Hello and welcome to this course on MITRE PRE- ATTACK. In this video, we're going to be talking about the section of the PRE-MITRE ATTACK framework that encapsulates the two techniques that fall under the PRE-ATTACK stages of MITRE ATTACK.

0:19 Let's start out with an introduction to PRE-ATTACK. The MITRE PRE-ATTACK matrix used to be its own stand-alone matrix under the general MITRE ATTACK framework. It like other matrices contained its own collection of tactics and techniques, and as we see in the image on this slide, it mapped primarily to the Recon and Weaponize stages of Lockheed Martin's cyber kill chain. Recently, the MITRE ATTACK framework underwent a bit of a redesign, and the PRE-ATTACK stages were incorporated into the enterprise matrix for the MITRE ATTACK framework. Now we have two tactics, reconnaissance, and resource development, that covers many of the same stages of an attack, as the previous standalone matrix. In this first stage of PRE-ATTACK, we're talking about network reconnaissance. This tactic and the techniques that fall under it are focused on information collection, trying to gather information about a target system in a variety of different methods. The techniques that fall under this particular tactic are listed here on this slide, so you can perform active scanning, where you interact with the organ, or with the target network, and try to learn about the systems and programs on it. There's also a variety of information that's gathered about victims, so information about victim hosts, victim identity, victim network, and victim organization. All of these have multiple sub-techniques under them, describing particular ways to collect this information. It's also the use of fishing for data collection rather than exploitation. Trying to learn information that could give hints about how an organization's network works, policies and procedures for security, etc. Then there's searching different sources of data, whether closed sources, open technical databases, open websites or domains, and victim owned websites. All of these are potential sources of information about an organization's network infrastructure, websites and other processes and users that are associated with this network. The other stage of the PRE-ATTACK section of the Mitre ATTACK framework is resource development. This particular tactic is focused on ensuring that the attacker has the tools, infrastructure, etc, that they require to achieve their goals. This includes steps like acquiring infrastructure, compromising accounts or infrastructure, developing capabilities, establishing accounts, and obtaining capabilities. It's essentially building up the back-end of the attackers' infrastructure so that they're able to execute attacks on any weaknesses that they've identified during the reconnaissance stage. Now let's talk about how we're going to use Python for PRE-ATTACK. It's important here to discuss what parts of the PRE-ATTACK stages we can actually implement via Python. The resource development tactic of PRE-ATTACK, largely occurs on the attacker's side and on the attacker's infrastructure, so there's not really much interaction with target systems for defenders to identify. The precise details about this resource development tactic depend heavily on the attacker's goals and the resources available to them. It could be that the resource development tactic requires nothing at all, could require significant expenditures of capital or a significant investment and infrastructure, and the details of that can vary greatly. For this reason, we're not going to be focusing on resource development when we're talking about Python for PRE-ATTACK. Instead, we're going to look at techniques from the reconnaissance tactic of PRE-ATTACK, investigating network scanning under the active scanning category, and then discussing DNS exploration, which is a subset of Search Open Technical Databases. In the next video, we'll start out with an introduction to network scanning. Thank you.