CS 3350 - Intro to Cybersecurity

Smith, John

Assignment 2

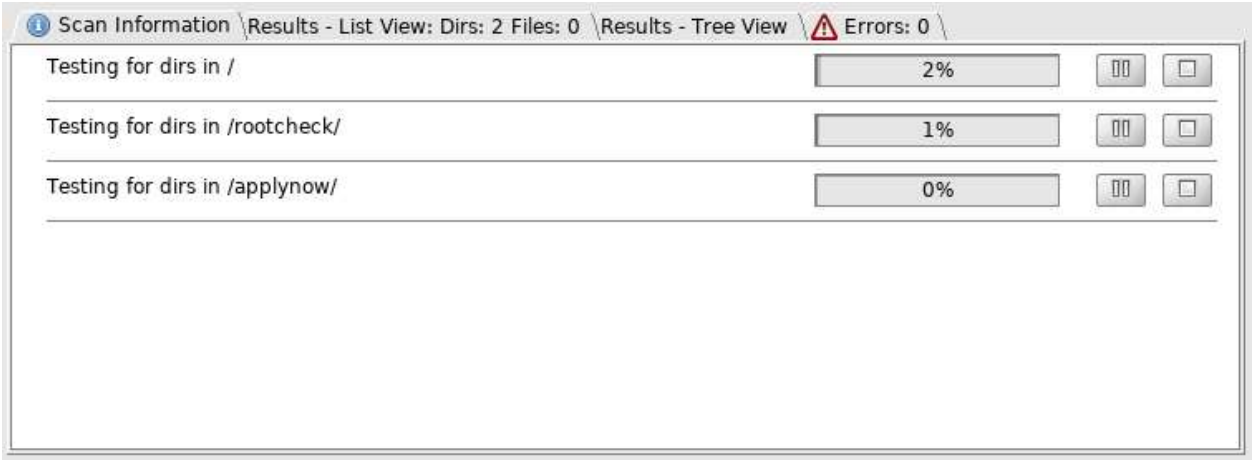
Dirbuster

Cybersecurity is a vast field focused on providing protection for everything on the web. As is often the case in cybersecurity, in order to protect against hackers, it helps to think like a hacker and use hacking tools. One of the most prominent targets for hackers is web application servers hosted by businesses and/or users. Of the many different methods that can be used to probe a server, the particular tool this paper will be reporting on is DirBuster. DirBuster can be dangerous, not because of any direct threat, but it can enable other more dangerous hacking tools. In cybersecurity, DirBuster is only a concern if a server has not been properly secured and has exposed directories or files that visiting users can access. This paper intends to explain what DirBuster is, how it works, provide an example of it in action and discuss its use cases and importance in cybersecurity.

While web servers may seem like a simple site, they contain files, directories, and scripts for running a website. This means that similarly to a computer, users can traverse a server if they know the different directories and file locations and if they have access. This fact allows hackers to create tools in order to learn about the file system that exists within a server, which is where DirBuster comes in. DirBuster is a file or directory reconnaissance tool that attempts to brute force directory and file names that may exist in a server (Awasthi, 2022). For hackers, both white-hat and not, it is used as an active reconnaissance tool to learn about the file system in place for a web server. If DirBuster is successful in finding additional links, it could then allow hackers to learn about the server and search for vulnerabilities that may exist.

DirBuster is a Java program created by developers in the OWASP community (Awasthi, 2022). In order to find the names, a word list is provided to DirBuster that it then spends testing different words and combinations of words in order to try and learn about the file system that exists in the server. These word

lists can be tailored to varying lengths depending on how vast of a search the hacker is performing and how much risk they want to take. DirBuster is also multithreaded which it takes advantage of in order to send multiple http or https requests with each name in the word list (Ibeankanma, 2022). This is part of the brute force method it uses, as DirBuster just continues sending requests and recording the response codes the server gives. DirBuster has several options the user can tweak, including to use only GET requests or switching between HEAD and GET requests, how many threads to use, whether to use list based brute force or just a pure brute force scanning type, and several starting options for specific directories to start, specific file extensions to search for, whether to brute force directories and files, to be recursive in its searching and whether or not to use blank extensions.



DirBuster being used in a hacking competition (Cosenza, 2020).

The above screenshot is an example of DirBuster being used in a hacking competition called the National Cyber League (NCL) Games. In these games, the students are given several different challenges that require knowledge of different hacking tools in order to find a flag. This example involves using DirBuster on a web server created by the NCL in order to find a flag. They use one of the prebuilt DirBuster wordlists in Kali Linux and a focus on searching for directories instead of files from the given web server url. The results of using DirBuster here are finding several flag#.txt files in different

directories spread throughout the given server. These flags act like points for the teams, where the goal is to find as many flags as possible within the given time frame.

While DirBuster can be used for unethical reasons by many hackers, it is mainly intended as a tool for learning and white-hat hacking. This is likely one of the many tools a white-hat hacker would use to attempt to penetrate a web server for a business or client that hired them. Additionally, this tool can be used by a programmer hoping to create their own web server in order to search for potential files and directories they may have left exposed to the public. In cybersecurity practices, knowing that DirBuster may be used by hackers in order to search for vulnerable directories and files allows developers and white-hat hackers to improve security by ensuring that guest users are not able to access these paths. Furthermore, since DirBuster sends repeated http or https requests, this can be used to monitor for a form of active reconnaissance that hackers may be using.

DirBuster is a powerful reconnaissance tool that allows users to learn about the file system that a web server has. While it is typically used as a learning tool or for securing web servers, it can certainly be used by hackers to search for vulnerabilities in a server. Since DirBuster is a popular tool, it has a lot of information online about it and how to protect against it, which helps new server developers better secure their own servers. In cybersecurity, knowing about DirBuster is just part of understanding how hackers perform active reconnaissance as there are several tools that also exist and many more that may be created. As these tools get better, the security needed to protect businesses and users on the web will need to get better.

Works Cited

Ibeakanma, Chioma. "What Is Directory Bursting and How Does It Work?" *MUO*, 19 Apr. 2022, www.makeuseof.com/what-is-directory-bursting/.

Awasthi, Arth. "Explaining DirBuster." Medium, FAUN-Developer Community, 1 July 2022, faun.pub/what-is-dirbuster-and-how-to-use-it-1db3c3d3113b.

Cosenza, Jeana. "A Beginner's Guide to Scanning with DirBuster for the NCL Games." A Beginner's Guide to Scanning with DirBuster for the NCL Games, 4 Mar. 2020, cryptokait.com/2020/03/04/a-beginners-guide-to-scanning-with-dirbuster-for-the-ncl-games/.

Young, Sid. "Directory Traversal Attacks - Beware Dirbuster • Conetix." Conetix, 23 July 2019, conetix.com.au/blog/directory-traversal-attacks-beware-dirbuster/.