0:00 Hello and welcome to this course in which we're talking about Python for pre-attack. Or more specifically, how we're going to be using Python scripts to achieve the reconnaissance tactic in the miter pre-attack section of the miter pre-attack framework. In this video, we're going to introduce one of the techniques we'll be using for reconnaissance, namely network scanning.

0:29 Knowledge of a target network is vital for an attacker because if they don't have information about the Systems Applications, etc, on a target network, they're working blindly to achieve their objective, and that can make achieving that objective much more difficult. For this reason, a vital part of the reconnaissance part of the miter attack framework is identifying as much information as possible about the target network architecture. Finding things that are potential target systems, for example, web servers running web applications, DNS servers, email servers, etc, identifying those Internet-facing services that could be a potential attack vector, and then looking for vulnerable applications. Maybe with our web application, looking to discover what type of CMS it might be running on, what type of content the website has, whether it's vulnerable to injection, cross-site scripting, etc, and so identifying how that particular application could be exploited and how it can be used in an attack. There are a variety of different methods for performing reconnaissance and learning about the target network architecture. Some examples of these include port scanning, where an attacker might use a tool like Nmap or create their own, to query each of the various ports on a computer on a target network and determine whether or not that port is opening and accepting data. If a port is open, the scanner might go on further to try to identify the application that's running on that particular port. One method for accomplishing this is the banner collection or banner grabbing. Many applications will print a banner stating information about themselves, for example, the SSH server, the software in use, version number, etc, and this sort of information is valuable both for learning what type of service is running on a particular port, but also the details of that particular surface. If you know that you're running a particular version of OpenSSH, you might be able to determine if that version has known vulnerabilities by consulting the CVE database. Alternatively, you can try to identify vulnerabilities in an application through vulnerability scanning. While you might picture this is targeted mainly at web applications, it can also be used for other services. For example, SMB was vulnerable to the eternal blue and other vulnerabilities from the Shadow Brokers leak, and so vulnerability scanning might involve sending eternal blue exploit packets to an SMB port to see whether or not a service listening there is vulnerable to eternal blue. In the active scanning or network scanning technique in the miter attack framework, there's a couple of sub techniques, scanning IP blocks and vulnerability scanning. The scanning IP blocks talk about looking at sections of the network and determining whether the IPs in that range are active, and if so, what type of computers are running on them, what services are running, etc. The other type of active scanning you might be performing for reconnaissance is vulnerability scanning, looking for those weaknesses in systems, listening on various ports to see whether or not any of those weaknesses may be exploitable. We're talking about network scanning here because we're going to be using Python and the Scapy library to develop a network scanner for reconnaissance as part of our discovery of how Python can be used to achieve miter attack techniques and tactics. Thank you.