SecTor: Old Security Vulnerabilities Live On

Security researcher identifies security vulnerabilities from the 1990s that still persist today.

By Sean Michael Kerner | October 02, 2012

TORONTO: The more things change, the more things stay the same.

At the SecTor security conference in Toronto, Jamie Gamble, security researcher at Accuvant, detailed how old security issues that first surfaced in the 1990s remain security concerns today. Gamble's talk, titled "The More Things Change: The Vulnerabilities that Time Forgot," included issues related to trust, networking and system configurations in Windows and Unix machines.

Trust lies at the root of many of Gamble's vulnerabilities.

"Machines trust each other and because of that you still find interesting vulnerabilities," Gamble said. "We're still lousy at network segmentation, VLANs have not solved the problem, and segmenting users from each other is still hard."

When everything on the network is trusted, unauthorized users get access to items they shouldn't be allowed to access. VLANs segment a network to a degree, though Gamble argued that most system administrators don't properly configure for proper role-based access control.

Password Problems

The issue of weak passwords has existed since the beginning of the computing age.

"People still pick bad passwords," Gamble said. "If you have a policy that forces people to have more complex passwords, they just pick passwords that look secure - but aren't."

Another issue that has existed since the 1990s are systems that allow users to login with password hashes. A password hash is a way to obfuscate a password. Gamble said if a system enables logins with a hash, then it is as insecure as a clear text password.

Password security is also an issue on Unix-based machines that use NIS or LDAP for network authentication. Gamble noted that with NIS, an attacker could simply run the command "ypcat password" to get a list of user directory passwords. LDAP is slightly more secure, although not perfect, he said.

"If you have Solaris running openLDAP, you can't do ypcat passwd to get the hashes," Gamble said. "But other simple methods exist."

Man in the Middle Attacks

Man in the Middle (MiTM) attacks are also a relic from the 1990s that are still effective. In a MiTM attack, an attacker sits in the middle of a connection stream and intercepts data and passwords. While data transport should be secured with proper SSL certificates, Gamble noted that many people still accept connections with

bad certificates.

He added that there are programs like dsniff,urlsniff, sslsnarf and ettercap that enable MiTM and sniffing of network connections. With new interfaces such as Easy-Cred, which is bundled in the Backtrack Linux security distribution, Gamble said it's now easier than ever before to carry out an attack.

SMB Attacks

SMB is the common protocol used for Microsoft file and print server connectivity. Back in 2001, Sysinternals released the Windows Server PSexec tool, which allows users to execute a command on a Windows Server via SMB. Gamble explained that while the tool was originally built for legitimate purposes, it has since been included in the open source Metasploit penetration testing framework, allowing for easy exploitation of Windows.

"You can't patch it," Gamble said about the technique. "It's a design flaw."

Rogue SMB servers are another SMB flaw that has been around since the late 1990s. Gamble explained that if an attacker sets up a rogue SMB server, it automatically grabs password hashes. "That's not new and it's just something that has not yet been fixed," Gamble said.

Insecure NFS Services

NFS is the Unix equivalent of SMB on Windows. According to Gamble, NFS is also a great way to share and exploit the home directories of users.

"It really just comes down to how NFS is setup and configured but there is no good guide out there on how to do it," Gamble said.

Privilege-based flaws are also common and have been for more than 15 years. Gamble said that on Unix-based systems in particular, many admins simply don't know how to properly set up permissions. Gamble suggests that security professionals check the /usr/local/bin and usr/local/sbin directories for third-party applications on a Unix machine. It's likely they will find insecure applications with permissions they don't need.

History Files

Another old flaw that continues to persist and be exploited has to do with history files on Unix systems. Gamble noted that history files are typically readable by anyone on the system.

"Who hasn't typed a password on the command line once or twice?" he said.

If that password was typed on the command line and not at the proper prompt, it could be saved in the history file, enabling an attacker to simply retrieve it. "These files should never be readable by other users," Gamble said.

As to why old vulnerabilities and issues continue to persist, Gamble suggested that modern security vulnerability scanners don't go far enough. In his view, they don't provide the context for what a vulnerability means and thus do not provide a full picture of risk.

So what is the fix? According to Gamble, it's more education and proactive auditing.

Sean Michael Kerner is a senior editor at InternetNews.com, the news service of the IT Business Edge Network, the network for technology professionals Follow him on Twitter @TechJournalist.