog ist Managing Director und Gründungsmitglied des Institute for Security and Open Methodologies, Erfinder, Initialautor, Projektleiter und Herausgeber des OSSTMM. *http://www.isecom.org/*

Martin Rutishauser ist Senior Consultant und Branch Manager Bern bei der OneConsult GmbH. Er auditiert seit 2002 nach OSSTMM, ist zertifizierter OSSTMM Trainer, OSSTMM Professional Security Analyst (OPSA) sowie OSSTMM Professional Security Tester (OPST). *http://www.oneconsult.com/*

Listing 14. *IDS/IPS-Tests mit stick*

```
# ./stick -h
Usage: stick [sH ip_source] [sC ip_class_C_spoof] [sR start_spoof_ip end_
                      spoof_ip]
   [dH ip_target] [dC ip_class_C_target] [dR starttargetip end_target_ip]
 ------------------------------------------------------------------------
 defaults destination to 10.0.0.1 and source default is 0.0.0.0-255.255.255.255
 Software Design for limitted Stress Test capablity.
stick # ./stick
Stress Test - Source target is set to all 2^32 possiblities
Destination target value of: 100000a
 sending rule 391
 sending rule 185
 sending rule 947
 sending rule 707
 sending rule 841
...
```

Listing 15. *Password-Cracking mit john*

```
# john
John the Ripper password cracker, version 1.7.2
Copyright (c) 1996-2006 by Solar Designer and others
Homepage: http://www.openwall.com/john/
Usage: john [OPTIONS] [PASSWORD-FILES]
--single   "single crack" mode
--wordlist=FILE --stdin   wordlist mode, read words from FILE or stdin
--rules   enable word mangling rules for wordlist mode
--incremental[=MODE]   "incremental" mode [using section MODE]
--external=MODE   external mode or word filter
--stdout[=LENGTH]   just output candidate passwords [cut at LENGTH]
--restore[=NAME]   restore an interrupted session [called NAME]
--session=NAME   give a new session the NAME
--status[=NAME]   print status of a session [called NAME]
--make-charset=FILE   make a charset, FILE will be overwritten
--show   show cracked passwords
--test   perform a benchmark
--users=[-]LOGIN|UID[,..]   [do not] load this (these) user(s) only
--groups=[-]GID[,..]   load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]   load users with[out] this (these) shell(s) only
--salts=[-]COUNT   load salts with[out] at least COUNT passwords only
--format=NAME   force ciphertext format NAME: DES/BSDI/MD5/BF/AFS/LM/NT/PO/
                      raw-MD5/IPB2/raw-sha1/md5a/KRB5/bfegg/nsldap/MYSQL/
                      mscash/lotus5/DOMINOSEC
--save-memory=LEVEL   enable memory saving, at LEVEL 1..3
scripts # john /etc/shadow
Loaded 2 password hashes with 2 different salts (FreeBSD MD5 [32/32])
guesses: 0  time: 0:00:00:08 13% (2)  c/s: 4977  trying: alorap
Session aborted
```

Anbieterbezogene Zertifizierungsmöglichkeit

Anbieter (Unternehmen und Organisationen) können sich von ISECOM als *ISECOM Licensed Auditor (ILA)* auf verschiedenen Leveln zertifizieren lassen. Diese Zertifizierung ist als Qualitätssiegel für Interessenten und Kunden gedacht. Sie beinhaltet unter anderem regelmässige Audits durch ISECOM hinsichtlich der korrekten Anwendung des OSSTMM, eine bestimmte Anzahl Mitarbeiter mit aktuellen OPST-, OPSA-, OPSE- und weiteren ISECOM-Zertifizierungen, wobei die Mitarbeiter die Zertifizierungsprüfung mindestens mit dem Prädikat *Gut* abgeschlossen haben müssen.

Schlusswort

Das OSSTMM bietet eine Hilfestellung für die Durchführung und Dokumentation von gründlichen Sicherheitsüberprüfungen. Selbstverständlich kann man Security Audits auch nach einer selbst entwickelten Methode oder gänzlich ohne Methode durchführen. Selbstentwickelte Methoden bergen aber die Gefahr, dass Aspekte vergessen werden, ohne dass dies explizit im Bericht ersichtlich ist. Zusätzlich dazu stellt die Anwendung des OSSTMM sicher, dass die von verschiedenen Auditoren durchgeführten Tests und deren Resultate vergleichbar sind. Das OSSTMM wird weltweit in tausenden Projekten eingesetzt, kontinuierlich weiterentwickelt und bei Technologieänderungen angepasst/aktualisiert. Die Anwendung des OSSTMM bietet die einmalige Gelegenheit der Verknüpfung von strategischen Methoden wie SOx-404 und ISO/IEC 27001/17799 mit der operativen Sicherheit – die technische Messung von Sicherheit ist präziser als das Schätzen von Eintrittswahrscheinlichkeit x Schadenausmass in der klassischen Risikoanalyse. Die verschiedenen von ISECOM angebotenen Zertifizierungsmöglichkeiten nach OSSTMM ermöglichen Privatpersonen und Unternehmen sich ihre OSSTMM-bezogene Kompetenz attestieren zu lassen. ●