

Dieses Glossar ist generisch und dient in erster Linie als Anhang zu Projektberichten aus dem Bereich Penetrationstest und wird auch online auf www.secuvera.de zum Download zur Verfügung gestellt. Sollten Begrifflichkeiten nicht oder nicht ausreichend erklärt sein, bitten wir um kurze Mitteilung an Herrn Tobias Glemser (Kontaktmöglichkeiten über unsere Homepage www.secuvera.de)

Stand: 06.03.2018

Begriff	Erläuterung
3-Way-Handshake	Der Verbindungsaufbau einer standardmäßigen TCP-Verbindung. Hierbei werden keine Nutzdaten ausgetauscht, sondern lediglich die Kommunikation über 3 Wege initialisiert. Der Initiator sendet ein SYN-Paket, welches vom Empfänger im Falle einer Verbindung auf einen offenen Port mit einem SYN-ACK beantwortet wird. Dies quittiert wiederum der Initiator mit einem ACK-Paket. Damit ist die Verbindung aufgebaut und es kann mit der eigentlichen Kommunikation begonnen werden.
802.11i	IEEE Standard, der weitestgehend WPA2 entspricht
802.1x	Framework zur Authentifizierung von Netzgeräten (z. B. 802.1x EAP-TLS)
Acunetix Scanner	Kommerzieller Web-Vulnerability-Scanner (www.acunetix.com)
Address Resolution Protocol	Das Address Resolution Protocol (ARP) dient zur Auflösung von IP-Adressen (logischer Bezeichner) zu MAC-Adressen
AFRINIC	AFRINIC (African Network Information Centre): Funktion analog RIPE
Angriffsvektor	Der Angriffsvektor setzt sich zusammen aus dem Angriffsweg und der Angriffstechnik.
AP	Abkürzung für Access-Point
APNIC	APNIC (Asia Pacific Network Information Centre): Funktion analog RIPE
aircrack/aircrack-ng	Toolkit zum Auditieren eigener WLAN-Netze auf Schwachstellen. Beinhaltet u. a. Sniffer-Funktionen (www.aircrack-ng.org)
ARIN	ARIN (American Registry For Internet Numbers): Funktion analog RIPE
ARP	siehe <i>Address Resolution Protocol</i>
ARP-Cache	Lokale Tabelle eines Systems (Gültigkeit meist 2 Minuten), die die Daten von <i>IP-Adressen</i> zu <i>MAC-Adressen</i> enthält, welche per <i>ARP</i> erhalten wurden.
ARP-Poisoning	Methode, die mittels Versenden unaufgeforderter <i>ARP</i> -Requests den <i>ARP-Cache</i> von Systemen ändert und so z. B. <i>Man-in-the-Middle</i> Attacken im geschwichten, nicht weiter geschützten <i>LAN</i> ermöglicht.
Backdoor	Eine vom Software-Hersteller eingebaute Hintertür, die diesem ermöglicht, Systeminformationen auszulesen oder Remote-Zugriffe auf das System zu erhalten.
Banner-Grabbing	Viele Server-Anwendungen geben beim initialen erfolgreichen Verbindungsaufbau eine Meldung aus. Insbesondere Web-Server zeigen sich hier häufig auskunftsfreudig. Diese Informationen lassen sich zur Einschränkung von Testszenarien und Abstimmung der Prüfungen auf das Zielsystem nutzen.
BlackBox-Test	Penetrationstest ohne Kenntnisse der zu prüfenden Umgebung, z. B. nur mit Kenntnis der IP-Adresse eines Zielsystems. Diese Angriffsform versucht die Sichtweise eines externen Angreifers ohne Kenntnisse interner Strukturen einzunehmen.

Begriff	Erläuterung
Brute-Force Passwort-Audit	<i>Online:</i> Überprüfung von Passwörtern, bei der definierte Kombinationen aus Buchstaben, Zahlen und Sonderzeichen bei der Anmeldung an das jeweilige System durchprobiert werden, z. B. Webseiten oder Server. <i>Offline:</i> Überprüfung von Passwörtern, bei der definierte Kombinationen aus Buchstaben, Zahlen und Sonderzeichen mittels des gleichen Algorithmus gehashed werden, wie beim zu knackenden Passwort. Das Ergebnis wird mit dem zu knackenden Hash verglichen und sofern diese übereinstimmen, hat man das Passwort geknackt.
BSI	siehe <i>Bundesamt für Sicherheit in der Informationstechnik</i>
BSSID	Basic Service Set Identifier, nach 802.11. Gibt die per Definition eindeutige <i>MAC-Adresse</i> eines Access-Points im WLAN an. Ermöglicht die Unterscheidung zwischen APs mit identischer <i>ESSID</i> .
Buffer Overflow	Exploit, der Schadcode (Payload) mittels eines Puffer-Überlaufs einbringt
Bundesamt für Sicherheit in der Informationstechnik	Zentraler IT-Sicherheitsdienstleister des Bundes, Herausgeber der <i>IT-Grundschutzkataloge</i> , Zertifizierungsstelle (www.bsi.de)
Burp/Burp Pro	Prüfwerkzeug mit automatisierten und halb-automatisierten Methoden zur Prüfung von Webanwendungen (http://www.portswigger.net/burp/editions.html)
CA	siehe <i>Certification Authority</i>
CAPTCHA	CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) werden eingesetzt, um automatisierte Angriffe, z. B. auf Login-Funktionen zu verhindern. Dabei wird der Benutzer aufgefordert einen angezeigten, optisch stark verfremdetem Text oder einen abgespielten verfremdeten Ton zu erkennen und das Gelesene bzw. Gehörte einzugeben. Nur im Falle einer Übereinstimmung wird Zugriff auf die Funktion gewährt.
Certification Authority (CA)	Eine Certification Authority (~Zertifizierungsstelle) ist eine Organisation, die digitale Zertifikate ausstellt. Hierfür betreibt die Organisation eine <i>PKI</i> , deren Bestandteil die CA ist.
Cipher Suite	Bezeichnet eine genaue Folge von Algorithmen, die zum Aufbau einer TLS-Verbindung für Schlüsselaustausch, Authentifizierung, Hashfunktion und Verschlüsselung genutzt werden.
CRLF injection//HTTP response splitting	HTTP-Header sind nach dem Schema "Schlüssel: Variable" aufgebaut. Sie werden durch CRLF (carriage return line feed, zu Deutsch Zeilenumbruch/Zeilenvorschub) getrennt. Mit Hilfe des HTTP-Response-Splitting können über eine gefälschte Variable z. B. eigene Header durch den Angreifer erzwungen werden. Diese werden in der Variable hinterlegt und dann vom Server ausgeliefert.
Cross-Site-Scripting (XSS)	Eine fehlerhafte Webapplikation kann ggf. durch fehlerhafte Überprüfung von Variablen missbraucht werden, um HTML und/oder Javascript-Code zu verarbeiten. Ein Angreifer kann so über einen Link oder eine Mitteilung in einem Forensystem potentielle Opfer der Schwachstelle auf die verwundbare Webapplikation locken, die dann den Code im Context der Webapplikation ausführt.
Connect-Scan	Im Gegensatz zum <i>SYN-Scan</i> erfolgt hier ein kompletter <i>3-Way-Handshake</i> , welcher auch in den Log-Dateien der meisten Systeme auftaucht.
Cowpatty	Recovery-Tool zur Wiederherstellung von <i>WPA/WPA2</i> -Schlüsseln.

Begriff	Erläuterung
Demilitarisierte Zone	Als Demilitarisierte Zone (DMZ) bezeichnet man im Allgemeinen einen geschützten Netzbereich, der sich zwischen 2 Netzen befindet. Klassischerweise trennt die DMZ das Internet vom LAN einer Organisation. In einer DMZ sind meist über das Internet erreichbare Server aufgestellt, z. B. Webserver.
Denial of Service (DoS)/distributed Denial of Service (DDoS)	Eine DoS-Attacke führt zur Nicht-Erreichbarkeit eines Systems oder eines Dienstes. DoS werden entweder durch entsprechende Exploits ausgelöst oder durch Überlastung der Systeme über viele Anfragen von vielen Systemen (distributed Denial-of-Service).
Digest-Authentication	Im Gegensatz zur Basic-Authentication wird bei dieser Form der Anmeldung das Passwort (und ggf. weitere schützenswerte Informationen) nicht im Klartext, sondern hashed übertragen. Der Hash wird hierbei über eine Kombination von Informationen gebildet, die definiert und beiden Parteien (Client und Server) bekannt sind. So kann jede Partei über diese Informationen (z. B. im einfachsten Fall Benutzername und Passwort) den Hash bilden. Dieser wird vom Client zum Server übertragen. Der Server kann nun den selbst erzeugten Hash mit dem übermittelten Hash abgleichen.
Directory-Browsing	Wenn bei einem Webserver in einem Verzeichnis keine sogenannte Index-Datei hinterlegt ist (die aufgerufen wird, wenn nur das Verzeichnis, jedoch kein Dateiname durch den Client angegeben wird), wird je nach Konfiguration der gesamte Verzeichnisinhalt dargestellt. Dieser beinhaltet ggf. Verweise auf temporäre- oder Sicherungs-Dateien mit sensitivem Inhalt, die ansonsten nicht oder nur sehr schwer eingesehen werden könnten.
DMZ	siehe <i>Demilitarisierte Zone</i>
Document Object Model	W3C-Standard. Schnittstellenspezifikation für Zugriffe auf XML- oder HTML-Dokumente, meist in Browsern verwendet.
DoS/DDoS	siehe <i>Denial of Service</i>
Domain-Name	siehe <i>Second-Level-Domain</i>
DOM	siehe <i>Document Object Model</i>
ESSID	Extended Service Set Identifier, konfigurierbarer Name eines WLAN-Netzes mit bis zu 32 Zeichen.
Ethereal	Tool für Sniffing und Protokollanalyse, wird als <i>Wireshark</i> weiterentwickelt
Exploit	Nutzt eine <i>Vulnerability</i> aus. Meist erscheinen Exploits kurz nach der Veröffentlichung einer Schwachstelle.
Extended Service Set Identifier	siehe <i>ESSID</i>
false negative	Eine <i>Vulnerability</i> ist vorhanden, wurde von einem Scanner jedoch nicht identifiziert.
false positive	Eine <i>Vulnerability</i> wurde von einem Scanner identifiziert, ist jedoch nicht vorhanden.
Fingerprinting	Methode zur Identifizierung von Art und Version eines Serverdienstes oder Betriebssystems. Häufig wird in den Headern einer Verbindung durch einen Serverdienst dessen Name und Version, z. B. Apache 2.28 für einen Apache-Webserver in Version 2.28 mitgesendet. Darüber hinaus gibt es weitere Methoden (z. B. Timing-Analyse) zur Identifizierung eines Serverdienstes bzw. des Betriebssystems.

Begriff	Erläuterung
First-Level-Domain	Die First-Level-Domain (auch Top-Level-Domain genannt) ist die höchste Ebene in der Namensauflösung. Die First-Level-Domain für Deutschland ist "de", für Frankreich "fr" usw. Es gibt auch länderunabhängige First-Level-Domains, z. B. "net" oder "org".
Friendly Access Points	Im Gegensatz zu einem Rogue Access Point ist dieser innerhalb eines Firmengeländes erreichbar, wird jedoch außerhalb betrieben und stellt damit kein Sicherheitsrisiko für das Unternehmen dar.
Full Qualified Domain Name	Ein Full Qualified Domain Name besteht aus der <i>First-Level-Domain</i> , der <i>Second-Level-Domain</i> und der <i>Third-Level-Domain</i> , also z. B. www.secuvera.de
FQDN	siehe <i>Full Qualified Domain Name</i>
Hash/Hash-Funktionen	Eine Hash-Funktion wird auch als Fingerprint bezeichnet. Ziel ist es, ähnlich wie bei der Identifikation einer Person über den Fingerabdruck, aus einer Information beliebiger Größe (z. B. einen langen Text) mittels eines standardisierten Verfahrens eine kürzere und damit leichter vergleichbare Information zu erzeugen. Hierbei soll aus der kürzeren Information nicht wieder auf die Inhalte der Ursprungsinformation geschlossen werden können, was ein Sicherheitsmerkmal des Hashing darstellt. So können gehashte Informationen unverschlüsselt über ein Netzwerk übertragen werden, ohne dass die Ursprungsinformationen damit exponiert werden.
Hybrid Passwort-Audit	Überprüfung von Passwörtern, die einen Wörterbuch Passwort-Audit mit einem Brute-Force Passwort-Audit kombiniert. Dabei werden Einträge aus dem Wörterbuch herangezogen und z. B. mit 2 randomisierten Buchstaben oder Zahlen ergänzt, so dass auch Passwörter wie "Helga12" mit vertretbarem Zeitaufwand gefunden werden können.
IPsec	IPsec ist eine Verschlüsselungsmethode, in der alle Informationen oberhalb IP (z. B. sämtliche Nutzdaten) zu verschlüsseln sind, unabhängig von der genutzten Applikation.
IT-Grundschutz-kataloge	Empfehlungen von Standard-Sicherheitsmaßnahmen für typische IT-Systeme, herausgegeben durch das <i>BSI</i> .
Kismet	Passiver Open-Source WLAN Scanner mit GPS Integration (www.kismetwireless.net)
L2TP	Tunnellösung bei der Nutzung von VPNs, allerdings ohne Verschlüsselungsfunktion. Zur Verschlüsselung der Verbindung kann auf andere Verfahren, wie z. B. IPsec, zurückgegriffen werden.
LACNIC	LACNIC (Latin American and Caribbean Internet Adresses Registry): Funktion analog RIPE
LAN	Local Area Network - lokales Datennetz (z. B. Firmennetze)
MAC-Adresse	Die MAC-Adresse (Media Access Control) ist per Definition weltweit einmalig und identifiziert ein Netzgerät auf Layer 2 Ebene (siehe <i>OSI-Modell</i>). Sie besteht aus einer 48 Bit großen hexadezimal geschriebenen Adresse, wobei die ersten 24 Bit eine Herstellerkennung enthalten, so dass aufgrund der MAC-Adresse der Hersteller des Netzgeräts (z. B. der Netzwerkkarte oder des Routers) ermittelt werden kann.
Malware	Oberbegriff über schädigende Software wie <i>Viren</i> , <i>Würmer</i> oder <i>Trojaner</i> .
Man-in-the-Middle (MitM)	Angriffsform, bei der man sich mittels <i>ARP-Poisoning</i> in die Lage versetzt, die Kommunikation zwischen 2 Kommunikationspartner zu <i>sniffen</i> .

Begriff	Erläuterung
Metasploit	OpenSource Toolkit mit Exploitdatenbank zur Ausnutzung von Buffer-Overflows und weiteren Exploits. (www.metasploit.com)
MitM	siehe <i>Man-in-the-Middle</i>
Network-Address-Translation	Wird auch als network Masquerading bezeichnet. Hierbei wird die Ziel- und/oder Quell-Adresse eines Pakets geändert um z. B. Computer eines privaten Netzwerks ohne Proxy über ein System mit dem Internet zu verbinden.
NAT	siehe <i>Network-Address-Translation</i>
nessus	Security-Scanner, der mittels <i>nessus-Plugins</i> Zielsysteme auf Schwachstellen prüft. Mittlerweile auch fähig andere Tools wie z. B. <i>nmap</i> anzusteuern.
nessus-Plugins	Jedes Plugin von <i>nessus</i> überprüft eine oder mehrere ähnliche Schwachstellen. Plugins sind in der Scriptsprache NASL geschriebene Mini-Programme.
Netblock	Bezeichnet einen IP-Adressbereich, der bei einer <i>RIR</i> registriert ist.
nmap	nmap ist seit Jahren der Portscanner schlechthin. Er bietet den höchsten Funktionsumfang und sehr verlässliche Ergebnisse.
Non-Exploitable	Eine <i>Schwachstelle</i> wurde von einem Scanner oder durch manuelle Verifikation festgestellt und ist auch prinzipiell vorhanden. Sie lässt sich jedoch praktisch nicht oder nur stark begrenzt ausnutzen.
N-Stealth	Kommerzieller <i>Web-Vulnerability-Scanner</i> (www.nstalker.com)
OSI-Modell	Das OSI-7-Schichten Modell ist ein Schichtenmodell zur Definition von Kommunikation von Systemen. Diese Schichten sind vereinheitlicht, standardisiert und ermöglichen interoperable Kommunikation zwischen Systemen.
Path-Traversal	Ein verwundbarer Webserver oder eine verwundbare Webapplikation mit entsprechender Funktion kann in diesem Fall dazu gebracht werden, Daten außerhalb des vorgesehenen Verzeichnisses auszulesen.
Payload	Programmcode, der bei der Nutzung eines Buffer-Overflows vom Zielsystem ausgeführt werden soll. Allgemein wird mit den Nutzdaten versucht einen Shellcode zu übertragen, um Zugriff auf das Zielsystem zu erhalten.
Penetrationstest	Im Allgemeinen: Sicherheitsüberprüfung einer IT-Umgebung ohne nähere Spezifikation der Tests
Phishing / Spear-Phishing	<i>Social Engineering</i> Angriff, bei dem Benutzer mittels einer glaubwürdigen Täuschung dazu gebracht werden sollen, sensible Informationen, z. B. Passwörter, an den Angreifer zu übermitteln. Ein typisches Beispiel sind E-Mails, die dazu auffordern Nutzerdaten zur Verifizierung auf einer verlinkten Homepage einzugeben, wobei E-Mail und Homepage vortäuschen zum Anbieter des Dienstes zu gehören. Sehr zielgerichtete Angriffe, z. B. auf Mitarbeiter eines Unternehmens oder einer bestimmten Abteilung, werden als Spear-Phishing bezeichnet.
PKI	siehe <i>Public Key Infrastructure</i>
Plain old Telephony Services (POTS)	Klassische Telefonie (Gegensatz zu VoIP)
Port	Bestandteil bei einer vollständigen Adressierung eines Server-Dienstes. Der Port identifiziert den am Server angesprochenen Dienst, z. B. Port 80 für einen Webserver.

Begriff	Erläuterung
Pre-Shared-Key (PSK)	Schlüssel bzw. Passwort, das vor der ersten Kommunikation dem Nutzer bzw. Endgerät mitgeteilt werden muss (auch Shared Secret genannt).
Probe-Requests	WLAN-Clients senden sogenannte Probe-Requests aus, um ihnen bekannte WLAN-Netze schneller zu finden bzw. ihnen bekannte Netze zu finden, bei denen der <i>SSID-Broadcast</i> abgeschaltet wurde.
Public Key Infrastructure (PKI)	Ein System, mit dem digitale Zertifikate erzeugt, verwaltet und geprüft werden können.
PSK	siehe <i>Pre-Shared-Key</i>
Rainbow-Tables Passwort-Audit	Überprüfung von Passwörtern mittels einer Datenbank, in der Hashwerte samt Klartext abgelegt sind. Damit lässt sich eine Brute-Force-Attacke einmal durchrechnen und nachher wie bei einem <i>Wörterbuch Passwort-Audit</i> verwenden.
Reverse-DNS-Lookup	Auflösen einer IP-Adresse zu einem FQDN.
RIPE	Die RIPE (Réseaux IP Européens) ist eine unabhängige, non-profit Organisation, die sich mit der Organisation und Reglementierung im Bereich IP-Netze in und um Europa befasst. In der Whols-Datenbank können zu einer IP-Adresse die entsprechenden registrierten Organisationen und Personen abgefragt werden.
RIR	Regional Internet Registries, bezeichnet die 5 Organisationen, die die Verteilung der öffentlichen IP-Adressen vornehmen. Dies sind <i>ARIN</i> , <i>APNIC</i> , <i>LACNIC</i> , <i>AFRINIC</i> und <i>RIPE</i>
Rogue Access-Point	Ein Access-Point, der nicht autorisiert an das Firmennetz angeschlossen wurde. Access-Points die im Empfangsbereich eines Firmengeländes liegen, jedoch definitiv außerhalb betrieben werden, werden auch <i>Friendly Access Points</i> genannt.
Round Trip Time (RTT)	Gibt in diesem Fall die Zeitspanne an (und die Häufigkeit), die ein System bei einem halb-offenen Verbindungsaufbau benötigt, um weitere Pakete zu senden (hilft zur Identifizierung des Betriebssystems).
RTT	siehe Round Trip Time
Salt	Bezeichnet eine beim Hashen von Passwörtern zusätzlich verwendete Information, um erfolgreiche <i>Rainbow-Tables Passwort Audits</i> zu verhindern. Wird als Salt der Benutzername verwendet, wird also ein Hash über den Benutzernamen und das Passwort in der Datenbank gespeichert. Damit ist als zusätzlicher Schutz gewährleistet, dass bei identischen Passwörtern verschiedener Nutzer die Passwort-Hashes unterschiedlich sind.
Schwachstelle	siehe Vulnerability
Security-Audit	Allgemeine Bezeichnung für eine Sicherheits-Überprüfung, die nicht ausschließlich technischer Natur sein muss (z. B. inkl. <i>Social Engineering</i>).
Second-Level-Domain	Die Second-Level-Domain (oder Domain-Name) bezeichnet den registrierfähigen Namen unterhalb einer <i>First-Level-Domain</i> . Man kann eine Second-Level-Domain für verschiedene <i>First-Level-Domains</i> registrieren, z. B. <i>secuvera.de</i> und <i>secuvera.com</i>
Sniffer	Programm, um Netzwerkverkehr auf einer Netzchnittstelle mitzuschneiden (sniffen) und auszuwerten.

Begriff	Erläuterung
Social Engineering	Ausnutzung der „Schwachstelle Mensch“. Dabei werden typisch menschliche Eigenschaft wie Gutgläubigkeit, Gutmütigkeit und Neugierde ausgenutzt, um an sensible Informationen oder Zugang zu Systemen zu gelangen. Typische Angriffe sind <i>Phishing</i> / <i>Spear-Fishing</i> oder das Verteilen infizierter Datenträger.
SPIT (SPAM over Internet Telephony)	SPIT sind unerwünschte Werbebotschaften per VoIP-Kommunikation. Relevant, wenn VoIP-Dienste direkt über das Internet angeboten werden.
Spoofing	Wörtlich: "Manipulation, reinlegend, Verschleierung". Meist vorgeben einer falschen Identität. Wenn Herr Meier sich als Herr Müller meldet, ist dies z. B. einfaches Spoofing.
SSID	Gebräuchliche Abkürzung für <i>ESSID</i> .
SSID-Broadcast	Häufige Einstellung in Funknetzen, bei der der Access-Point in regelmäßigen Abständen seine <i>SSID</i> sendet.
Stack-Fingerprinting	Beim Stack-Fingerprinting wird durch das Verhalten beim Senden ungültiger Anfragen der IP-Stack des angegriffenen Systems analysiert, um Rückschlüsse auf das Betriebssystem zuzulassen.
SYN-Scan	Scan auf TCP-Basis, auch "Stealth-Scan" genannt, da beim 3-Way-Handshake nie das finale ACK-Paket durch den Scanner gesendet wird und es nie zu einem vollständigen Verbindungsaufbau kommt. Dies wird von den meisten Systemen nicht geloggt.
SQL-Injection	Bei Angriff auf eine Webanwendung kann ggf. über ein Eingabeformular oder eine GET-Variable ein in der Webanwendung nach Übergabe der Variable aufgerufenes SQL-Statement verändert werden. Somit sind Zugriffe auf Tabellen mit sensiblen Inhalten möglich.
tajanas	Security-Scanner der secuvera zur automatisierten Prüfung von Systemen inkl. Reporting-Tools.
Third-Level-Domain	Eine Third-Level-Domain (oder Subdomain) gibt den Namen eines spezifischen Rechners unterhalb einer <i>Second-Level-Domain</i> an. Gebräuchlichster Name ist hierbei "www", weitere gebräuchliche Namen sind z. B. "mail" oder "test".
Time-To-Live	Parameter einer IP-Verbindung, der pro Netzwerkhop um den Wert 1 reduziert wird. So wird verhindert, dass ein Paket, das an ein nicht vorhandenes System gesendet wird, das Netzwerk dauerhaft belastet. Sobald ein System die TTL von 1 auf 0 reduziert, löscht dieses System das Paket.
TLD	siehe <i>Top-Level-Domain</i>
Toolgestützter Penetrationstest	Überprüfung von IT-Umgebungen unter Zuhilfenahme von Tools wie nmap und nessus bzw. anderen spezialisierteren Tools. Diese Überprüfungsform gibt einen ersten Aufschluss über das Sicherheitsniveau einer Umgebung, ist jedoch kein Ersatz für manuelle Methoden. Der toolgestützte Schritt wird gemeinhin als Vulnerability-Assessment (VA) bezeichnet.
Top-Level-Domain	siehe <i>First-Level-Domain</i>
Trojaner	Schadprogramm, das es einem Angreifer ermöglicht Informationen über das angegriffene System zu erhalten oder es gar fernzusteuern. Daher werden Trojaner auch gerne als Remote-Administration-Toolkit (RAT) bezeichnet.
TTL	siehe <i>Time-To-Live</i>
UDP-Scan	Scan auf UDP-Basis, ob ein Port erreichbar ist

Begriff	Erläuterung
URI	Uniform Resource Identifier, einem spezifischen Schema folgender Verweis, z. B. auf eine Datei auf einem Webserver in Form von https://www.secuvera.de/test/test.html
Version-Scan	<i>Connect-Scan</i> , der auf Basis von <i>Banner-Grabbing</i> und anderen Technologien versucht, den Dienst an einem Port möglichst genau zu identifizieren.
Virtual LAN (VLAN)	Methode, um Netze logisch voneinander zu trennen. Im Gegensatz zum Subnetting findet die Trennung auf Layer 2 des ISO/OSI Referenzmodells statt.
Virtual Private Network (VPN)	Netzarchitektur, in der an verschiedenen Standorten befindliche Systeme (meist) durch Verschlüsselung ein gemeinsames Netzwerk über eine unsichere Verbindung (z. B. Internet) etablieren. Klassischerweise wird dies von Heimarbeitern oder Außendienstmitarbeitern genutzt, um sich über das Internet in das Firmennetzwerk einzuwählen und so alle Dienste des internen Netzes zu nutzen.
Virus	Schadprogramm, das auf einem "infizierten" Computer Schadroutinen ausführt.
VLAN	siehe <i>Virtual LAN (VLAN)</i>
Voice over IP (VoIP)	Telefonie über IP-Dienste
VPN	siehe Virtual Private Network
VA	siehe <i>Vulnerability-Assessment</i>
Vulnerability	Bezeichnet eine Schwachstelle. Gemeint sind meist Software-Schwachstellen, die häufig durch einen <i>Exploit</i> tatsächlich ausgenutzt werden können. Es gibt jedoch weitere mögliche Schwachstellen, z. B. organisatorische oder im Bezug auf Gebäudesicherheit.
Vulnerability-Assessment	Ein Vulnerability-Assessment (VA) ist die Prüfung mit Hilfe von Tools wie z. B. Port- und Vulnerability-Scannern auf technische Schwachstellen. Nicht zu verwechseln mit einem Penetrationstest, der zwar auf einem VA fußt, jedoch deutlich über die Tool-Reports hinausgeht.
Vulnerability-Scanner	Ein Programm zur automatisierten Überprüfung bekannter <i>Vulnerabilities</i> eines Systems. Dies kann zum einen ein allgemeiner Scanner sein, der viele Dienste und Schwachstellen kennt, oder ein sehr spezialisiertes Programm, das für eine Anwendung (z. B. Webserver) geschrieben wurde und deutlich mehr spezialisierte Tests beinhaltet. Bekannte Vertreter sind z. B. <i>nessus</i> oder <i>n-stealth</i>
WAF	siehe <i>Webanwendungs-Firewall/Web Application Firewall</i>
WAN	Wide Area Network - Weitverkehrsdatennetz (z. B. das Internet)
Wardialing	Mittels speziellen Programmen werden Rufnummernkreise auf fälschlich aufgestellte Modems oder andere anwahlfähige Geräte durchsucht. Die Ergebnisse werden dann mit dem Rufnummernplan abgeglichen.
Wardriving	Bezeichnet das Umherfahren mit Laptop, WLAN-Karte (mit externer Antenne) und GPS-Maus zum Kartografieren von Gebieten bzgl. der WLAN-Versorgung. Wardriving an sich hat nichts mit Eindringen in fremde Netze zu tun, da nur passiv die Daten empfangen werden.
Warwalk	Bezeichnet einen zu Fuß durchgeführten <i>Wardrive</i> .
watobo	watobo ist ein Prüfwerkzeug zur semi-automatisierten Prüfung von Webanwendungen (http://sourceforge.net/projects/watobo/)

Begriff	Erläuterung
Webanwendungs-Firewall/Web Application Firewall	Technologie zum Schutz von Web-Anwendungen vor Angriffen. Die Anfragen eines Clients müssen eine WAF passieren, ebenso wie die Antworten. Damit gibt es verschiedene Einsatzgebiete, z. B. Schutz vor Angriffen im HTTP-Datenstrom, aber auch Veränderung der aufgerufenen Adressen.
Webscarab	OpenSource HTTP/HTTPS Proxy, um aktiv in Datenströme der genannten Protokolle eingreifen zu können. (http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)
WEP	Bezeichnet die Verschlüsselungsmethodik von WLAN-Geräten. Mittlerweile als sehr schwach erkannt und bietet daher nur noch sehr geringen Schutz, da definiert brechbar.
WhiteBox-Test	Penetrationstest mit detaillierteren Kenntnissen als bei einem <i>Black-Box</i> -Test. Je nachdem, welcher Angriffstyp (z. B. Mitarbeiter, Dienstleister, etc.) werden mehr oder weniger Information herausgegeben.
Wireshark	Tool für Sniffing und Protokollanalyse, für viele Plattformen verfügbar (www.wireshark.org)
Wörterbuch Passwort-Audit	Im Gegensatz zum <i>Brute-Force</i> Passwort-Audit werden hierbei ausschließlich Passwörter, die aus Wörterbüchern entstammen genutzt.
WPA/WPA2	Nachfolger von WEP. Zur Erhöhung der Sicherheit werden während einer Session dynamisch wechselnde Schlüssel genutzt. Zur Authentisierung kann entweder ein Pre-Shared-Key (PSK) oder Zertifikate genutzt werden.
Wurm	Schadprogramm, das einem Virus entspricht, sich jedoch selbst fortpflanzt. Die am häufigsten anzutreffenden Würmer verbreiten sich per eMail.
XML-Bombe	Dieser Angriff nutzt die Möglichkeit, einen XML-Parser durch viele Verweise zu überlasten.
XSS	Siehe <i>Cross-Site-Scripting</i>