Fach : IT-12	Thema : **Überblick - Angriffe**

Angriffe	Recherchieren Sie die Grundfunktion der folgenden Angriffe :
Backdoor	„Hintertür"; siehe auch TrapDoor; ist eine Software, in der Regel ein Server, der über einen bestimmten Port den Zugang zu einen System oder zu Daten
	ermöglicht; -> Fernzugriff auf das komplette System -> **Trojaner**; Software die die Zugriffssicherung umgeht
Brute-Force-Angriff	Über „brutales" Durchprobieren aller Zeichen wird z.B. ein Passwort oder ein Krypto-Schlüssel ermittelt
CSRF, cross site	Ein System wird dazu gebracht falsche HTTP-Requests zu stellen; damit wird ein Web-Browser veranlasst vom User unerwünschte Aktionen auszuführen
request forgery	-> Datenänderung mittels HTTP-Requests; auch als SessionRiding bekannt; die Web-Session eines unbewussten „Helfers" wird von einem Angreifer übernommen -> über diese Session wird ein drittes System angegriffen
Flaming	Oberflächliche, provokative Meinungsäußerungen um ernsthafte Diskussionen zu stören oder abzuwürgen
	Verstoß gegen die Netiquette in Foren und sollte unterbleiben bzw. sofort gelöscht werden – Cyber-Mobbing
Hijacking	Ist eine „gewaltsame" Übernahme einer Internetdomäne, eines Benutzerkontos bzw. einer Sitzung (Session-Hijacking), durch z.B. fälschen einer IP-
	Adresse mittels z.B. Spoofing; auch CSRF kann verwendet werden
Hoax	Ist kein Angriff, nur nervig sind z.B. Falschmeldungen per E-Mail, SMS, usw.
IP-Spoofing	Fälschen einer IP-Adresse um eine bestehende, authentifizierte Verbindung zu verwenden um z.B. trotz einer Firewall in ein System zu kommen
Nuke-Attacke	Ist eine DoS-Attacke (DenialOfService) bei der durch Versenden falscher ICMP-Pakete versucht wird ein System lahm zu legen bzw. zu überlasten
	Inzwischen veraltet, die meisten System reagieren nicht mehr auf derartige Attacken
Pharming	Weiterentwicklung vom Phishing; es werden Sitzungen auf falsche Webseiten umgeleitet; der DNS-Cache wird hier gefälscht, damit wird eine falsche IP-
	Zuordnung zu Webseiten-URLs erreicht. Ein User befindet sich auf einer gefälschten Webseite -> auch DNS-Cache Poisoning genannt
Phishing	Ist allgemein der Versuch an Benutzer-Daten heranzukommen durch z.B. Umleiten auf gefälschte Webseiten (Pharming), SocialEngineering (gefälschte
	E-Mails); das Ziel ist es an z.B. Zugang zu Bank-Accounts zu erhalten und damit Konten abzuräumen
Scareware	Software die Angst beim User erzeugen soll z.B. eine kostenfreie Virensoftware meldet einen Fehler der real nicht vorhanden ist; gegen Gebühr wird
	dann versprochen dieses Problem zu beseitigen; oder die Scareware verursacht einen Schaden der dann kostenpflichtig behoben werden muss
XSS, cross site	Ziel ist es an geschützte Daten des Users zu gelangen durch z.B. die Ausführung von Skript-Code in einer Webseite. Anfällig wenn Daten unverschlüsselt
scripting	Übertragen werden ohne Prüfung durch den Webbrowser, d.h. auch Benutzerdaten werden unverschlüsselt übertragen
TMTO, time	Angriff zum Identifizieren von Schlüsseln bei dem durch Ausprobieren von teilweise gespeicherten Begriffen die Schlüssel ermittelt werden;
memory trade-off	mathematisch optimiertes Testprogramm zum Aufdecken von Schlüsseln und Passwörtern
Skimming	Verschiedene Verfahren um Bank-Daten auf Kreditkarten oder EC-Karten aus zu lesen oder auch um Zugriff auch Bank-Konten zu erhalten; z.B. durch
	Anbringen falscher Lesegeräte, Montage von Überwachungskameras, usw.;
	Die Informationen der EC-Karten werden teilweise auf Blanko-Karten überspielt mit denen dann ebenfalls ein Banking möglich ist.

Fach : IT-12	Thema : **Überblick - Angriffe**

Scraping	Es werden unterschiedlichste User-Daten "zusammen gekratzt", d.h. gesammelt, für eine kommerzielle Auswertung und zum Verkauf, über z.B. Konsumverhalten, Status, Kaufkraft, für Versicherungen oder Arbeitgeber etc. Dazu werden z.B. falsche Foren mit Diskussionen über Gesundheitsfragen angelegt oder auch Daten aus sozialen Netzwerken
Snooping	Abhören von Daten in einem Netzwerk um z.B. Kennungen und Passwörter zu erhalten z.B. mittels eines Sniffers
Trap Door	Spezielles Back-Door bei dem, durch die Programmierer, Default-Passwörter oder Kennungen vergeben werden über die Zugriff auf ein System erlangt werden kann.
Sniffer	Mithören des gesamten Netzwerkverkehrs und Analyse der Daten-Pakete z.B. für eine Verkehrsflussanalyse oder Auffinden von Kennungen, Passwörter Zur Analyse können auch Filter eingesetzt werden; ein Tool in der Systemadministration um Fehler und Schwachstellen aufzudecken
Spyware	Dient zum Ausspionieren von PCs und auch zum Spionieren von Webbrowser History um Marktverhalten zu studieren und gezielt Werbung zu posten Zum Spionieren werden oft auch Trojaner verwendet die die Daten per E-Mail versenden.
Smurf-Attacke	Ist ebenfalls eine DoS Attacke die mittels ICMP Pakete versucht das attackierte System zu überlasten; -> ICMP Pakete als Broadcast an alle Systeme in einem Netz gesendet wobei als Absender die IP des Opfer-PCs eingetragen wurde

Angriffe	Finden und erläutern Sie noch weitere Angriffe aus dem Bereich IT-Sicherheit
Exploit	Allg. Schwachstelle eines Systems die durch einen Angreifer ausgenutzt werden kann; es werden z.B. Fehlfunktionen eines Programms ausgenutzt um Zugang zu einem System zu erhalten; vergleichbar mit der Brechstange eines Einbrechers
Shoulder Surfing	„Über die Schulter schauen" – Daten ausspionieren durch Beobachten von Usern
Java DriveBy	Java Exploit – Ausführung von Java-Angriffs-Code der im Web-Browser nicht sichtbar ist
Golden Ticket	Kerberos-Ticket – Authentifizierung von ActiveDirectory – Account; über ein GoldenTicket ist der Zugriff auf das ActiveDirectory über Jahre möglich Ist ein Kerberos-Authentifizierungstoken des KRBTGT-Kontos, eines besonderen, verborgenen Kontos
Man in the Middle	Ein Angreifer schaltet sich zwischen eine authentifizierte Verbindung; jedes Datenpaket läuft nicht direkt sondern über den „Main in the Middle" Die Datenpakete können damit beliebig verändert oder auch umgelenkt werden
Evasive Attack	Ist eine Technik um Angriffe und Angriffs-Muster zu verstecken. Die Angriffe können damit versteckt ablaufen und werden nicht entdeckt z.B. über Verschlüsselung oder Aufteilen der Angriff-Pakete in kleiner Einheiten -> damit können die Muster nicht entdeckt werden
RootKit	Software die Sicherheitslücken ausnutzt um als Administrator (root) Zugriff auf ein System zu erhalten
Ransomware	Nützt eine Sicherheitslücke, d.h. ein sog. Exploit (z.B. EternalBlue – SMB-Protokoll-Schwachstelle), um ein spezielles Backdoor zu installieren. Dieses Backdoor dient zur Verschlüsselung der Festplatte. Die Entschlüsselung erfolgt angeblich nach Zahlung eines bestimmten Betrags
Social Engineering	Über soziale Kontakte (E-Mails, Besucher, Bewerber usw.) werden sensible Informationen weiter gegeben; z.B. über CEO Betrug können falsche Überweisungen in Millionen-Höhe veranlasst werden