

Aktive/Kreative IT-Sicherheit; Live-Hacking;
Penetration Szenarios; WLAN-Hacking
Ersteller: Norbert Nienhoff gt. Hornefeld
Quellen: Internet, Schulungswissen, Praxiswissen



Norbert Nienhoff
4MyIT gt. Hornefeld

Bitte Nutzen Sie das Wissen, dass Sie aus dieser Unterlage erlangen, nur zur Abwehr von Angriffen oder um Ihre System besser zu schützen!

Inhaltsverzeichnis/Orientierung:

Informationssicherheit.....	4
1. Installation und Konfiguration der Penetrations-Plattform.....	6
Grundsätzliches zu Ubuntu:	9
1.0.1 Installation der Tools.....	15
1.2.1 Metasploit Framework3	17
1.2.2 Fast-Track.....	17
1.2.3 Nessus Installation Version 4.2.0	17
Installation des Dienstes: dpkg -i Nessus-4.2.0-ubuntu910_i386.deb	17
Der Nessus-Client – z. B. Firefox → https://127.0.0.1:8834/	18
1.2.4 Installation von ettercap-gtk.....	18
1.2.5 Installation von aircrack-ng.....	18
1.2.6 Installation vom apache2-Webserver	18
1.3 Starten/Stoppen des Web-Servers – Apache.....	19
1.4 Starten/Stoppen des TFTP-Dienstes -- atftpd.....	19
2. Arbeiten mit NetCat	19
2.1 Mit NetCat eine Remote-Shell erzeugen.....	19
2.2 Mit NetCat einen Ports-Scan durchführen	21
2.3 Mit NetCat Dateien übers Netzwerk schicken/empfangen	21
2.4 Web-Server-Banner auslesen	22
3. „Informationsgewinnung“ im Netzwerk	22
3.1 Arbeiten mit Wireshark	22
3.2 Arbeiten mit nmap.....	23
3.3 Arbeiten mit Nessus	24
3.3.1 Vorgehen beim scannen eines Netzwerks mit Nessus 4.2.0	24
3.4 Arbeiten mit ettercap-gtk	30
3.4.1 ARP-Poisoning und Netzwerkverkehr mithören.....	31
3.4.2 DNS-Spoofing – DNS-Adressen nach belieben umleiten + Angriff	35
3.4.3 Content-Filter/Inhaltsfilter definieren	37

4. Erkannte Sicherheitslücken angreifen	39
4.1 Sicherheitslücke erkannt – was nun??.....	39
4.1.1 Grundsätzlicher Ablauf eines Angriffs	40
4.2 Funktionsweise von Exploits	41
4.3 Das Arbeiten mit dem Framework 3	41
4.3.1 Das arbeiten auf einem fremden System mit dem -- meterpreter.....	42
4.3.2 die msfconsole.....	45
4.3.3 das grafische Front-End -- msfweb	45
4.3.4 der vollautomatische Angriff mit fasttrack	47
4.3.5 Beispielangriff: Implementieren eines Keyloggers und eines „Connectors“	52
4.3.6 Ausbringen einer Anwendung die den „Weg nach Hause kennt“	54
5. Angriffe anonymisieren.....	55
5.1 der Relay-Agent -- rinetd	56
5.2 Aktionen anonymisieren mit Proxymittel.....	58
5.3 WEP-WLAN knacken.....	61
6. Abschlusswort	64

Abbildungsverzeichnis:

Abb. Installation 1 – Vmware-Player Installation.....	7
Abb. Installation 2 – Vmware-Player Installation.....	7
Abb. Installation 3 – Vmware-Player Installation.....	8
Abb. Installation 4 – Vmware-Player Installation – Bridged Network.....	8
Abb. Konfig. 1 – administrativ task	9
Abb. Konfig. 2 -- Netzwerkeinstellung	10
Abb. Konfig. 3 -- Netzwerkeinstellung	10
Abb. Konfig. 4 – Netzwerkeinstellung – Ip-Adresse eintragen	10
Abb. Konfig. 5 -- Netzwerkeinstellung	11
Abb. Konfig. 6 -- Netzwerkeinstellung	11
Abb. Konfig. 7 – Netzwerkeinstellung – ifconfig down/up	11
Abb. Konfig. 8 -- Spracheinstellungen.....	12
Abb. Konfig. 9 -- Spracheinstellungen.....	12
Abb. Konfig. 10 -- Spracheinstellungen.....	13
Abb. Konfig. 11 – Spracheinstellungen - LogOut	13
Abb. Konfig. 12 – Spracheinstellungen -Tastatur	13
Abb. Konfig. 13 – Spracheinstellungen -Tastatur	14
Abb. Konfig. 14 – Terminal in Panel	14
Abb. Konfig. 15 – Synaptic Paketverwaltung.....	14
Abb. Konfig. 16 – Synaptic Paketverwaltung.....	15
Abb. Installation /pentest.....	16
Abb. Installation Webserver.....	18
Abb. 1: nc-listen	20
Abb. 2 netstat.....	20
Abb. 3 netcat-Verbindung	20
Abb. 4 netcat-Connection.....	21
Abb. 5 netcat-Connection.....	21
Abb. 6 netstat-nessus	25
Abb. 7 nessus-Client - Firefox	25
Abb. 8 nessus-Client – Firefox.....	26
Abb. 9 nessus-Client – Firefox - Policy	26
Abb. 10 nessus-Client - Firefox - Plugins	27

Abb. 11 nessus-Client - Firefox – Scan einrichten.....	27
Abb. 12 nessus-Client - Firefox - Scan	28
Abb. 13 nessus-Client - Firefox - Scan	28
Abb. 14 nessus-Client - Firefox - Bericht	29
Abb. 15 nessus-Client - Firefox - Bericht	29
Abb. 16 nessus-Client - Firefox – Informationen zum BID.....	30
Abb. 17 ettercap	31
Abb. 18 ettercap	31
Abb. 19 ettercap	32
Abb. 20 ettercap	32
Abb. 21 – über Targets → Current Targets → kann man sich seine Auswahl anschauen.....	33
Abb. 22 ettercap-mitm.....	33
Abb. 23	33
Abb. 24 ettercap	33
Abb. 25 ettercap-SSL-Zertifikat.....	34
Abb. 26 ettercap-Auswertung	34
Abb. 27 msfcli-ettercap-Angriff.....	35
Abb. 28 ettercap-Angriff	36
Abb. 29 ettercap-Angriff	36
Abb. 30 ettercap-Angriff-netstat	36
Abb. 31 ettercap-Angriff-msfcli.....	37
Abb. 32 ettercap-Angriff-dns_spoof	38
Abb. 33 ettercap-Angriff-dns_spoof	38
Abb. 34 ettercap-Angriff-dns_spoof	38
Abb. 35 msfcli-meterpreter	42
Abb. 36 msfcli-meterpreter-netstat	42
Abb. 37 msfcli-meterpreter-help	43
Abb. 38 msfcli-meterpreter	43
Abb. 39 msfcli-meterpreter	44
Abb. 40 msfcli-meterpreter	44
Abb. 41 msfcli-meterpreter	44
Abb. 42 msfcli-meterpreter-execute.....	45
Abb. 43 msfweb	46
Abb. 44 msfweb	46
Abb. 45 msfweb	46
Abb. 46 msfweb	47
Abb. 47 msfweb-remoteshell	47
Abb. 48 fasttrack	48
Abb. 49 fasttrack	49
Abb. 50 fasttrack-mass-client-attack.....	50
Abb. 51 fasttrack-g	51
Abb. 52 fasttrack-g - RemoteShell.....	51
Abb. 53 Angriff mit dem meterpreter-registry.....	52
Abb. 54 Angriff mit dem meterpreter-registry.....	53
Abb. 55 Angriff mit dem meterpreter-RemoteShell	53
Abb. 56 Angriff mit dem meterpreter-Trojaner	54
Abb. 57 Opfer-Ansicht 1.9.56.3	57
Abb. 58 Relay-Ansicht – rinetd – 1.9.56.203	57
Abb. 59 Angreifer-Ansicht – meterpreter-Shell – 1.9.56.203	58
Abb. 60 NetCat-Shell auf Port 1025 ohne Proxytunnel.....	59
Abb. 61 Remoteverbindung	59

Abb. 62 NetCat-Shell auf Port 1025 mit Proxytunnel	60
Abb. 63 proxytunnel-Befehl.....	60
Abb. 64 Remoteverbindung	61
Abb. 65 FritzBox-Konfiguration WEP	61
Abb. 66 WEP-Parameter	62
Abb. 67 airodump-ng	63
Abb. 68 aircrack-ng.....	63

Praxisteile:

##### Praxisteil 1 – Installation #####	19
##### Praxisteil 2 NetCat #####	. 22
##### Praxisteil 3 – Informationen sammeln #####	39
##### Praxisteil 4 – Angreifen #####	55
##### Praxisteil 5 -- Angriffe anonymisieren#####	64