

Inhaltsverzeichnis

VORWORT	7
1 NMAP – DER EINSTIEG	9
1.1 Nmap in Betrieb nehmen	11
1.2 Erste Schritte mit Nmap	14
2 NMAP KENNENLERNEN	25
2.1 Ziele für Nmap	25
2.2 Host erkennen	29
2.2.1 List-Scan	30
2.2.2 Ping-Scan	31
2.2.3 TCP-ACK-Ping	32
2.2.4 UDP-Ping	33
2.2.5 ICMP-Ping-Arten	34
2.2.6 IP-Protokoll-Ping	34
2.2.7 ARP-Ping	35
2.2.8 Traceroute	35
2.2.9 DNS-Auflösung	35
2.3 Port-Scanning in der Praxis	36
2.4 Scan-Tutorial	39
2.5 Port-Scan-Techniken	44
2.5.1 TCP-SYN-Scan	45
2.5.2 TCP-Connect-Scan	46
2.5.3 UDP-Scan	46
2.5.4 TCP-NULL-, FIN- und Xmas-Scans	47
2.5.5 TCP-ACK-Scan	48

2.5.6	TCP-Window-Scan	48
2.5.7	TCP-Maimon-Scan	49
2.5.8	Benutzerdefinierter TCP-Scan	49
2.5.9	Idle-Scan	49
2.5.10	IP-Protokoll-Scan	50
2.5.11	FTP-Bounce-Scan	51
2.6	Port-Auswahl.....	52
3	ERMITTLERFUNKTIONEN	55
3.1	Services ermitteln.....	55
3.2	Betriebssystem ermitteln	59
4	AUSFÜHRUNG OPTIMIEREN.....	61
4.1	Bessere Performance.....	61
4.2	Firewall und IDS umgehen	65
4.3	Berichtsausgabe.....	68
5	NMAP IN DER PRAXIS	73
5.1	Webserver scannen	74
5.1.1	HTTP-Methoden	74
5.1.2	Offener Web-Proxy.....	75
5.1.3	Interessante Dateien und Verzeichnis aufdecken	76
5.1.4	Brute-Force-Attacke	78
5.1.5	Benutzer-Accounts auslesen	79
5.1.6	Zugangsdaten testen	80
5.1.7	Brute-Force-Attacke gegen WordPress	81
5.1.8	Brute-Force-Attacke gegen Joomla!	82
5.1.9	Web Application Firewall erkennen	83
5.1.10	Schwachstellen aufdecken	83

5.2 Test von Datenbanken.....	87
5.2.1 MySQL-Datenbanken abrufen	87
5.2.2 MySQL-Benutzer auslesen	88
5.2.3 MySQL-Variablen auslesen	88
5.2.4 Root-Account finden	89
5.2.5 Brute-Force-Attacke gegen MySQL	90
5.2.6 Unsichere MySQL-Konfigurationen	90
5.3 Mailserver im Visier.....	92
5.3.1 E-Mail-Accounts aufdecken	92
5.3.2 Offene Relays aufspüren	94
5.3.3 SMTP-Passwort knacken	94
5.3.4 SMTP-User auslesen	95
5.3.5 POP3-Server attackieren	95
5.3.6 IMAP-Server attackieren	96
6 MIT ZENMAP ARBEITEN	97
6.1 Scannen und auswerten	98
6.2 Netzwerktopologien	106
6.3 Der Profileditor	111
6.4 Erweiterte Zenmap-Funktionen.....	113
7 EIGENE TEST-SKRIPTS	115
7.1 Basics	115
7.2 Skript-Struktur.....	117
7.3 Skript-Kategorien	119
7.4 Gruß an die Welt!	121
7.5 Feinschliff	124

ANHANG A – MORE INFO.....	127
ANHANG B – EIGENE TESTUMGEBUNG	129
INDEX	131
WEITERE BRAIN-MEDIA.DE-BÜCHER	137
Weitere Titel in Vorbereitung	140
Plus+	140