# Transcript: C701 and C795 – Nmap Overview w/ Jenny Heiner

*The following transcript is a verbatim account of the video or audio file accompanying this transcript.*

Speaker: Jenny Heiner

WGU is IT audio series. Flexible, portable, profound.

Jenny

In this degree program, one of the many network discovery and security auditing tools you will use, is Nmap. Nmap is praised for its flexibility and which it supports dozens of advanced techniques. It is powerful, portable, easy, free, well-documented, and supported by a large number of users developers. It has also won numerous awards, including information security product of the year by Linux Journal, InfoWorld and Codetalker Digest.

Best of all, its capabilities are profound, which proves in its popularity. Thousands of people download Nmap every day. You may have noticed the tool is featured in the Matrix Reloaded, Die Hard 4, The Bourne Ultimatum and so many more great movies. But the movies are not the only publications Nmap has been showcased. It has also been referenced in magazines, books, and you might just find Nmap in one comic book series. Can you believe it?

Nmap celebrated its 24th birthday on September 1st, 2021, as Nmap was first released in Phrack Magazine Issue 51, September 1st, 1997. With its extensive reference guide and man pages, Nmap users are given all the resources needed to jump in and quickly learn this tool and all of its features. But Nmap isn't just a security tool, it offers the community. Significant effort has been put into the development of this Nmap community where white papers, tutorials, and an Nmap book are available to its users. You can also subscribe to the Nmap hackers mailing list, its development lists and if you're old school, visit the IRC channel and join the fun. You can also jump into this community visiting Nmap Facebook page, Twitter feed, or pull in an RSS feed. Even if you are a novice with Nmap, you can start default scanning minutes after you download the latest release.

It is always best to use the latest release because Nmap is constantly improving, improving on performance, adding new capabilities, and fixing any accidental bugs. Gordon Lyon, known as Fyodor, Nmap original author and the author of the Nmap book, extensively and eloquently describes how to install Nmap, host discovery techniques, port scanning, remote OS detection, how to optimize the performance of Nmap, the Nmap scripting engine, service and application detection, and Nmap output formats. Everything you ever wanted to know about Nmap is articulated in this book, and it is a fantastic read. You will also find figures and examples throughout which support the discussions. Even though this book is centered around everything Nmap, you will also learn what a port is, why to scan ports, common ports, most valuable ports and there is a script writing tutorial.

Another great aspect of this book is that it discusses how to defend against Nmap, like blocking the probes, restricting information returned, and returning misleading information. If you're not fond of a command line environment, Fyodor also discusses the Zenmap GUI users guide. This book will undoubtedly contribute to making you a better information security expert as it was designed to support users at all different experience levels. There are a number of great scanners out there, like Angry IP, ZMapp, Hping or Advanced Port Scanner. But Nmap has been a personal favorite of mine and here's why. I prefer the command line environment. The most common options, a summary is extensive and print it by just running Nmap with no switches. This makes it easy to use and the output is simple to interpret. The scans are robust and I can run several types of scans and save the output to a file for later parsing if needed. Some of my preferred scans are OS detection, using decoys, and having the ability to set my own timing. The future of Nmap is to handle web scanning and allow for users to scan their own systems from the Cloud. They also plan to internationalized Nmap by supporting many different languages and publishing a Wiki. There's also talks about a future web discussion forum. You can check out Nmaps to-do list, and read up on all the things they're working on right now.

Get started at Nmap.org and as always, whatever you intend to scan, be certain you have written authorization to do so.

Schedule time with your instructor to explore more deeply. WGU, a new kind of you.