Beginner's Guide to **Brute Force & DDoS Attacks**

WHAT TO DO WHEN THE BARBARIANS ARE AT YOUR DOOR

www.alienvault.com

Attackers are constantly looking for ways to exploit any weakness in your security defenses. As security professionals, we spend endless hours trying to stay one step ahead of sophisticated attackers attempting to slothfully penetrate our defenses. However, not all attacks are sophisticated or quiet.

Brute force account cracking and Distributed Denial of Service (DDoS) attacks continue to be effective ways for attackers to wreak havoc on organizations.

In this paper we'll explore both types of attacks and provide guidance on what you should do to defend your network.

What is a Distributed Denial of Service Attack?

The fundamental premise of distributed denial of service attacks is simple: flooding services or public websites with so much network traffic they can't function properly (or at all). This can take a devastating toll on targeted organizations — shutting off their revenue streams, and damaging both their brands and customer relationships, with a single stroke.

Historically, distributed denial of service attacks have taken several common forms. Read on to learn about each one...

BASIC DENIAL OF SERVICE

Basic denial of service (DoS) simply involves a single computer/source slamming the targeted site or service with excessive requests (e.g., to view the site or run a search function).

DISTRIBUTED DENIAL OF SERVICE

Distributed denial of service (DDoS) is a variation in which a botnet is used to generate the traffic. Because the botnet is distributed over hosts in many locations, it's slower and harder for an organization to mount an effective defense. Simple rules, such as blocking a particular domain or IP range, no longer apply.

REFLECTED DISTRIBUTED DENIAL OF SERVICE

Reflected distributed denial of service is more sophisticated yet. Here, the botnet poses as the targeted site, using spoofed IP addresses, and tricks other servers/services (not associated with the botnet) into overwhelming the target. For instance, a botnet might persuade public servers that have enabled the Network Time Protocol (NTP) into sending excessive network traffic to the target.

The goal of the attacker is the same in all cases. If the site's architecture can't block the traffic, or scale to meet the demand level, the site or service is effectively taken offline, and the organization suffers significant business consequences. Attackers often leverage this fact to extort payments in a modern-day version of the protection racket.

Distributed Denial of Service Attack
Mitigation & Protection Techniques

DDoS attacks launched by botnets truly have two victims: the targeted organization (whose services/sites are shut down) and the hosts of the botnet (whose architectures are being commandeered to perform illegal actions, while legitimate business activity is compromised).

So mitigating and protecting against distributed denial of service really means addressing both scenarios. Common steps would certainly include:

1. Applying all relevant security patches, as quickly as possible after they are published, to all relevant endpoints

2. Shutting down unnecessary services/ports when possible (such as NTP or UDP)

3. Standard botnet protection as described here in an AlienVault® blog post

DISTRIBUTED DENIAL OF ATTACK RESPONSE OPTIONS

Beyond what has discussed so far, organizations have a variety of effective denial of service attack protection options.

NETWORK INGRESS FILTERING

Network ingress filtering is codified by the Internet Engineering Task Force as BCP 38. It contains best practices to detect and handle any incoming traffic that uses spoofed IP addresses; spoofed packets are simply discarded before being sent to servers. This technique is particularly effective against distributed denial of service attacks when used by an organization’s Internet Service Provider (ISP), so arranging with the ISP to implement is well worth the time.

THIRD-PARTY PROVIDERS

Another powerful response to distributed denial of service attacks: contract with a third-party provider that specializes in filtering such attacks. Essentially, if an attack should occur, incoming traffic can be routed to the contractor to scrub, which then sends back only the legitimate traffic to the organization. The scrubbing process involves sophisticated algorithms that examine packets in various respects (IP address, HTTP header information, etc.) and is often itself operating in a high-performance, scalable cloud architecture, to ensure it can handle even the largest attacks.

DEDICATED NETWORK SOLUTIONS APPLIANCES

Dedicated network solutions/appliances, deployed internally, are also available to help organizations cope with distributed denial of service attacks. These work in a roughly similar fashion — by creating a baseline of expected traffic, they can detect and respond to a DDoS attack, scrubbing out false traffic and forwarding only what is left to services. However, since this approach still requires consuming limited internal resources such as bandwidth and processing power, it’s typically not as scalable in handling the most devastating attacks as a third-party specialist.

Also important, though it feels counter-intuitive to security professionals: advertising to the public that the organization is prepared for distributed denial of service attacks.

If an attacker perceives in advance that a DDoS attack isn't likely to be successful, the odds fall that the attack will be launched in the first place! (Compare this to not just installing a security system in your home, but advertising its existence with a sign in your front yard.)

The Future of Distributed Denial of Service Attack Detection, Protection, & Mitigation

DDoS attacks continue to evolve. Today, for instance, advanced persistent threat (APT) attacks can flood both a targeted organization and its ISP via scheduled sequences of many different attack vectors (such as the application layer, cross-site scripting, and SYN packet floods) — and they can last for a period of weeks.

So, going forward, organizations will have to develop a defensive strategy of equal sophistication. They will need to take advantage of all the techniques described above, and new ones as they emerge, to create a layered, multifaceted security architecture that prevents and defends against the effects of distributed denial of service attacks as comprehensively as possible.

Brute Force Attack

Why bother to pick a lock if you can simply kick in the door?

That’s the logic behind the brute force attack, one of the most common of all security exploits. The idea behind brute force is simple: simply try all possibilities until you find the one that works. Typically, there is no prioritization of some possibilities over others. Instead, all are tried systematically in a simple sequence, such as alphanumerical.

Brute force attacks fall, generally speaking, into two classes. The more common involves an online resource or service, such as an e-mail service; here, the hacker attempts to find a correct password.

Offline brute force attacks, on the other hand, are less common because they involve trying to decrypt a file (such as a UNIX password file), and thus require obtaining the file in the first place.

As a group, all brute force attacks combined are (according to a 2015 McAfee Security Report) the second-most common of all exploit types,

amounting to some 25% of the total.*

WordPress sites in particular are often hit with such attacks in order to obtain control of the publishing platform and leverage it for malicious purposes.

* #1 is Denial of Service

Why are Brute force Attacks Employed?

What's the motive behind a brute force attack? The most obvious is also the most common: privileged access to restricted data, applications, or resources of all kinds.

In some cases, a brute force attack is also a logical stepping-stone or pivot point — by brute-forcing to point A, it's then possible to launch subsequent exploits (perhaps of a different type) to get to points B-Z. The hacker may also seek to install something such as a rootkit, add a new bot to a botnet, create a command and control center for a botnet, or (if possible) simply steal money or sensitive information (such as credit card numbers or banking credentials) that lead directly to money.

How to Identify Brute Force Attacks

So how can you spot a brute force attack while it is happening? No single indicator is certain, but these are all logical possibilities. Many failed log-ins from the same IP address. This is a particularly strong sign (though if the attacker is using a botnet, IP addresses will obviously vary).

- Logins with multiple username attempts emerging from the same IP address
- Logins for a single account coming from many different IP addresses
- Excessive bandwidth consumption over the course of a single session
- Failed login attempts from alphabetically sequential usernames or passwords
- A referring URL drawn from someone's mail or IRC client
- A referring URL that contains the username and password in this format: http://user:password@www.example.com/login.htm
- A referring URL drawn from known password-sharing websites
- Failed log-in attempts that include passwords commonly used by users and hackers alike (123456, password, qwerty, pwnyou, etc.)

Putting Up a Stout Defense

Toward fending off a brute force attack, a variety of straightforward options include:

- **Locking the account after a fixed number of failed attempts.** Apple's failure to implement this initially in its iCloud service led, in 2014, to successful brute force hacks and the mass distribution of embarrassing celebrity photos.
- **Delaying the response time.** The more time between permitted password attempts, the more slowly the brute force attack will proceed, and the more time is available for sysadmins to discover an attack is underway.
- **IP address lock-out.** If failed attempts from a given IP address exceed a maximum predefined number, that address can be locked out… though if the attacker is using a botnet, with many IP addresses for its bots, this approach will be inadequate.
- **Detection tools.** Based on key indicators such as the bulleted list provided above, tools such as OSSEC can sometimes detect a brute force attack is underway and take direct action to block it, notify administrators of it, or both.
- **Brute force site scanners.** The idea behind these tools is to go through site logs looking for signs that a brute force exploit has recently been attempted. While the horse may be out of the barn in such a case, it's still worthwhile knowing that it happened, so that effective measures can be implemented to prevent a recurrence.

The Future of Brute Force Attacks

Unfortunately, brute force is a class of attack that's unlikely to vanish any time soon. Going forward, in fact, it's clear that brute force attacks are likely to become both more prevalent and more effective.

This is a simple consequence of the fact that the more computational power you have, the faster and more successful a brute force attack is likely to be, all other factors being equal. And in today's world of botnets, not to mention scalable grid and cloud architectures, computational power is relatively cheap and easy to get.

In the near future, in fact, artificial intelligence may even be applied to simplify/prioritize the brute force process by focusing on the most promising possibilities first. This being the case, security professionals will have to stay on their toes.

HOW ALIENVAULT HELPS DEFEND AGAINST DDOS AND BRUTE FORCE ATTACKS

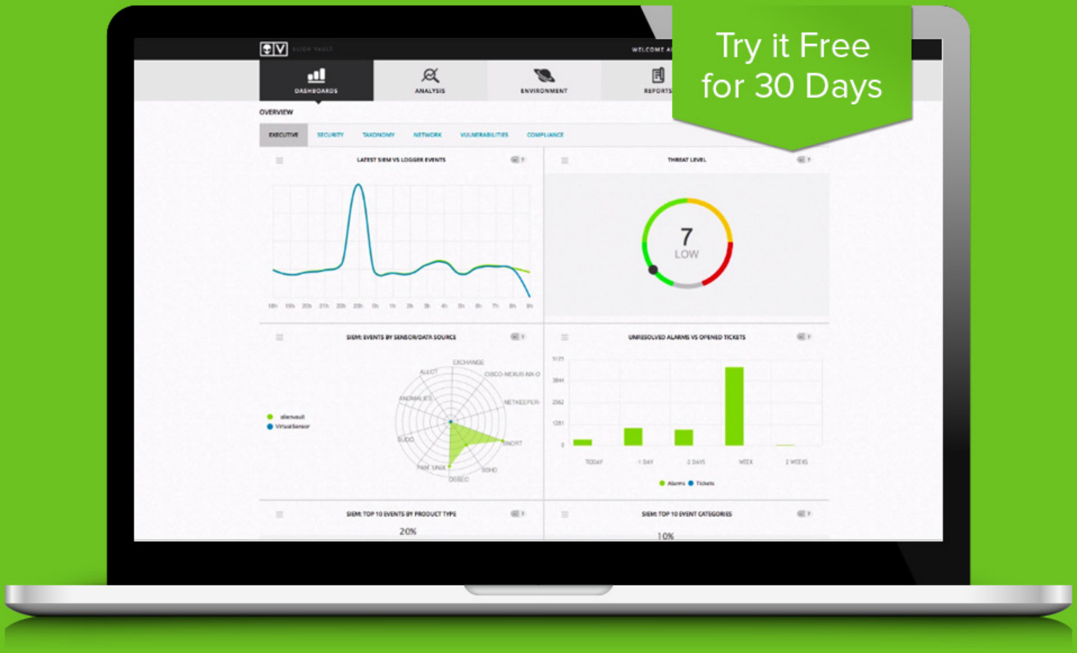
DDoS and brute force login attacks continue to plague organizations because they are simple and effective in meeting attacker's objectives. The key in defending against these types of attacks is your ability to detect and quickly respond to minimize the impact to your organization.

The AlienVault Unified Security Management (USM)™ platform provides the essential security capabilities that organizations of all sizes need to detect, prioritize, and respond to threats like DDoS and brute force attacks. To keep our users up to date with new and evolving threats, the AlienVault Labs team performs the threat research that most IT teams simply don't have the expertise, time, budget, or tools to do themselves. This research is then converted into actionable feeds that are pushed out regularly to the USM platform with updated correlation directives and malicious behavioral signatures.

In addition, USM can be tightly integrated with the Open Threat Exchange (OTX)™. You have the opportunity to join, contribute, and benefit from this community of like-minded and similarly exposed IT teams that share threat intelligence and IP reputation of known bad actors that have been operating DDoS and brute force campaigns against them.

Be ready when the barbarians come knocking with the advanced threat detection and response capabilities of AlienVault USM.

Next Steps: Play, share, enjoy!


DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
OVERVIEW
EXECUTIVE
SECURITY
TAXONOMY
NETWORK
VULNERABILITIES
COMPLIANCE
LATEST SIEM VS LOGGER EVENTS
THREAT LEVEL
7
LOW
SIEM: EVENTS BY SENSOR/DATA SOURCE
UNRESOLVED ALARMS VS OPENED TICKETS
SIEM: TOP 10 EVENTS BY PRODUCT TYPE
SIEM: TOP 10 EVENT CATEGORIES
20%
10%

Try it Free for 30 Days

- Learn more about threat management with AlienVault USM
- Create a personalized demo
- Start detecting threats today with a free 30-day trial
- Join the Open Threat Exchange

www.alienvault.com