EXTRACTING INFORMATION FROM E-MAIL SERVERS

E-mail servers can provide a wealth of information for hackers and penetration testers. In many ways, e-mail is like a revolving door to your target's organization. Assuming your target is hosting their own e-mail server, this is often a great place to attack. It is important to remember, "You can't block what you must let in." In other words, for e-mail to function properly, external traffic must pass through your border devices like routers and firewalls, to an internal machine, typically somewhere inside your protected networks.

As a result of this, we can often gather significant pieces of information by interacting directly with the e-mail sever. One of the first things to do when attempting to recon an e-mail server is to send an e-mail to the organization with an empty .bat file or a nonmalicious .exe file like calc.exe. In this case, the goal is to send a message to the target e-mail server inside the organization in the hope of having the e-mail server inspect, and then reject the message.

Once the rejected message is returned back to us, we can attempt to extract information about the target e-mail server. In many cases, the body of the message will include a precanned write-up explaining that the server does not accept e-mails with potentially dangerous extensions. This message often indicates the specific vendor and version of antivirus that was used to scan the e-mail. As an attacker, this is a great piece of information to have.

Having a return message from a target e-mail server also allows us to inspect the headers of the e-mail. Inspecting the Internet headers will often allow us to extract some basic information about the e-mail server, including IP addresses and the specific software versions or brand of e-

mail server running. Knowing the IP address and software versions can be incredibly useful when we move into the exploitation phase.