CERT Incident Note IN-98-06: Automated Scanning and Exploitation

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Automated Scanning and Exploitation

Wednesday, December 9, 1998

The CERT Coordination Center has received reports of intruders executing widespread attacks using scripted tools to control a collection of information-gathering and exploitation tools. The combination of functionality used by the scripted tools enables intruders to automate the process of identifying and exploiting known vulnerabilities in specific host platforms.

One scripted tool we are aware of uses a port scanning tool to perform widespread scanning to identify hosts responding on TCP port 111 (portmapper). This functionality is similar to the widespread scanning activity discussed in CERT Incident Note IN-98.02:

http://www.cert.org/incident_notes/IN-98.02.html

The scripted tool then uses an advanced scanning tool to attempt to identify the operating system architecture of hosts identified in the widespread scanning. The scripted tool looks for hosts identified to be running Linux. This functionality is similar to the advanced scanning techniques described in CERT Incident Note IN-98.04:

http://www.cert.org/incident_notes/IN-98.04.html

For each host identified as responding on TCP port 111 and appearing to be running Linux, the scripted tool uses an exploit tool to attempt exploitation of the mountd vulnerability described in CERT Advisory CA-98.12:

http://www.cert.org/advisories/CA-98.12.mountd.html

If the exploit tool is successful in gaining privileged access to the host, the exploit tool executes a series of shell commands to provide the intruder with a passwordless privileged account.

The scripted tool then logs the hostname of each compromised host to a file.

Conclusion

To help protect your systems from the various automated tools being used by the intruder community, we urge you to ensure that all machines in your network are up to date with patches and properly secured.