

Faszination Cybercrime

Das umfassende
Cybercrime & -security
Kompendium

Band 2

P bis Z

Klaus-Peter Baumdick

2024

Copyright: 2024

Klaus-Peter Baumdick
c/o COCENTER
Koppoldstr. 1
86551 Aichach

Text:

Libreoffice Writer 7.3.4.2

Coverdesign:

Klaus-Peter Baumdick

Grafik:

aitubo.ai

Erste Auflage

ISBN:

978-3-384-27243-0

Inhaltsverzeichnis

Pass-the-Hash-Angriff.....	9
Pass-the-Ticket-Angriff.....	12
Paros Proxy.....	15
PASTA.....	19
Patator.....	22
Patch-Management.....	24
Path Traversal.....	26
Payload.....	29
PCI-DSS.....	32
Penetrationstests.....	37
Pharming.....	39
Phishery.....	40
Phishing as a Service.....	43
Phishing.....	46
Physical Security.....	48
Pikabot.....	50
Ping Flood.....	52
Ping of Death.....	54
Policy Management.....	55
Port-Scanning.....	57
Powersploit.....	59
Privacy by default.....	61
Privacy by design.....	65
Privatsphäre.....	69
Privilege Escalation.....	71
Process Hollowing.....	72
Proxychains.....	79
Psiphon.....	82
Ptrace/Kmod Local Root Exploit.....	86
Quantenkryptographie.....	97
Quarantäne.....	99
Query Injection.....	101

Quick Response.....	103
Rafel RAT.....	108
R-U-Dead-Yet (RUDY).....	110
RainbowCrack.....	113
Ransomware.....	114
Ransomware Defense.....	116
Reaver.....	118
Recon-ng.....	120
Red Hat Hacker.....	125
Red Team Testing.....	126
Red Teams.....	128
Reflective DLL Injection.....	130
Regulatory Compliance.....	134
Remediation Strategies.....	138
Remote Access Security.....	140
Remote Access Tools (RATs).....	143
Remote Code Execution (RCE).....	144
Remote Thread Injection.....	146
Replay-Angriff.....	151
Responder.....	153
Reverse Engineering.....	156
RFID Hacking.....	159
Risk Management.....	160
Riviera Beach Ransomware Attack.....	162
Robert Tappan Morris.....	166
Ruler.....	167
Salzen.....	170
SAM-Dumping.....	172
SCADA.....	175
Schwachstellenanalyse.....	177
Script-Kiddies.....	180
Selenium.....	182
Server-Side Request Forgery (SSRF).....	186
Session Fixation.....	189

Session Hijacking.....	189
Shadow Brokers.....	189
ShadowHammer.....	190
Shamoon.....	194
Shellter.....	198
Shimming.....	201
Sicherheitsarchitektur.....	203
Sicherheitsaudit.....	206
Sicherheitsbedrohungen.....	209
Sicherheitsbewertung.....	211
Sicherheitslösungen.....	213
Sicherheitslücken.....	216
Sicherheitsmanagement.....	219
Sicherheitsmaßnahmen.....	221
Sicherheitsrichtlinien.....	224
Sicherheitsrisiken.....	226
Sicherheitsstrategien.....	229
Sicherheitsüberwachung.....	231
Side Channel Attack.....	234
Silent Librarian.....	236
Skimming.....	237
Slowloris.....	239
Smart Contract Bugs.....	242
Smishing.....	244
Smokeloder.....	246
Smurf-Attack.....	249
Sn1per.....	251
Snort.....	254
Social Credit System.....	258
Social Engineering.....	260
Social-Engineer Toolkit (SET).....	264
Software Supply Chain Compromise.....	267
SolarWinds-Hack.....	270
Sony Pictures Hack.....	273

Spam.....	275
Spear Phishing.....	277
SpiderFoot.....	279
Splunk.....	282
SQL Injection.....	284
Sqlmap.....	286
SQLninja.....	290
SSL-Strippen.....	295
Steganographie.....	297
Stoertebecker.....	302
StoneDrill.....	303
STP Angriff.....	307
STRIDE.....	309
Stuxnet.....	317
Sublist3r.....	318
Supply Chain Attacks.....	322
Suricata.....	324
Swift Banking Hack.....	328
Sybil-Angriff.....	330
SYN-Flood.....	332
Syrian Electronic Army (SEA).....	334
SystemBC.....	335
Tailgating.....	337
Target-Datenleck.....	339
Targeted Watering Hole Attack.....	341
tcpdump.....	344
Tesla Model S Hack.....	349
THC.....	350
THC-Amap.....	351
THC-Hydra.....	353
THC-SSL-DOS.....	353
The Dark Overlord.....	356
The Equation Group.....	357
The Onion Router.....	358

The Phrack Magazine.....	360
The Sleuth Kit (TSK).....	361
theHarvester.....	365
Threat Connect.....	368
Threat Hunting.....	370
Threat Intelligence.....	375
Threat Modeling.....	379
Tokenization.....	385
Tor-Netzwerk.....	389
Tor's Hammer.....	394
Transport Layer Security (TLS).....	396
Trickbot.....	400
Trojaner.....	403
Trufflehog.....	406
Two-Factor Authentication.....	410
Typosquatting.....	414
Überwachung und Intrusion Detection.....	416
UDP Flooding.....	422
Unerwünschte Software und Malware-Bekämpfung.....	424
Unified Threat Management.....	431
Unternehmenssicherheit und Risikomanagement.....	438
Upgrades und Patch-Management.....	444
Ursachenanalyse bei Sicherheitsvorfällen.....	451
USB HID Attack.....	457
USB-Drop-Angriff.....	459
USB-Sicherheit und Risiken.....	461
Use Case Analysen in der Cybersecurity.....	466
User Authentication (Benutzerauthentifizierung).....	470
Utah Data Center.....	477
V3B Phishing Kit.....	480
Veil-Evasion.....	483
Vendor Risk Management.....	487
Verschleierungstechniken.....	492
Virtual Private Network (VPN).....	492

Virtualization Security.....	500
Virus Detection.....	505
Vishing.....	515
VLAN Hopping.....	517
VOHO-Kampagne.....	520
Voice Biometrics.....	528
VPN Security (VPN-Sicherheit).....	535
Vulnerability Assessment.....	539
Vulnerability Disclosure.....	543
Vulnerability Management.....	549
Vulnerability Scanning.....	556
Vulnerability Scans.....	561
W3af.....	563
WAF.....	570
WannaCry.....	577
Wapiti.....	582
WARC-Format.....	586
Warcrawling.....	588
Wardialing.....	590
Wardriving.....	595
Watering Hole Attack.....	599
Web Application Security.....	605
Web Browser Security.....	612
Website-Defacements.....	621
Weevely.....	622
White Hat Hacker.....	626
White Hat Hacking.....	630
Wi-Fi Security.....	638
WiFi Pineapple.....	638
Wifiphisher.....	644
Wifite.....	651
Wiper Malware.....	658
Wireless Security.....	666
Wireshark.....	673

WPA/WPA2-Handshake-Angriff.....	681
WPA.....	682
Wpscan.....	690
WPSeku.....	697
Würmer.....	701
X.509-Zertifikate.....	707
Xerosploit.....	716
Xerxes.....	718
XML External Entity (XXE) Attack.....	722
XML Injection.....	724
XML-Sicherheit.....	727
XMRig.....	735
XOR-Verschlüsselung.....	739
XSRF.....	745
XSS.....	752
XSS Worm (Samy).....	758
XSSer.....	762
YAML-Sicherheit.....	766
YARA.....	772
Yersinia.....	779
Yield Protection.....	784
YubiKey.....	784
zANTI.....	790
zBang.....	793
Zeek.....	797
Zero-Click-Attacken.....	801
Zero-Day-Exploits.....	803
Zero-Day-Exploit.....	806
Zmap.....	810
Hilfreiche Links.....	814
Ahmia.....	814
Blogs von Sicherheitsunternehmen.....	814
Fake-Personen Generator.....	814
Exploit Database.....	815

News und Trends.....	815
Offizielle Webseiten und Organisationen.....	816
Sicherheitstools.....	816
Besondere Suchmaschinen.....	817
Cookiedatabase.....	817
Quick Referenz zu nmap.....	817
WiFi Datenbank.....	818
Hackertools.....	818
Tor-Browser.....	818
SpiderFoot.....	818
Quellen.....	818
Weitere namentlich bekannte Hacks.....	819

Pass-the-Hash-Angriff

Ein Pass-the-Hash (PtH)-Angriff ist eine Technik, die von Angreifern verwendet wird, um sich in einem Netzwerk zu bewegen und Zugang zu Ressourcen zu erlangen, ohne dass sie das Klartext-Passwort eines Benutzers kennen müssen. Stattdessen verwenden sie den kryptografischen Hash eines Passworts, um sich als der entsprechende Benutzer auszugeben. Dieser Angriff ist besonders relevant in Umgebungen, die auf Microsoft Windows basieren, da dort NTLM (NT LAN Manager) Authentifizierungsprotokolle verwendet werden, die anfällig für diese Art von Angriff sind.

Wie funktioniert ein Pass-the-Hash-Angriff?

1. Erfassen des Hashes:

- Der Angreifer muss zuerst den Hash des Passworts eines Benutzers erfassen. Dies kann durch verschiedene Methoden erfolgen, wie z.B.:
- Credential Dumping: Tools wie Mimikatz können verwendet werden, um Passwort-Hashes aus dem Speicher eines kompromittierten Systems zu extrahieren.
- MitM-Angriffe: Man-in-the-Middle-Angriffe oder andere Netzwerktechniken können genutzt werden, um Hashes während der Übertragung zu erfassen.

2. Verwenden des Hashes:

- Nachdem der Hash erfasst wurde, verwendet der Angreifer diesen Hash, um sich gegenüber anderen Systemen als der legitime Benutzer zu authentifizieren. Der Hash wird in den Authentifizierungsprozess eingespeist, als wäre es das eigentliche Passwort.

3. Bewegung im Netzwerk:

- Mit dem Hash kann der Angreifer auf verschiedene Ressourcen zugreifen, wie z.B. Dateien, Datenbanken und andere Systeme im Netzwerk, die denselben Hash zur Authentifizierung verwenden. Dieser Schritt wird oft als "laterale Bewegung" bezeichnet.

Beispiel eines Pass-the-Hash-Angriffs

1. Kompromittierung eines Workstations:

- Der Angreifer kompromittiert eine Workstation und führt ein Tool wie Mimikatz aus, um NTLM-Hashes aus dem Speicher zu extrahieren.

2. Extrahieren des Hashes:

- Der Angreifer extrahiert den Hash eines Administrator-Kontos oder eines anderen privilegierten Benutzers.

3. Benutzen des Hashes:

- Der Angreifer verwendet den erlangten Hash, um sich auf anderen Maschinen im Netzwerk als dieser Benutzer zu authentifizieren, ohne das tatsächliche Passwort zu kennen.

4. Zugriff auf Ressourcen:

- Der Angreifer bewegt sich lateral durch das Netzwerk, greift auf sensible Daten zu oder führt weitere Angriffe durch, wie z.B. das Installieren von Malware oder das Erstellen von Backdoors.

Schutzmaßnahmen gegen Pass-the-Hash-Angriffe

1. Verwendung von Kerberos:

- Wo möglich, Kerberos anstelle von NTLM verwenden, da Kerberos sicherer ist und weniger anfällig für Pass-the-Hash-Angriffe.

2. Einschränkung von Privilegien:

- Minimieren der Anzahl von Benutzerkonten mit administrativen Rechten und Verwendung von Privileged Access Management (PAM), um den Zugriff zu kontrollieren.

3. Sichere Konfigurationen und Patching:

- Sicherstellen, dass Systeme und Anwendungen stets auf dem neuesten Stand sind, um Sicherheitslücken zu schließen, die zur Hash-Erfassung genutzt werden könnten.

4. Verwendung von multifaktorieller Authentifizierung (MFA):

- Implementierung von MFA, um die Authentifizierung nicht nur von einem Passwort oder Hash abhängig zu machen.

5. Netzwerksegmentierung:

- Segmentierung des Netzwerks, um zu verhindern, dass ein kompromittiertes Konto Zugang zu kritischen Systemen im gesamten Netzwerk erhält.

6. Überwachung und Erkennung:

- Einsatz von Monitoring-Tools und Intrusion Detection Systems (IDS), um verdächtige Aktivitäten zu erkennen, die auf einen Pass-the-Hash-Angriff hinweisen könnten.

Pass-the-Ticket-Angriff

Ein Pass-the-Ticket (PtT)-Angriff ist eine Methode, die von Angreifern verwendet wird, um Zugang zu einem Netzwerk zu erhalten, indem sie gestohlene Ticket-Dateien (normalerweise Kerberos-Tickets) verwenden, um sich als legitimer Benutzer auszugeben. Ähnlich wie bei Pass-the-Hash-Angriffen werden hierbei kryptografische Artefakte wie Kerberos-Tickets ausgenutzt, um unberechtigten Zugriff zu erlangen.

Funktionsweise eines Pass-the-Ticket-Angriffs:

1. Erfassen der Ticket-Datei:

- Der Angreifer muss zuerst Zugriff auf die Ticket-Datei eines legitimen Benutzers erhalten. Diese Dateien enthalten kryptografische Token, die von einem Authentifizierungsserver (normalerweise ein Domain Controller) ausgestellt wurden.

2. Weitergabe des Tickets:

- Nachdem die Ticket-Datei erfasst wurde, verwendet der Angreifer sie, um sich gegenüber anderen Diensten oder Systemen im Netzwerk als der legitime Benutzer auszugeben. Dies ermöglicht es dem Angreifer, auf Ressourcen zuzugreifen, für die der legitime Benutzer berechtigt ist.

3. Ausnutzung von Berechtigungen:

- Durch die Verwendung des gestohlenen Tickets kann der Angreifer auf Ressourcen zugreifen, die für den legitimen Benutzer zugänglich sind. Dies kann sensible Daten, Systemadministrationsrechte oder andere privilegierte Funktionen umfassen.

Beispiel eines Pass-the-Ticket-Angriffs:

1. Erfassen eines Ticket-Granting Tickets (TGT):

- Der Angreifer erlangt Zugriff auf die Ticket-Datei eines Benutzers, die ein Ticket-Granting Ticket (TGT) enthält, das normalerweise vom Key Distribution Center (KDC) ausgestellt wurde.

2. Weitergabe des TGTs:

- Der Angreifer verwendet das TGT, um Zugriff auf andere Dienste oder Ressourcen im Netzwerk zu erhalten. Er gibt sich als der legitime Benutzer aus, für den das TGT ausgestellt wurde.

3. Zugriff auf Ressourcen:

- Durch die erfolgreiche Weitergabe des Tickets kann der Angreifer auf Ressourcen zugreifen, die für den legitimen Benutzer

zer zugänglich sind, wie z.B. Dateien, Anwendungen oder Netzwerkressourcen.

Schutzmaßnahmen gegen Pass-the-Ticket-Angriffe:

1. Monitoring und Auditierung:

- Überwachen Sie das Netzwerk auf verdächtige Aktivitäten, die auf den Missbrauch von Tickets hinweisen könnten, und protokollieren Sie alle Authentifizierungsereignisse.

2. Einsatz von Endpunkt-Sicherheitslösungen:

- Implementierung von Sicherheitslösungen auf Endpunkten, die das Abfangen und die Weitergabe von Ticket-Dateien erkennen können.

3. Sichere Konfiguration von Diensten:

- Konfigurieren Sie Dienste und Anwendungen so, dass sie die Verwendung von Tickets streng überwachen und verdächtige Aktivitäten blockieren oder alarmieren.

4. Regelmäßiges Patchen und Updates:

- Halten Sie alle Systeme und Anwendungen auf dem neuesten Stand, um Sicherheitslücken zu schließen, die von Angreifern ausgenutzt werden könnten, um Tickets zu stehlen.

5. Least Privilege-Prinzip:

- Beschränken Sie die Berechtigungen von Benutzern und Diensten auf das absolute Minimum, das für die Ausführung

ihrer Aufgaben erforderlich ist, um das Potenzial für Missbrauch zu reduzieren.

6. Verwendung von Verschlüsselung:

- Implementierung von Verschlüsselungstechniken, um die Sicherheit von Ticket-Dateien während der Übertragung zu gewährleisten und das Risiko des Abfangens durch Angreifer zu verringern.

Paros Proxy

Paros Proxy ist ein Tool, das für Sicherheitsanalysen und Penetrationstests von Webanwendungen verwendet wird. Es fungiert als Man-in-the-Middle (MitM)-Proxy, der den Datenverkehr zwischen dem Client und der Webanwendung abfängt und analysiert. Hier sind die Hauptmerkmale und typischen Anwendungsfälle von Paros Proxy:

1. Man-in-the-Middle (MitM)-Angriffe. Paros Proxy ermöglicht es einem Sicherheitsforscher oder Penetrationstester, als Proxy-Server zwischen dem Client und der Webanwendung zu agieren. Dadurch kann der Datenverkehr überwacht, manipuliert und analysiert werden.
2. HTTP- und HTTPS-Unterstützung. Das Tool unterstützt sowohl unverschlüsselte HTTP- als auch verschlüsselte HTTPS-Verbindungen, wodurch es möglich ist, auch den verschlüsselten Datenverkehr zwischen Client und Server zu analysieren.

3. Session Recording und Wiedergabe. Paros Proxy kann Sitzungen aufzeichnen, einschließlich der HTTP- und HTTPS-Anfragen und -Antworten, die zwischen dem Client und der Webanwendung ausgetauscht werden. Diese Aufzeichnungen können später zur Analyse oder Wiedergabe verwendet werden.
4. Webanwendungs-Sicherheitsscanner. Es enthält Funktionen zur automatisierten Schwachstellenanalyse von Webanwendungen, einschließlich SQL-Injection, Cross-Site Scripting (XSS) und anderen Sicherheitslücken.
5. Interaktive Manipulation des Datenverkehrs. Paros Proxy erlaubt es dem Benutzer, den HTTP- und HTTPS-Datenverkehr in Echtzeit zu manipulieren, indem Anfragen geändert oder gesendet werden, um das Verhalten der Webanwendung zu testen und Schwachstellen zu identifizieren.
6. Berichterstellung. Es bietet Funktionen zur Erstellung von Berichten über gefundene Sicherheitslücken und Schwachstellen, die in der Webanwendung entdeckt wurden.

Typische Anwendungsfälle

1. Sicherheitsbewertung von Webanwendungen. Sicherheitsforscher und Penetrationstester verwenden Paros Proxy, um Schwachstellen in Webanwendungen zu identifizieren und zu analysieren, einschließlich Sicherheitslücken wie SQL-Injection, XSS und Cross-Site Request Forgery (CSRF).