DDOS RESILIENCY SCORE (DRS)

„Ein offener Standard zur Beurteilung der
Belastbarkeit einer Organisation gegenüber DDoS-Angriffen“
Version 1.00.01 (Deutsche Version)
10. Januar 2017
.....
Inhaltsverzeichnis

1. Einleitung

Der DDoS Resiliency Score, kurz 'DRS', beziffert die Fähigkeit einer Organisation, DDoS-Angriffen diverser Schweregrade zu widerstehen. Das Bewertungsschema ist exponentiell, wie die Richterskala für Erdbeben. Die exponentielle Messung spiegelt die große Bandbreite von DDoS-Angriffen wider und ermöglicht die Plazierung sehr einfacher Angriffe mit geringem Umfang zusammen mit ausgereiften Attacken mit vielen Vektoren und 100 GB/s auf einer gemeinsamen Skala.
Der Bewertungsmechanismus des DRS basiert auf sieben aufsteigenden Stufen von DDoS-Angriffen und der Fähigkeit, den einzelnen Stufen zu widerstehen. Jede Stufe bringt neue Angriffsarten, besser ausgereifte Angriffsvektoren und ein größeres Traffic-Volumen mit sich. Damit steigen auch die Anforderungen für die Verteidigung; jede Stufe erfordert eine kürzere Reaktionszeit zur Schadensbegrenzung und eine geringere Latenz.
Eine Benotung mit 3,8 würde beispielsweise bedeuten, dass eine Organisation die dritte Angriffsstufe bestanden, bei einigen Angriffen der vierten Stufe aber versagt hat.
Aus praktischen Gründen ist 7 als höchste Benotung festgelegt. Eventuell wird die Skala in Zukunft erweitert, um den Entwicklungen neuer DDoS-Angriffe Rechnung zu tragen.

2. Verwendung

Der DRS ist ein Messwerkzeug, mit dem Organisationen ihre Strategie zur Schadensbegrenzung sowie ihre Widerstandsfähigkeit gegenüber DDoS-Angriffen quantitativ bewerten können. Der DRS sorgt außerdem für Objektivität in einem stark umstrittenen Bereich. Er ermöglicht beispielsweise einen Effektivitätsvergleich verschiedener Technologien durch Benotung. Außerdem führt der DRS eine gemeinsame Sprache ein, in der Verwaltungs- und Technikteams kommunizieren können. Eine Benotung mit 4,7 kann die Leitung darauf hinweisen, dass die Fähigkeiten zur Schadensbegrenzung seit der letzten Benotung mit 3,5 verbessert wurden. Dabei wird auch eine Liste bestimmter Angriffsvektoren zusammengestellt, die blockiert bzw. nicht blockiert werden. Diese Liste kann dann von Technikteams analysiert werden. Es wird empfohlen, jede DDoS-bezogene Entscheidung wie beispielsweise Investitionen in Technologien mithilfe des DRS bemessen werden, um Kosteneffizienz zu gewährleisten.

3. Stufen – Definition

3.1 Stufen – Abstrakte Definition

Im Folgenden werden die Stufen genau definiert. Es gibt 7 Stufen. Jede dieser Stufen hat auch einen Umgangsnamen. In diesem Abschnitt wird jede Stufe abstrakt definiert.

Stufe 1 ("Auf blauen Dunst") - Bei einem einfachen Angriff auf blauen Dunst wird geprüft, ob überhaupt DDoS-Widerstandsfähigkeit vorhanden ist. Es werden 1-2 Vektoren bei geringer Frequenz eingebracht.

Stufe 2 ("Skript-Kiddy") - Ein primitiver DDoS-Angriff von einem "Skript-Kiddy". UDP Flood wird hinzugefügt. Die Angriffsfrequenz steigt leicht an, bleibt aber niedrig.

Stufe 3 ("Elementar") - Ein "elementarer" DDoS-Angriff mit mehreren Angriffsvektoren. Beinhaltet eine größere Bandbreite, ist aber noch nicht ausgereift.

Stufe 4 ("Ausgereift") – Auf dieser Stufe werden zum ersten Mal ausgereifte Angriffsvektoren verwendet. Beispielsweise beginnen UDP-Amplified-Reflected-Angriffe mit dieser Stufe.

Stufe 5 ("Andauernd") - Beinhaltet andauernde Angriffe mit **mehreren Vektoren, die noch besser ausgereift sind und sich u.U. abwechseln**; dabei wird nach Schwächen gesucht, und der Umfang erhöht sich. Äquivalent zu einem APT-Angriff (Advanced Persistent Attack).

Stufe 6 ("Extrem") - Ein extremer DDoS-Angriff. Raffinesse und Umfang werden erhöht; exotische Angriffe sind dabei.

Stufe 7 ("staatlich gesponsert") - Auf dieser Stufe werden alle bekannten Techniken zum Durchbrechen der DDoS-Abwehr verwendet.

3.2 Berücksichtigte Belastbarkeitsfaktoren

Die Widerstandskraft einer Organisation gegen DDoS-Angriffe wird durch mehrere Faktoren definiert, die im Folgenden aufgeführt sind. Jeder dieser Faktoren wird mit jeder Stufe erhöht.

Arten von Angriffsvektoren

- Auf jeder Stufe werden mehr Angriffsvektoren eingeführt.

Umfang von Angriffsvektoren

- Jede Stufe beinhaltet Angriffsvektoren mit höherem Umfang. Im Umfang sind die reine Bandbreite (Byte pro Sekunde), Pakete pro Sekunde und Transaktionen pro Sekunde enthalten. Grenzen des Angriffsvolumens werden in Abschnitt 3.3 definiert.

Ausgereiftheit von Angriffsvektoren

- Auf jeder Stufe werden raffiniertere Angriffsvektoren eingeführt. Dies wird in Abschnitt 3.4 definiert.

Anforderungen zur Schadensbegrenzung

- Jede Stufe macht es für die Organisation erforderlich, den Angriff effizienter abzumildern. Hierbei werden Parameter wie die Reaktionszeit zur Schadensbegrenzung und die Latenz während der Schadensbegrenzung gemessen. Dies wird in Abschnitt 3.5 definiert.

3.3. Maximales Volumen pro Angriffsstufe

Im folgenden Abschnitt wird das maximale Angriffsvolumen beschrieben, das bei den einzelnen Stufen verwendet wird. Das Volumen wird jeweils in BPS (Bit pro Sekunde), PPS (Pakete pro Sekunde) und TPS (Transaktionen pro Sekunde) angegeben. Bitte beachten Sie, dass nicht jeder Angriffsvektor das maximale Volumen nutzen kann, das für die

betreffende Stufe definiert ist.

Stufe	Maximales Volumen pro Stufe		
	BPS	PPS	TPS
1	10 MB/s	10.000	1.000
2	100 MB/s	100.000	5.000
3	1 GB/s	1 Mio.	10.000
4	10 GB/s	5 Mio.	100.000
5	100 GB/s	10 Mio.	1 Mio
6	500 GB/s	25 Mio.	> 1 Mio
7	>500 GB/s	100 Mio.	> 1 Mio

3.4 Angriffsvektoren - Perfektionseigenschaften

Auf jeder Stufe erfolgen fortgeschrittenere Angriffe – nicht nur bezüglich des Umfangs oder der Art der Angriffsvektoren, sondern auch bezüglich der Eigenschaften der einzelnen Angriffe. Beispielsweise ist IP-Addressen-Spoofing eine Technik, die in DDoS zur Erzeugung effektiverer Angriffe genutzt wird. Spoofing und weitere Techniken zur Erzeugung effektiverer Angriffe werden als 'Perfektionseigenschaften' bezeichnet. Grob betrachtet sind "Perfektionseigenschaften" äquivalent zu 'Ausweichtechniken', die bei Nicht-DDoS-Angriffen verwendet werden.
Im folgenden Abschnitt werden die einzelnen Eigenschaften beschrieben; außerdem wird angegeben in welcher Stufe sie erstmalig einbezogen wird ("Start in Stufe") und für welchen Angriffsvektor sie gilt ("Gilt für").

3.4.1 IP-Adressen-Spoofing

IP-Adressen-Spoofing (kurz 'Spoofing') ist die Erzeugung von Internet-Protokoll-(IP)-Paketen mit einer gefälschten Quell-IP-Adresse.

Name der Eigenschaft	Spoofing
Beginnt bei Stufe	2
Gilt für	Zustandslose Angriffe

3.4.2 URL-Randomisierung

URL-Randomisierung ist eine Technik, die zur Erzeugung eines effektiveren DDoS-Angriffs verwendet wird, der einige Schadensbegrenzungstechnologien und Caching-basierte Abwehrmethoden umgehen. Sie wird bei webbasierten Angriffen verwendet, HTTP und HTTPS. Die Randomisierung kann entweder im Pfad oder in den Parametern oder in beiden erfolgen.

Name der Eigenschaft	**URL-Randomisierung**
Beginnt bei Stufe	**3**
Gilt für	**HTTP und HTTPS**

3.4.3 Verbergen des Fingerabdrucks von Angriffstools (Fingerprint-Obfuscation)

Viele für Angriffe verwendete Tools hinterlassen Fingerabdrücke in den angreifenden Paketen. Beispielsweise gibt der Headless-Browser PhantomJS standardmäßig seinen Namen im Feld "User-Agent" an. Dadurch können Schadensbegrenzungstechnologien den Angriff mithilfe einer Signatur blocken. Anspruchsvolle Angreifer streben jedoch an, die Fingerabdrücke Ihrer Angriffstools, die nicht wesentlich sind, zu verbergen oder zu verschleiern.

Name der Eigenschaft	**Fingerprint-Obfuscation**
Beginnt bei Ebene	**4**
Gilt für	**Tools mit Fingerabdrücken**

3.5 Anforderungen zur Schadensbegrenzung pro Stufe

Auch Belastbarkeit ist ein Faktor für die Abwehreinheit. Eine Organisation, die in der Lage ist, einen Angriff nach zehn Sekunden vollständig zu entschärfen, ist belastbarer als eine, der dies erst nach zehn Minuten möglich ist. Dieser Parameter wird als 'Reaktionszeit zur Schadensbegrenzung' bezeichnet.

Ein weiterer Parameter ist ‘Latenz’. Ein Dienst, dem bei einem andauernden Angriff 1 Millisekunde mehr Latenz zur Verfügung steht, ist belastbarer als einer, dem 1 zusätzliche Sekunde fehlt. Reaktionszeit zur Schadensbegrenzung und Latenz werden in gleicher Weise in die Bewertung einbezogen. Jede Ebene stellt wachsende Anforderungen. Ein Angriffsvektor wird als 'bestanden' betrachtet, wenn alle angegriffenen Dienste schnell wieder funktionstüchtig werden und eine angemessene Latenz haben.

3.5.1 Anforderungen an die Reaktionszeit zur Schadensbegrenzung

Die Reaktionszeit zur Schadensbegrenzung für die einzelnen Stufen wird wie folgt definiert:

Stufe	**Maximaler Ausfall**
1	**24 Stunden**
2	**6 Stunden**
3	**2 Stunden**
4	**1 Stunde**
5	**30 Minuten**
6	**10 Minuten**
7	**1 Minute**

3.5.1 Latenzanforderungen

Die Latenz wird als das Delta oder die zusätzliche Zeit bei der Rundreise eines durchschnittlichen Pakets im Dienst definiert. Das Delta wird im Gegensatz zur normalen Rundreisezeit nicht angegriffen.

Stufe	Maximale Latenz
1	10 Sekunden
2	5 Sekunden
3	3 Sekunden
4	2 Sekunden
5	1,5 Sekunden
6	1 Sekunde

7	0,5 Sekunden

4. Angriffsvektoren

Im folgenden Abschnitt werden die Angriffsvektoren definiert, die auf den einzelnen Stufen verwendet werden.

4.1 Angriffsvektoren - Darstellung

Jeder Angriffsvektor wird im folgenden Format angegeben

<ID> <Name des Angriffsvektors> <Eigenschaften>

4.1.1 Angriffsvektor-Identifier (ID)

Die Angriffsvektor-ID, kurz als 'ID' bezeichnet, ist eine eindeutige Nummer, die für den Angriffsvektor steht. Die ID ist eine 6-stellige Zahl im folgenden Format:
PFANNN
Hierbei wird jede Zifferdurch einen Buchstaben ausgedrückt, der für Folgendes steht

Ziffer	Definition
P	Die Stufe des Angriffsvektors
F	Gattung des Angriffsvektors
A	Die erste Stufe, auf der dieser Angriffsvektor erscheint
NNN	Eindeutige Zahl, die jeweils einem Angriffsvektor zugewiesen wird

'FANNN' steht für einen individuellen Angriffsvektor, und wenn 'P' vorangestellt ist, werden damit die Angriffsvektor-Einstellungen auf den einzelnen Stufen dargestellt.

4.1.1.1. Nummerierung der Gattungen von Angriffsvektoren

In der folgenden Tabelle wird die Nummerierung der Gattungen von Angriffsvektoren definiert, die als Teil der Art des Angriffsvektors verwendet wird.

Ziffer	Gattung des Angriffsvektors
1	Netzwerkangriffe – TCP
2	Netzwerkangriffe – UDP

3	Netzwerkangriffe – Sonstige (z. B. ICMP, GRE)
5	Angriffe auf Anwendungen
8	Schwer erkennbar und schleichend

4.1.2. Angriffsvektoren - Arten

Der Name des Angriffsvektors (laut Definition in Abschnitt 4.2)

4.1.3. Angriffsvektoren - Eigenschaften

Über die verschiedenen Stufen hinweg werden die gleichen Angriffsvektoren verwendet. Beispielsweise wird SYN Flood auf allen Stufen verwendet, allerdings werden jedes Mal Intensität und Niveau gesteigert. Die Intensität von SYN Flood auf Stufe 1 beträgt 10.000 PPS, auf Stufe 2 sind es 100.000 PPS usw.

4.1.4.1 Eigenschaften von Angriffsvektoren - Volumen

Eigenschaft	Beschreibung / Darstellung
vol_bps=VALUE	Angriffsvolumen in Byte pro Sekunde wie im Feld VALUE definiert.
vol_pps=VALUE	Angriffsvolumen in Paketen pro Sekunde wie im Feld VALUE definiert
vol_cps=VALUE	Angriffsvolumen in Verbindungen pro Sekunde wie im Feld VALUE definiert.
vol_tps=VALUE	Angriffsvolumen in Transaktionen pro Sekunden (auch bekannt als Anfrage/ Sekunde) wie im Feld VALUE definiert

VALUE wird als numerischer Wert angegeben, häufig mit 'K', 'M', 'G' für 'Kilo', 'Mega' und 'Giga'.

4.1.4.1 Eigenschaften von Angriffsvektoren - Perfektionseigenschaften

Die Perfektionseigenschaften von Angriffsvektoren werden in Abschnitt 3.4 definiert. In diesem Abschnitt wird die ihre Darstellung behandelt.

Darstellung	Perfektionseigenschaft (Abschnitt mit der Beschreibung)
ip_spoofing	IP-Adressen-Spoofing (3.4.1)

url_rand	URL-Randomisierung (3.4.2)
no_fingerprint	Fingerabdruck des Angriffsvektors wird verborgen (3.4.3)

4.2. Angriffsvektoren - Spezifikation

Im folgenden Abschnitt werden die Angriffsvektoren in der Reihenfolge ihres Auftretens auf den verschiedenen Stufen angegeben. Die verwendeten Namen sind Bezeichnungen, die in der Branche akzeptiert sind; zusätzliche Informationen über Angriffsvektoren sind im Internet zu finden.
Die Angriffe werden im folgenden Format angegeben
<ID> <Name> <Beschreibung & Spezifikation>
Zeilenvorschub
11001 SYN Flood
Eine Flutung mit TCP-SYN-Paketen, Datengröße SOLLTE 0 sein.

51002 HTTP GET Flood
Eine Flutung mit HTTP-Anfragen.

22003 UDP Flood
Eine Flutung mit UDP-Paketen. Datengröße sollte groß oder sogar maximal sein. DST-Port kann 80 sein.

13004 TCP RST Flood
Eine Flutung mit RST-Paketen.

33005 ICMP Flood
Eine Flutung mit ICMP-Ping-Paketen. Datengröße SOLLTE groß sein.

53006 HTTPS GET Flood
Eine Flutung mit HTTPS-Anfragen.

14007 TCP SYN+ACK Flood
Eine Flutung mit SYN+ACK-Paketen. Die Datengröße SOLLTE klein oder Null sein.

14008 TCP ACK Flood
Eine Flutung mit ACK-Paketen. Die Datengröße SOLLTE klein oder Null sein.

14009 TCP PSH Flood
Eine Flutung mit TCP-PSH-Paketen.

14010 TCP FIN Flood
Eine Flutung mit TCP-FIN-Paketen. Die Datengröße SOLLTE klein oder Null sein.

24011 NTP Reflection Flood
Eine NTP-Reflected-Flutung unter Verwendung des Arguments MONLIST

24012 DNS Query Flood

Eine Flutung mit DNS-Abfragen.

25013 DNS Garbage Flood
Eine Flutung mit SYN+ACK-Paketen. DST-Port muss 53 sein. Die Daten sind Müll (keine ordnungsgemäße DNS-Anfrage oder -Antwort). Datengröße SOLLTE groß sein.

55014 HTTP Flood Cookie Support
Eine HTTP-Flutung, bei der das Angriffstool Cookies unterstützt und auf eine HTTP 302 Redirect Response antworten kann.

85015 HTTP Search Page
Eine HTTP-Flutung auf eine oder mehrere Suchfunktionen auf der angegriffenen Website.

85016 HTTP Large File Download
Eine HTTP-Flutung, die auf eine oder mehrere große Dateien gerichtet ist, die sich auf der Website befinden.

25017 DNS Recursive
Eine Flutung mit DNS-Paketen, bei der sich die Subdomain immer wieder ändert (1000.ddostarget.com, 1001.ddostarget.com usw.)

55018 RUDY (HTTP)
RUDY, auch 'R.U.D.Y' geschrieben, kurz für "Are You Dead Yet" (Bist du schon tot) ist ein HTTP-basierter, schwer erkennbarer und schleichender DDoS-Angriff, bei dem POST-
Abfragen mit großer Content-Length verwendet werden. Allerdings sendet der Angreifer die Daten Byte für Byte, um die Verbindung ständig aufrecht zu erhalten.

55019 Slowloris
Ein schwer erkennbarer und schleichender HTTP-basierter Angriff auf die Apache-Serverfamilie. Bei diesem Angriff werden mehrere HTTP-Anfragen gesendet, wobei jede Anfrage unvollständig ist.

55020 SSL Renegotiation
Ein schwer erkennbarer und schleichender HTTP-basierter Angriff, der die Option zur SSL-Neuverhandlung nutzt. Der Server wird zu einer Neuverhandlung der SSL veranlasst, die viel Rechnerleistung in Anspruch nimmt.

16021 Tsunami SYN Flood
SYN Flood mit sehr großem Datenumfang (normalerweise befinden sich in SYN-Paketen keine Daten)

26022 CHARGEN Reflective Flood
Ein Art UDP-Reflection-Amplification-Angriff, der das Protokoll CHARGEN verwendet

56023 HTTP Flood JavaScript Support
Eine HTTP-Flutung im angreifenden Client kann JavaScript (JS) verarbeiten und daher standardmäßige JS-DDoS-Abwehrmaßnahmen überwinden.

56024 HTTPS Flood Cookie Support
Wie '55014 HTTP Flood Cookie Support', jedoch über HTTPS.

57025 HTTP Flood Headless Browser
Eine HTTP-Flutung im angreifenden Client ist ein Headless-Browser und beinhaltet daher alle Technologien und Bibliotheken eines normalen Browsers und kann mehrere standardmäßige DDoS-Abwehrmaßnahmen überwinden.

57026 HTTPS Flood JavaScript Support
Wie '56023 HTTP Flood JavaScript Support', jedoch über HTTPS.

57027 HTTPS Flood Headless Browser
Wie '57025 HTTP Flood Headless Browser', jedoch über das HTTPS-Protokoll.

57028 R.U.D.Y. (HTTPS)
Wie '55018 RUDY (HTTP)', jedoch über das HTTPS-Protokoll.

4.3 Angriffsvektoren - Spezifikation per Stufe
Die folgenden Angriffsvektoren werden auf den einzelnen Stufen einbezogen. Das Format ist
<ID> <Name des Angriffsvektors>:<Eigenschaften des Angriffsvektors>

STUFE 1
111001 SYN Flood : vol_pps=10K
151002 HTTP GET Flood : vol_tps=1K

STUFE 2
211001 SYN Flood : vol_pps=100K, ip_spoofing
222003 UDP Flood : vol_bps=10M, ip_spoofing
251002 HTTP GET Flood : vol_tps=10K

STUFE 3
311001 SYN Flood : vol_pps=1M, ip_spoofing
311001 TCP RST Flood : vol_bps=500M, ip_spoofing
322003 UDP Flood : vol_bps=500M, ip_spoofing
333005 ICMP Flood : vol_bps=500M, ip_spoofing
351002 HTTP GET Flood : vol_tps=25K
353006 HTTPS GET Flood : vol_tps=5K

STUFE 4
411001 SYN Flood : vol_pps=5M, ip_spoofing
411001 TCP RST Flood : vol_bps=1G, ip_spoofing
414007 TCP SYN+ACK : vol_bps=1G, ip_spoofing
414008 TCP ACK flood : vol_bps=1G, ip_spoofing
414009 TCP PSH Flood : vol_bps=1G, ip_spoofing
414010 TCP FIN Flood : vol_bps=1G, ip_spoofing
422003 UDP Flood : vol_bps=1G, ip_spoofing
433005 ICMP Flood : vol_bps=1G, ip_spoofing
424011 NTP Reflection Flood : vol_bps=1G
451002 HTTP GET Flood : vol_tps=50K, url_rand

453006 HTTPS GET Flood : vol_tps=10K, url_rand
424012 DNS Query Flood : vol_tps=50K, ip_spoofing

STUFE 5
511001 SYN Flood : vol_bps= 10G, ip_spoofing
551002 HTTP GET Flood : vol_tps= 100K, url_rand
522003 UDP Flood : vol_bps= 10G, ip_spoofing
513004 TCP RST Flood : vol_bps= 10G, ip_spoofing
533005 ICMP Flood : vol_bps= 10G, ip_spoofing
553006 HTTPS GET Flood : vol_tps= 20K, url_rand
514007 TCP SYN+ACK Flood : vol_bps= 10G, ip_spoofing
514008 TCP ACK Flood : vol_bps= 10G, ip_spoofing
514009 TCP PSH Flood : vol_bps= 10G, ip_spoofing
514010 TCP FIN Flood : vol_bps= 10G, ip_spoofing
524011 NTP Reflection Flood : vol_bps= 10G
524012 DNS Query Flood : vol_tps= 100K, ip_spoofing
525013 DNS Garbage Flood : vol_bps= 10G, ip_spoofing
555014 HTTP Flood Cookie Support : vol_tps= 20K, url_rand
585015 HTTP Search Page : vol_tps= 20K
585016 HTTP Large File Download : vol_tps= 20K
525017 DNS Recursive : vol_tps= 100K, ip_spoofing
555018 RUDY (HTTP) : vol_tps= 20K
555019 Slowloris : vol_tps= 20K
555020 SSL Renegotiation : vol_tps= 20K

STUFE 6
Die folgenden Angriffsvektoren werden in Stufe 6 einbezogen:
611001 SYN Flood : vol_bps= 50G, ip_spoofing
651002 HTTP GET Flood : vol_tps= 250K, url_rand
622003 UDP Flood : vol_bps= 50G, ip_spoofing
613004 TCP RST Flood : vol_bps= 50G, ip_spoofing
633005 ICMP Flood : vol_bps= 50G, ip_spoofing
653006 HTTPS GET Flood : vol_tps= 50K, url_rand
614007 TCP SYN+ACK Flood : vol_bps= 50G, ip_spoofing
614008 TCP ACK Flood : vol_bps= 50G, ip_spoofing
614009 TCP PSH Flood : vol_bps= 50G, ip_spoofing
614010 TCP FIN Flood : vol_bps= 50G, ip_spoofing
624011 NTP Reflection Flood : vol_bps= 50G
624012 DNS Query Flood : vol_tps= 250K, ip_spoofing
625013 DNS Garbage Flood : vol_bps= 50G, ip_spoofing
655014 HTTP Flood Cookie Support : vol_tps= 50K, url_rand
685015 HTTP Search Page : vol_tps= 50K
685016 HTTP Large File Download : vol_tps= 50K
625017 DNS Recursive : vol_tps= 250K, ip_spoofing
655018 RUDY (HTTP) : vol_tps= 50K, no_fingerprint
655019 Slowloris : vol_tps= 50K, no_fingerprint
655020 SSL Renegotiation : vol_tps= 50K
616021 Tsunami SYN Flood : vol_bps= 50G, ip_spoofing
626022 CHARGEN Reflective Flood : vol_bps= 50G
656023 HTTP Flood JavaScript Support : vol_tps= 50K, url_rand
656024 HTTPS Flood Cookie Support : vol_tps= 50K, url_rand

STUFE 7
Die folgenden Angriffsvektoren werden in Stufe 7 einbezogen:

711001 SYN Flood : vol_bps= 100G, ip_spoofing
751002 HTTP GET Flood : vol_tps= 1M, url_rand
722003 UDP Flood : vol_bps= 100G, ip_spoofing
713004 TCP RST Flood : vol_bps= 100G, ip_spoofing
733005 ICMP Flood : vol_bps= 100G, ip_spoofing
753006 HTTPS GET Flood : vol_tps= 50K, url_rand
714007 TCP SYN+ACK Flood : vol_bps= 100G, ip_spoofing
714008 TCP ACK Flood : vol_bps= 100G, ip_spoofing
714009 TCP PSH Flood : vol_bps= 100G, ip_spoofing
714010 TCP FIN Flood : vol_bps= 100G, ip_spoofing
724011 NTP Reflection Flood : vol_bps= 100G
724012 DNS Query Flood : vol_tps= 1M, ip_spoofing
725013 DNS Garbage Flood : vol_bps= 100G, ip_spoofing
755014 HTTP Flood Cookie Support : vol_tps= 50K, url_rand
785015 HTTP Search Page : vol_tps= 50K
785016 HTTP Large File Download : vol_tps= 50K
725017 DNS Recursive : vol_tps= 1M, ip_spoofing
755018 RUDY (HTTP) : vol_tps= 50K, no_fingerprint
755019 Slowloris : vol_tps= 50K, no_fingerprint
755020 SSL Renegotiation : vol_tps= 50K
716021 Tsunami SYN Flood : vol_bps= 100G, ip_spoofing
726022 CHARGEN Reflective Flood : vol_bps= 100G
756023 HTTP Flood JavaScript Support : vol_tps= 50K, url_rand
756024 HTTPS Flood Cookie Support : vol_tps= 50K, url_rand
757025 HTTP Flood Headless Browser : vol_tps= 50K, url_rand, no_fingerprint
757026 HTTPS Flood JavaScript Support : vol_tps= 50K, url_rand
757027 HTTPS Flood Headless Browser : vol_tps= 50K, url_rand, no_fingerprint
757028 R.U.D.Y. (HTTPS) : vol_tps= 50K, no_fingerprint

5. Vorgehensweise zur Bewertungsberechnung

Im folgenden Abschnitt wird erklärt, wie die tatsächliche Bewertung berechnet wird.

5.1 Allgemeine Beschreibung

Die DRS-Bewertung wird anhand stufenbasierter Tests gemessen. Um eine Stufe zu bestehen, müssen die Schutzvorkehrungen einer Organisation die auf dieser Stufe genutzten Vektoren simultan entschärfen. Angriffe werden in Sequenzen durchgeführt: Angriffsvektoren der Stufe 1, Angriffsvektoren der Stufe 2 usw. Wenn die Organisation in der Lage ist, dem Angriff auf dieser Stufe zu widerstehen, geht sie zur nächsten über. Wenn die Organisation beispielsweise in der Lage war, den Angriffsvektoren der Stufe 1 zu widerstehen, fährt der Test mit den Angriffsvektoren der Stufe 2 fort. Dieser Vorgang wird fortgesetzt, bis die Organisation bei einer Stufe versagt.

5.2 Bestehen oder Nichtbestehen eines Angriffsvektors

Wenn die Organisation in der Lage war, einem Angriffsvektor zu widerstehen und ihre Dienste effektiv und zeitgerecht

bereitzustellen, wird der Angriffsvektor als bestanden ('Bestandener Angriffsvektor') betrachtet, andernfalls als nicht bestanden ('Nicht bestandener Angriffsvektor').

5.3 Stufenbewertung

Nach Durchführung der Angriffe einer bestimmten Stufe und Erfassung der Ergebnisse wird die Stufenbewertung berechnet. Dieser Wert wird als 'Stufenbewertung' bezeichnet.
Die Stufenbewertung wird als Division des bestandenen Angriffsvektors durch die Gesamtzahl der Vektoren auf dieser Stufe plus der Stufennummer minus eins berechnet.
Wenn beispielsweise auf Stufe 3 6 von 10 Angriffsvektoren bestanden wurden, ergibt sich eine Stufenbewertung von 2,6.

5.4 Bestehen, Erfüllen und Nichtbestehen einer Stufe

Durch die Stufenbewertung wird bestimmt, ob diese Stufe bestanden, erfüllt oder nicht bestanden wurde. Dies richtet sich nach dem 'Bestanden-Wert' und dem 'Nicht-bestanden-Wert' pro Stufe, die in der folgenden Tabelle definiert werden. Liegt die Stufenbewertung oberhalb des Bestanden-Werts, so gilt die Stufe als 'Bestanden', und der Test geht zur nächsten Stufe über. Liegt die Testbewertung unterhalb des Nicht-bestanden-Werts, so gilt die Stufe als 'Nicht bestanden'. Liegt die Stufenbewertung zwischen den beiden Werten, gilt die Stufe als 'Erfüllt'. Bei 'Erfüllt' und 'Nicht bestanden' wird der Test nicht auf der nächsten Stufe fortgesetzt; dennoch beeinflussen sie die abschließende Bewertung wie im Folgenden beschrieben.

Level	Bestanden-Wert	Nicht-bestanden-Wert
1	75%	40%
2	75%	40%
3	75%	40%
4	85%	40%
5	85%	40%
6	85%	40%
7	85%	40%

5.5 Abschließende Bewertung

Bei jedem bestandenen Test geht der Test zur nächsten Stufe über. Wenn die letzte Bewertung auf der letzten Stufe 'Erfüllt' war, dann ist diese Bewertung die 'Abschließende Bewertung'. Wenn die letzte Bewertung 'Nicht bestanden' war, dann ist die Abschließende Bewertung

die Bewertung der vorherigen Stufe, d.h. der letzten bestandenen Stufe.

Haftungsausschluss:

Der DDoS Resiliency Score (DRS) wurde von Red Button Ltd. als praktisches Tool zur Bewertung der Schadensbegrenzungsstrategie und der Widerstandsfähigkeit eines Unternehmens gegenüber DDoS-Angriffen entwickelt. Die Entwickler des DRS übernehmen keine Garantie oder gesetzliche Gewährleistung hinsichtlich der Fähigkeit des DRS, DDoS- oder sonstige Angriffe auf eine Organisation vollständig zu verhindern. Red Button Ltd. schließt hiermit jegliche andere ausdrückliche oder stillschweigende Gewährleistung aus, einschließlich, jedoch ohne Beschränkung, jeglicher Garantie hinsichtlich der Tauglichkeit des DRS für einen bestimmten Zweck.
Anmerkung zur deutschen Übersetzung:
Die deutsche Übersetzung nebst kleinen Änderungen wurde von der zeroBS aus Kiel/Deutschland durchgeführt.

Kontakt:
mail: drs@zero.bs
web: https://zero.bs