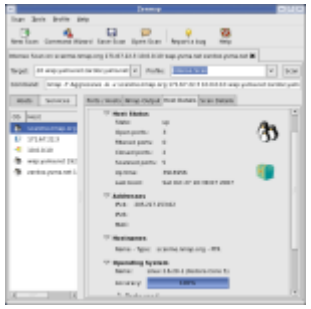
Nmap Security Scanner
- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists
- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools
- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More

Site News
Advertising
About/Contact

Site Search



Intro | Reference Guide | Book | Install Guide
Download | Changelog | Zenmap GUI | Docs
Bug Reports | OS Detection | Propaganda | Related Projects
In the Movies | In the News

Nmap Network Scanning

Detect Nmap Scans

Chapter 11. Defenses Against Nmap

Detect Nmap Scans

Some people believe that detecting port scans is a waste of time. They are so common that any organization connected to the Internet will be regularly scanned. Very few of these represent targeted attacks. Many are Internet worms endlessly pounding away seeking some Windows vulnerability or other. Some scans come from Internet research projects, others from curious or bored individuals exploring the Internet. I scanned tens of thousands of IPs seeking good examples and empirical data for this book. Other scans actually are malicious. Script kiddies regularly scan huge ranges for systems susceptible to their exploit du jour. While these folks have bad intentions, they are likely to move along on their own after finding no vulnerable services on your network. The biggest threat are attackers specifically targeting your organization, though those represent such a small percentage of detected scans that they are extremely tough to distinguish. So many administrators do not even bother recording port scans.

Other administrators take a different view. They contend that port scans are often precursors to attacks, and should at least be logged if not responded to. They often place detection systems on internal networks to reduce the flood of Internet port scan activity. The logs are sometimes analyzed for trends, or submitted to 3rd parties such as Dshield for world-wide correlation and analysis. Sometimes extensive logs and scary graphs measuring attacks are submitted to management to justify adequate budgets.

System logs alone are rarely sufficient for detecting port scans. Usually only scan types that establish full TCP connections are logged, while the default Nmap SYN scan sneaks through. Even full TCP connections are only logged if the particular application explicitly does so. Such error messages, when available, are often cryptic. However, a bunch of different services spouting error messages at the same time is a common indicator of scanning activity. Intrusive scans, particularly those using Nmap version detection, can often be detected this way. But only if the administrators actually read the system logs regularly. The vast majority of log messages go forever unread. Log monitoring tools such as Logwatch and Swatch can certainly help, but the reality is that system logs are only marginally effective at detecting Nmap activity.

Special purpose port scan detectors are a more effective approach to detecting Nmap activity. Two common examples are PortSentry and Scanlogd. Scanlogd has been around since 1998 and was carefully designed for security. No vulnerabilities have been reported during its lifetime. PortSentry offers similar features, as well as a reactive capability that blocks the source IP of suspected scanners. Note that this reactive technique can be dangerous, as demonstrated in the section called “Reactive Port Scan Detection”.

Despite being subject to threshold-based attacks discussed in the section called “Avoiding Intrusion Detection Systems”, these port scan detection tools work pretty well. Yet the type of administrator who cares enough to keep tabs on port scans will also want to know about more serious attacks such as exploit attempts and installed backdoors. For this reason, intrusion detection systems that alert on a wide range of suspicious behavior are more popular than these special-purpose tools.

Many vendors now sell intrusion detection systems, but Nmap users gravitate to an open-source lightweight IDS named Snort. It ranked as the third most popular security tool among a survey group of 3,243 Nmap users (http://sectools.org). Like Nmap, Snort is improved by a global community of developers. It supports more than two thousand rules for detecting all sorts of suspicious activity, including port scans.

A properly installed and monitored IDS can be a tremendous security asset, but do not forget the risks discussed in the section called “Subverting Intrusion Detection Systems”. Snort has had multiple remotely exploitable vulnerabilities, and so have many of its commercial competitors. Additionally, a skilled attacker can defeat most IDS rules, so do not let your guard down. IDSs too often lead to a false sense of security.


Block and Slow Nmap with Firewalls


Clever Trickery