Directory Traversal Scenario

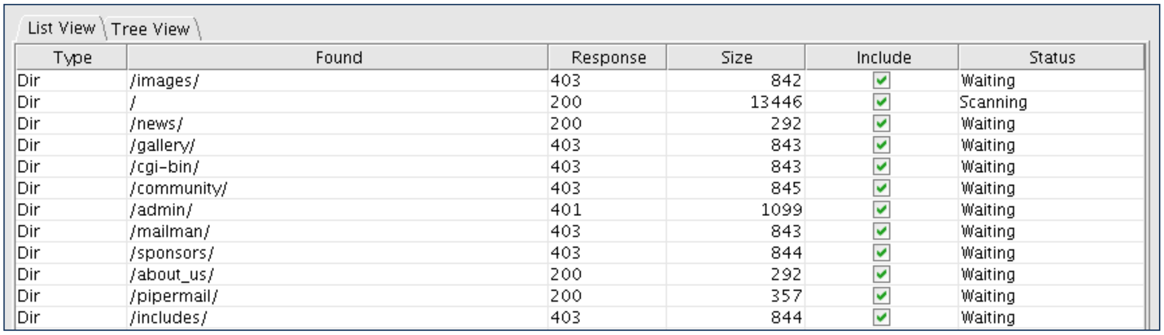
Directory Traversal is a form of web application intrusion used by hackers to attempt to discover your web application files and software. In this white paper, we briefly discuss the Directory Traversal scenario, provide an example of how it is used, explain how NetGladiator stops the attack, and tie this in to your overall layered security approach.

Directory Traversal Description

Directory Traversal is one of the techniques used to discover file structure as well as software utilized by the server. This is essentially a brute force attempt to discover what files exist, what their permissions are, and what their function is in the overall web application.

Example

At right is a sample output of a directory traversal tool. The software is brute-forcing common names from a very large list. When it gets a response code of anything other than 404 (does not exist), it prints it here for further exploration. The attacker can then manually explore interesting results (like pipermail and admin above) for vulnerabilities.



Type	Found	Response	Size	Include	Status
Dir	/images/	403	842	☑	Waiting
Dir	/	200	13446	☑	Scanning
Dir	/news/	200	292	☑	Waiting
Dir	/gallery/	403	843	☑	Waiting
Dir	/cgi-bin/	403	843	☑	Waiting
Dir	/community/	403	845	☑	Waiting
Dir	/admin/	401	1099	☑	Waiting
Dir	/mailman/	403	843	☑	Waiting
Dir	/sponsors/	403	844	☑	Waiting
Dir	/about_us/	200	292	☑	Waiting
Dir	/pipermail/	200	357	☑	Waiting
Dir	/includes/	403	844	☑	Waiting

How NetGladiator Stops This Attack

Directory Traversal relies on sending many requests in a short period of time. Without the ability to send hundreds of thousands of requests, the tool used above is useless. NetGladiator stops this attack by tracking requests on a per IP basis. If the requests exceed a threshold, the IP is blocked. The assumption here is that no normal user sends thousands of requests per minute.

The NetGladiator is a key device in a layered security approach. Its behavior-based anomaly detection identifies potential attackers through recognizing unusual patterns of behavior, as hackers explore and utilize your website much differently than a normal user.

Layer This With...

There are four primary actions you can take to limit the successfulness of a directory brute-forcing tool:

1. Turn off directory listings.
2. Put all sensitive interfaces behind a .htaccess file that has password authentication.
3. Remove all old versions of software, especially software that is no longer used.
4. Keep up-to-date on security releases for software and your web server.

When developing an IT security policy and implementing security controls, the single most important thing to consider is how the different controls you use will layer within your security profile. Because no single piece of equipment or software will be able to thwart 100% of attacks, good layering provides the best chance to stop a hacker from their ultimate goal.

About APconnections, Inc.

APconnections is an innovation-driven technology company that delivers best-in-class network traffic management solutions to give our customers better networks, with zero maintenance, at the best prices. We specialize in turn-key bandwidth shaping and intrusion prevention system (IPS) appliances.

Since 2003, APconnections' mission has been to provide simple turn-key network optimization appliances to any network topology. Our products are simple to install, easy to use, require little maintenance, and are offered at the best prices.

APconnections is based in Lafayette, Colorado, USA. We released our first commercial offering in July 2003, and since then thousands of customers all over the world have put our products into service. Today, our flexible and scalable solutions can be found in many types of public and private organizations of all sizes across the globe, including: Fortune 500 companies, major universities, K-12 schools, Internet providers, law firms, hotels, hospitals, libraries, business centers, small businesses, non-profits, military, and government agencies on six (6) continents.

To Learn More...

We would be a happy to discuss the NetGladiator technology, to help you to determine if this is the right solution for you. Please email ips@apconnections.net or call us at **303.997.1300 x123**.