

Dos vs DDoS Attacks: The Differences and How To Prevent Them



TIM KEARY - NETWORK ADMINISTRATION EXPERT TO BUSINESSES

November 21, 2018



What's a DoS attack? What's a DDoS attack and what's the difference?

A **DoS attack** is a denial of service attack where a computer (or computers) is used to flood a server with TCP and UDP packets. A **DDoS attack** is where multiple systems target a single system with a DoS attack. The targeted network is then bombarded with packets from multiple locations.

“ All DDoS = DoS but not all DoS = DDoS.



Denial of Service (DoS) and **Distributed Denial of Service (DDoS)** attacks are two of the most intimidating threats that modern enterprises face. Few forms of attack can have the financial ramifications as that of a successful DoS attack. Security surveys indicate that the cost of a DDoS attack averages between **\$20,000-\$40,000 per hour**.

This is an astronomical figure and can put even the largest organizations under pressure.

>>>Jump to edge service solution providers for DDoS attacks<<<

A successful DDos attack not only **puts you out of action for a substantial time period** but can even **cause certain systems to malfunction**. Every day you're out of action piles up costs you would otherwise be without. In this article, we're going to look at the dangers of DoS vs DDoS to see what the difference is.

Contents [\[hide\]](#)

1. What's a DoS attack? What's a DDoS attack and what's the difference?
2. What is a DoS Attack?
3. What is a DDoS Attack?
4. Broad Types of DOS and DDOS Attacks
5. Most Common Forms of DDOS Attacks
6. DoS vs DDoS: What's the Difference?
7. Why do DoS and DDoS Attacks Occur?
8. How to Prevent DoS and DDoS attacks 
9. Edge Services Vs DDOS Attacks 
10. DoS vs DDoS Attacks: A Manageable Menace

What is a DoS Attack?

A **DoS attack** is a **denial of service attack** where a computer (or computers) is used to **flood a server with TCP and UDP packets**. During this type of attack, the service is put out of action as the packets sent **overload the server's capabilities and make the server unavailable** to other devices and users throughout the network. DoS attacks are used to shut down individual machines and networks so that they can't be used by other users.

There are a number of different ways that DoS attacks can be used. These include the following:

- **Buffer overflow attacks** – This type of attack is the most common DOS attack experienced. Under this attack the attacker [overloads a network address](#) with traffic so that it is put out of use.
- **Ping of Death or ICMP flood** – An [ICMP](#) flood attack is used to take unconfigured or misconfigured network devices and uses them to send spoof

packets to ping every computer within the network. This is also known as a ping of death (POD) attack.

- **SYN flood** – SYN flood attacks send requests to connect to a server but don't complete the handshake. The end result is that the network becomes inundated with connection requests that prevent anyone from connecting to the network.
- **Teardrop Attack** – During a teardrop DOS attack an attacker sends IP data packet fragments to a network. The network then attempts to recompile these fragments into their original packets. The process of compiling these fragments exhausts the system and it ends up crashing. It crashes because the fields are designed to confuse the system so that it can not put them back together.

The ease with which DoS attacks can be coordinated has meant that they have become **one of the most pervasive cybersecurity threats** that modern organizations have to face. DoS attacks are simple but effective and can bring about devastating damage to the companies or individuals they are aimed at. With one attack, an organization can be put out of action for days or even weeks.

The time an organization spends offline adds up. Being unable to access the network costs organizations thousands every year. Data may not be lost but the disruption to service and downtime can be massive. Preventing DoS attacks is one of the basic requirements of staying protected in the modern age.

What is a DDoS Attack?

A **DDoS attack** is one of the most common types of DoS attack in use today. During a DoS attack, **multiple systems target a single system with a DoS attack**. The **targeted network is then bombarded with packets from multiple locations**. By using multiple locations to attack the system the attacker can put the system offline more easily. The reason for this is that there is a larger number of machines at the attackers' disposal and it becomes difficult for the victim to pinpoint the origin of the attack.

In addition, using a DDoS attack **makes it more complicated to recover**. Nine times out of ten the systems used to execute DDoS attacks have been compromised so that the attacker can launch attacks remotely through the use of slave computers. These slave computers are referred to as zombies or bots.

These bots form a network of devices called a **botnet** that is managed by the attacker through a command and control server. The command and control server allows the

attacker or botmaster to coordinate attacks. Botnets can be made up of anywhere between a handful of bots to hundreds of different bots.

See also: [Understanding DoS and DDoS attacks](#)

Broad Types of DOS and DDOS Attacks

There are a number of broad categories that DOS attacks fall into for taking networks offline. These come in the form of:

- **Volumetric Attacks** – Volumetric attacks are classified as any form of attack where a network's bandwidth resources are deliberately consumed by an attacker. Once network bandwidth has been consumed it is unavailable to legitimate devices and users within the network. Volumetric attacks occur when the attacker floods network devices with ICMP echo requests until there is no more bandwidth available.
- **Fragmentation Attacks** – Fragmentation attacks are any kind of attack that forces a network to reassemble manipulated packets. During a fragmentation attack the attacker sends manipulated packets to a network so that once the network tries to reassemble them, they can't be reassembled. This is because the packets have more packet header information than is permitted. The end result is packet headers which are too large to reassemble in bulk.
- **TCP-State Exhaustion Attacks** – In a TCP-State Exhaustion attack the attacker targets a web server or firewall in an attempt to limit the number of connections that they can make. The idea behind this style of attack is to push the device to the limit of the number of concurrent connections.
- **Application Layer Attacks** – Application layer or Layer 7 attacks are attacks that target applications or servers in an attempt to use up resources by creating as many processes and transactions possible. Application layer attacks are particularly difficult to detect and address because they don't need many machines to launch an attack.

Most Common Forms of DDOS Attacks

As you can see, DDoS attacks are the more complex threat because they use a range of devices that increase the severity of attacks. Being attacked by one computer is not the same as being attacked by a botnet of one hundred devices!

Part of being prepared for DDOS attacks is being familiar with as many different attack forms as you can. In this section, we're going to look at these in further detail so you

can see how these attacks are used to damage enterprise networks.

DDoS attacks can come in various forms including:

Ping of Death – During a Ping of Death (POD) attack the attacker sends multiple pings to one computer. POD attacks use manipulated packets to send packets to the network which have IP packets that are larger than the maximum packet length. These illegitimate packets are sent as fragments.

Once the victim's network attempts to reassemble these packets network resources are used up, they are unavailable to legitimate packets. This grinds the network to a halt and takes it out of action completely.

DDoS attacks can come in various forms including:

- **UDP Floods** – A UDP flood is a DDoS attack that floods the victim network with User Datagram Protocol (UDP) packets. The attack works by flooding ports on a remote host so that the host keeps looking for an application listening at the port. When the host discovers that there is no application it replies with a packet that says the destination wasn't reachable. This consumes network resources and means that other devices can't connect properly.
- **Ping Flood** – Much like a UDP flood attack, a ping flood attack uses ICMP Echo Request or ping packets to derail a network's service. The attacker sends these packets rapidly without waiting for a reply in an attempt to make the network unreachable through brute force. These attacks are particularly concerning because bandwidth is consumed both ways with attacked servers trying to reply with their own ICMP Echo Reply packets. The end result is a decline in speed across the entire network.
- **SYN Flood** – SYN Flood attacks are another type of DoS attack where the attacker uses the TCP connection sequence to make the victim's network unavailable. The attacker sends SYN requests to the victim's network which then responds with a SYN-ACK response. The sender is then supposed to respond with an ACK response but instead the attacker doesn't respond (or uses a spoofed IP address to send SYN requests instead). Every request that goes unanswered takes up network resources until no devices can make a connection.
- **Slowloris** – Slowloris is a type of DDoS attack software that was originally developed by Robert Hansen or RSnake to take down web servers. A Slowloris attack occurs when the attacker sends partial HTTP requests with no intention of

completing them. To keep the attack going, Slowloris periodically sends HTTP headers for each request to keep the network's resources tied up. This continues until the server can't make any more connections. This form of attack is used by attackers because it doesn't require any bandwidth.

- **HTTP Flood** – In a HTTP Flood attack the attacker uses HTTP GET or POST requests to launch an assault on an individual web server or application. HTTP floods are a Layer 7 attack and don't use malformed or spoofed packets. Attackers use this type of attacks because they require less bandwidth than other attacks to take the victim's network out of operation.
- **Zero-Day Attacks** – Zero-Day attacks are attacks that exploit vulnerabilities that have yet to be discovered. This is a blanket term for attacks that could be faced in the future. These types of attacks can be particularly devastating because the victim has no specific way to prepare for them before experiencing a live attack.

DoS vs DDoS: What's the Difference?

The **key difference between DoS and DDoS** attacks is that **the latter uses multiple internet connections** to put the victim's network offline whereas **the former uses a single connection**. DDoS attacks are more difficult to detect because they are launched from multiple locations so that the victim can't tell the origin of the attack. Another key difference is the volume of attack leveraged, as DDoS attacks allow the attacker to send massive volumes of traffic to the victim's network.

It is important to note that DDoS attacks are executed differently to DoS attacks as well. **DDoS attacks** are executed through the **use of botnets** or networks of devices under the control of an attacker. In contrast, **DoS attacks** are generally launched through the **use of a script or a DoS tool** like **Low Orbit Ion Cannon**.

Why do DoS and DDoS Attacks Occur?

Whether it is a DoS or DDoS attack, there are many nefarious reasons why an attacker would want to put a business offline. In this section, we'll look at some of the most common reasons why DoS attacks are used to attack enterprises. Common reasons include:

- **Ransom** – Perhaps the most common reason for DDOS attacks is to extort a ransom. Once an attack has been completed successfully the attackers will then demand a ransom to halt the attack and get the network back online. It isn't

advised to pay these ransoms because there is no guarantee that the business will be restored to full operation.

- **Malicious Competitors** – Malicious competitors looking to take a business out of operation are another possible reason for DDoS attacks to take place. By taking an enterprise's network down a competitor can attempt to steal your customers away from you. This is thought to be particularly common within the online gambling community where competitors will try to put each other offline to gain a competitive advantage.
- **Hacktivism** – In many cases the motivation for an attack won't be financial but personal and political. It is not uncommon for hacktivist groups to put government and enterprise sites offline to mark their opposition. This can be for any reason that the attacker deems to be important but often occurs due to political motivations.
- **Causing Trouble** – Many attackers simply like causing trouble for personal users and networks. It is no secret that cyber attackers find it amusing to put organizations offline. For many attackers, DDoS attacks offer a way to prank people. Many see these attacks as 'victimless' which is unfortunate given the amount of money that a successful attack can cost an organization.
- **Disgruntled Employees** – Another common reason for cyber attacks is disgruntled employees or ex employees. If the person has a grievance against your organisation then a DDoS attack can be an effective way to get back at you. While the majority of employees handle grievances maturely there are still a minority who use these attacks to damage an organization they have personal issues with.

How to Prevent DoS and DDoS attacks

Even though DOS attacks are a constant threat to modern organizations, there are a number of different steps that you can take to stay protected before and after an attack. Before implementing a protection strategy it is vital to recognize that you won't be able to prevent every DoS attack that comes your way. That being said, you will be able to **minimize the damage of a successful attack** that comes your way.

Minimizing the damage of incoming attacks comes down to three things:

- Preemptive Measures

- Test Run DOS Attacks
- Post-attack Response

Preemptive measures, like network monitoring, are intended to help you **identify attacks before they take your system offline** and act as a barrier towards being attacked. Likewise, **test running DoS attacks allows you to test your defenses** against DoS attacks and refine your overall strategy. Your post-attack response will determine how much damage a DoS attack does and is a strategy to get your organization back up and running after a successful attack.

Preemptive Measures: Network Monitoring

Monitoring your network traffic is one of the best preemptive steps you can take. Monitoring traffic will allow you to see the signs of an attack before the service goes down completely. By monitoring your traffic you'll be able to **take action the moment you see unusual traffic** levels or an unrecognized IP address. This can be the difference between being taken offline or staying up.

Before executing an all-out attack, **most attackers will test your network with a few packets before launching the full attack**. Monitoring your traffic will allow you to monitor for these small signs and detect them early so that you can keep your service online and avoid the costs of unexpected downtime.

See also: [25 best network monitors](#)

Test Run DoS Attacks

Unfortunately, you won't be able to prevent every DoS attack that comes your way. However, you can make sure you're prepared once an attack arrives. One of the most direct ways to do this is to **simulate DDoS attacks against your own network**. Simulating an attack allows you to **test out your current prevention methods** and helps to **build up some real-time prevention strategies** that can save lots of money if a real attack comes your way.

Post-Attack Response: Create a Plan

If an attack gets off the ground then you need to have a plan ready to run damage control. **A clear plan can be the difference between an attack that is inconvenient and one that is devastating**. As part of a plan, you want to **designate roles to**

members of your team who will be responsible for responding once an attack happens. This includes designing procedures for customer support so that customers aren't left high and dry while you're dealing with technical concerns.

Edge Services Vs DDOS Attacks

Undoubtedly one of the most effective ways to meet DDoS attacks head-on is to utilize an **edge service**. An edge service solution like **StackPath** or **Sucuri** can sit at the edge of your network and intercept DDoS attacks before they take effect. In this section, we're going to look at how these solutions can keep your network safe from unscrupulous attackers.

StackPath Edge Services

One of the biggest concerns when staying protected against DDOS attacks is preventing damage whilst maintaining performance. StackPath edge services have been designed to minimize performance degradation and fight off all common forms of DDOS attacks. With StackPath edge services, you can **recognize attacks in real-time and block them** before they take the network offline.

User Agents ▼2 of 2 Active

Block requests with missing or invalid user agent string [Show More ▼](#)

WAF & OWASP Top Threats ▲10 of 10 Active

StackPath's core rule set & OWASP's most critical web-application security risks [Hide ▲](#)

Type	Description	
SQL Injection	Block requests with parameters suspected of a SQL injection attack attempt. SQL injection attacks attempt to exploit vulnerabilities in a web application's code and seek to gain access and control over the database. A successful attack would typically result in stolen data or the site being defaced or taken down.	<div>On</div>
XSS Attack	Block requests with parameters suspected of a Cross-Site-Scripting attack attempt. Cross Site Scripting attacks attempt to exploit vulnerabilities in a web application and seek to inject a client side script either across an entire site or to a specific user's session. A successful attack would typically allow forbidden access to a user's actions and data.	<div>On</div>
Shellshock	Block requests with parameters suspected of a Shellshock attack attempt. A Shellshock attack is an attempt to exploit a server's vulnerabilities to gain full access and control over them. A successful attack would typically either abuse a server's resources or hack the website.	<div>On</div>
Remote File Inclusion	Block requests with parameters suspected of a Remote File Inclusion attempt. Remote File Inclusion attempts to exploit vulnerabilities in a web application (typically in PHP) to execute a script from a 3rd party server. RFI attacks provide a backdoor for the hacker to change the behavior of a server and web application.	<div>On</div>
Wordpress WAF Ruleset	Enable a set of rules designed to block common Wordpress exploits.	<div>On</div>
Apache Struts Exploit	Patch known vulnerabilities in the Apache Struts framework by blocking requests with parameters suspected of exploiting these vulnerabilities.	<div>On</div>
Local File Inclusion	Block requests with parameters suspected of a Local File Inclusion attempt. Local File Inclusion attempts seek to exploit vulnerabilities in a web application to execute potentially harmful scripts on your servers.	<div>On</div>

For more sophisticated attacks, [Stackpath's Web Application Firewall \(WAF\)](#) prevents application layer assaults from seeping through. Application layer attacks are blocked by algorithms that can detect the signs of malicious traffic before it reaches your network.

OVERVIEW

ORIGIN SETTINGS

CACHE SETTINGS

EDGE SSL

EDGE RULES

Force HTTPS Connections

On

This setting will force HTTPS connections on your CDN site and is our recommended setting. Please make sure you have an Edge SSL Certificate for this to work properly. **Warning:** Please make sure you have an Edge SSL Certificate for this to work properly.

Force www Connections

Off

To force the www on your site, simply turn this on. Once on, we'll redirect to make sure all requests to your website have www in the URL. **Warning:** This can break your site if you're using h8j6q7r9.stackpathcdn.com to load assets.

Custom Rules | 4

Add Custom Rule

Name	Action
Canonical Header	Edit Delete
User-Agent Redirection	Edit Delete
no cache query string	Edit Delete
test header	Edit Delete

Results Per Page 15

< 1 >

StackPath also offers the [StackPath Edge Delivery 200](#) service for larger networks that has a number of other measures to defend against other types of DDOS attacks like **UDP floods**, **SYN floods**, and **HTTP floods** as well. No matter what kind of DDOS attack you are subjected to, StackPath solutions have core functions that can help you stay protected from being taken offline.

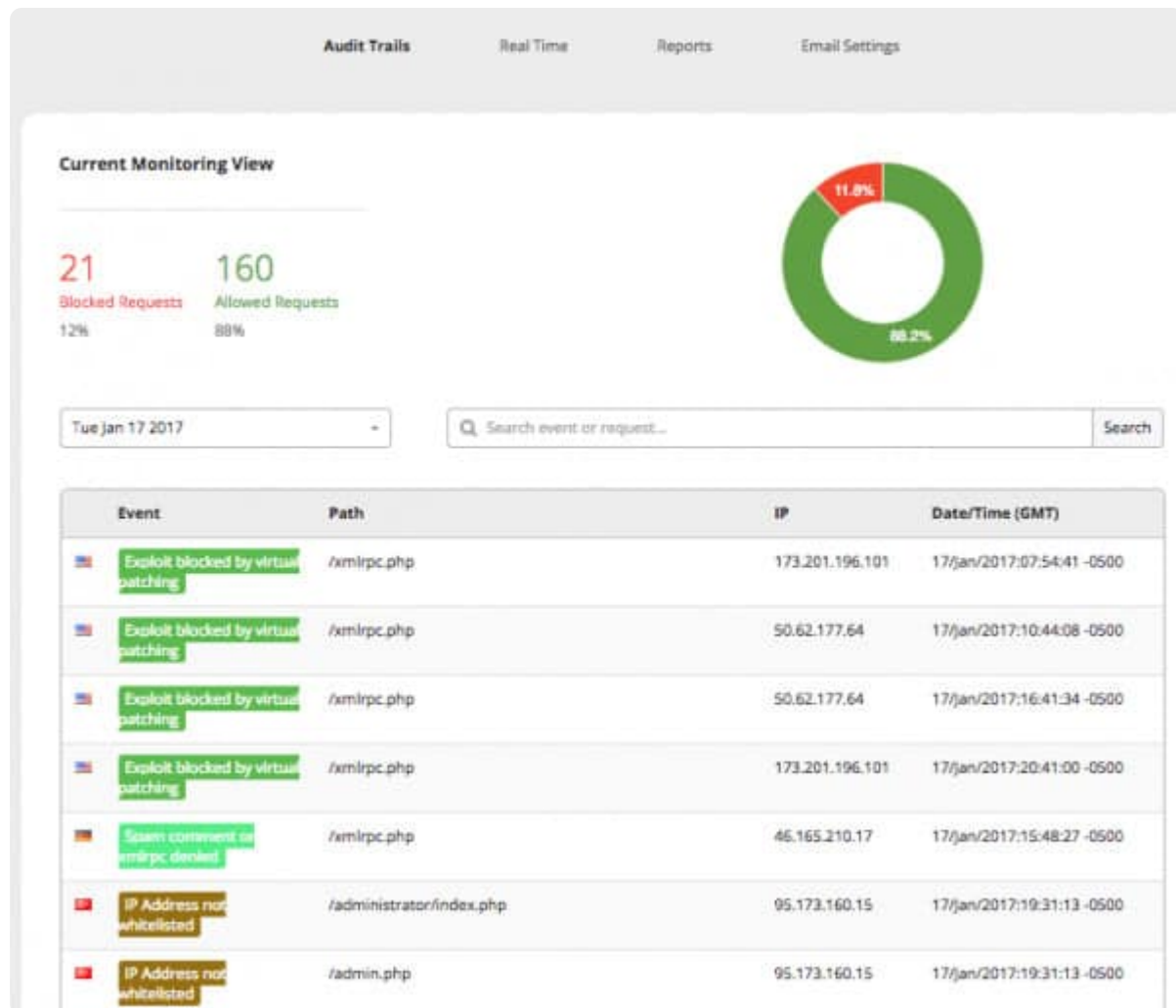


StackPath Edge Delivery 200

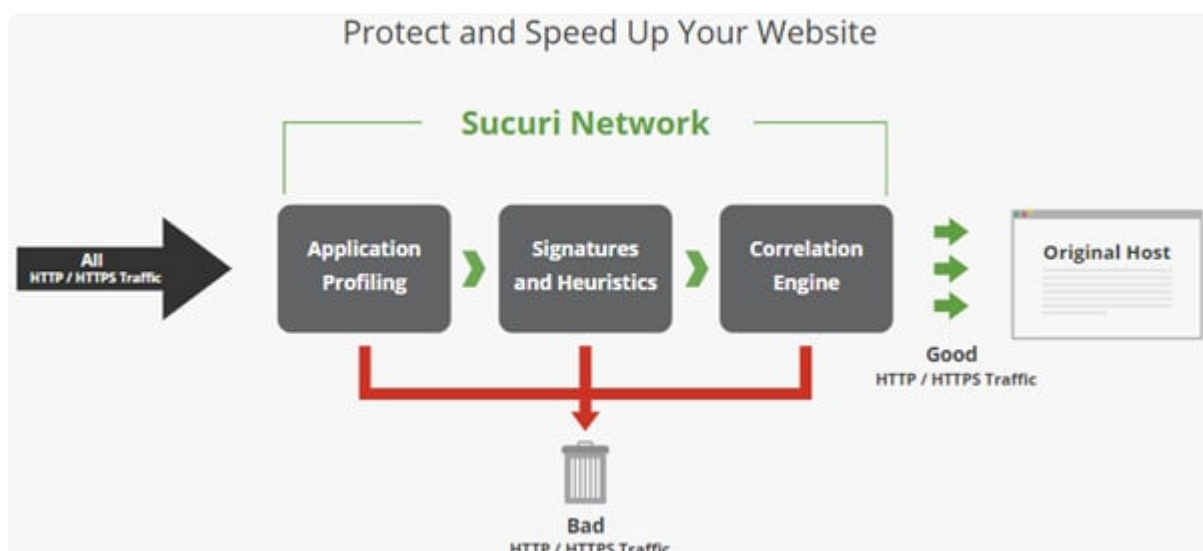
[Find a Suitable Plan at Stackpath.com](#)

[Sucuri Edge Services](#)

Another leading provider of DDoS prevention solutions is **Sucuri's DDoS Protection & Mitigation service**. Sucuri is adept at handling **layer 7 HTTP floods** but can also prevent **TCP SYN floods**, **ICMP floods**, **Slowloris**, **UDP floods**, **HTTP cache bypass**, and **amplified DNS DDoS** to name a few.



Sucuri has a website application firewall approach that has a **globally distributed network with 28 points of presence**. There is also no cap on attack size so no matter what happens you stay protected. The Sucuri WAF is cloud-based SaaS solution which intercepts HTTP/HTTPS requests that are sent to your website.



One particularly useful feature is **the ability to identify if traffic is coming from the browser of a legitimate user or a script being used by an attacker**. This ensures that everyday users can still access the site and its services while malicious users are blocked from launching their attacks. Sucuri offers [various plans](#) for their edge services according to your network needs.



See also: [The 5 Best Edge Services Providers](#)

DoS vs DDoS Attacks: A Manageable Menace

There are few attacks as concerning as DoS attacks to modern organizations. While having data stolen can be extremely damaging, having your service terminated by a brute force attack brings with it a whole host of other complications that need to be dealt with. Just a day's worth of downtime can have a substantial financial impact on an organization.

Having a familiarity with the types of DoS and DDoS attacks that you can encounter will go a long way towards minimizing the damage of attacks. At the very least you want to **make sure that you have a [network monitoring tool](#)** so that you can detect unusual traffic that indicates a potential attack. Though if you're serious about addressing DoS attacks then you need to make sure that you **have a plan to respond after the attack**.

DoS attacks have become one of the most popular forms of cyberattack in the world because they are easy to execute. As such it is incredibly important to be proactive and implement as many measures as you can to prevent attacks and respond to attacks if they are successful. In doing so, you will limit your losses and leave yourself in a position where you can return to normal operation as quickly as possible.

See also: [100+ Terrifying Cybercrime and Cybersecurity Statistics & Trends](#)

Further Reading:

- [The 5 Best Edge Services Providers](#)
- [Understanding DoS and DDoS attacks](#)

Popular Posts



26 Best Network Monitoring Tools and Software of 2019

March 18, 2019 / by Tim Keary



10 Best Free TFTP Servers for Windows, Linux and Mac

February 28, 2019 / by Jon Watson