In this series of three articles, Mark Fischer <mailto:Mark.Fischer@SecurityGuild.com>, a student in the first cohort of the Norwich University MSIA (Master of Science in Information Assurance) program, has very kindly consented to share one of his essays with readers of this newsletter. The topic in that particular week was penetration tests, and Mr Fischer continues this time with how he and his colleague penetrated their client’s networks.

* * *

The goals of our network attack were to start with only physical access to the network and attempt to gain access to their mainframes and selected NT and Novell servers. Our Rules of Engagement required us to consult with our point of contact after we identified possible targets so he could tell us which ones to focus on and which to avoid. This was done to prevent us from accidentally damaging their production systems and to help us focus on the most important servers. They had scores of NT servers and attacking all of them would take too much time (and money) so we worked with the client to focus on the ones that would provide the most value.

* Novell *

They had a Novell NDS tree with containers for each business unit. It was a legacy system used primarily for file and print services. Using standard tools like Pandora and CheckNull we were able to gain admin access to Novell system within a few hours. It was of limited practical value because almost no valuable information was stored on the Novell servers. We had control of the system, but it did not get us closer to the “crown jewels” we were after.

* Windows NT *

Acme was migrating to a Windows NT network and had a number of interesting applications running on them, including Internet Information Server (IIS) web servers, SQL Server database servers, and some specialized application servers. There was a large domain for file and print services, though not all of the servers were members of the domain.

We began with the domain controller. We were able to enumerate all the accounts and found a couple of accounts with trivial passwords (blank or same as the username). Unfortunately, they were all normal user accounts, not Administrator accounts. We enumerated more than a dozen Administrator accounts, but all had decent passwords on them.

We repeated the light reconnaissance procedure against the IIS and SQL servers and found that all the passwords on the servers were pretty good. No easy access this way. One of the intranet web servers was vulnerable to the Remote Data Services (RDS) vulnerability made famous by Rain Forest Puppy (rfp). We were able to dump the SAM and crack all of the passwords on that
One administrator account had the same password on all the web and SQL servers and we were able to gain control over all of them.

Unfortunately, that password was not the same as any of the domain admin passwords so we had to work another angle to get in there. Next we took a look at a server called W2KTEST, a Windows 2000 Server being tested by the IT staff. It was a stock W2K server running IIS 5.0, SMTP, etc. We dumped the accounts and found a local Admin account with a blank password, dumped the SAM and cracked the rest of the passwords. We found one username/password combination from W2KTEST that also worked on the domain. It was an admin account on the domain and with it we were able to dump the SAM and crack all of the passwords on the domain. Success!

* The Mainframe *

We reported our success with the web and SQL servers and the domain controller to our point of contact. We also wanted to talk to him about how we could use that information to go after the mainframe. Our plan was to install software keyboard taps on selected computers to capture people’s mainframe passwords when they logged on using a 3270 emulator.

After a few hours of discussion on the subject over dinner we decided not to pursue that angle. Our contact had decided that he was comfortable that the approach would likely work but didn’t want to assume the risks of us actually doing it. The mainframes were their lifeblood with tens of billions of dollars of policy information. Our contact pointed out that if we were to inadvertently cause a problem it would be his head on the chopping block and the entire security program would suffer. We all agreed that the prudent and professional thing was to leave the mainframe alone.

* * *

Next time: social engineering.

* * *

Mark Fischer < mailto:Mark.Fischer@SecurityGuild.com > is the founder and Managing Director of Security Guild, LLC, an information security consulting company. He is a Certified Information Systems Security Professional (CISSP) and a graduate of the Rochester Institute of Technology. He has been building and breaking systems and networks for more than 15 years.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information
Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 Mark Fischer. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.