Global Information Assurance Certification Paper

By: Paul W. DePriest
GSEC Practical Assignment Version 1.2b

The Importance of the Ramen Worm

As Linux becomes a more popular choice, we can expect the quantity and severity of attacks on Linux systems to increase. This means that those of us administering Linux systems need to pay detailed attention to security. It is no longer just a Microsoft Windows problem. The attackers will not leave us alone. Just look at the Ramen worm. This paper describes the Ramen worm, explains how to detect it, how to "clean up" after it and finally why this attack is significant (lessons we should learn).

What is the Ramen Worm?

On January 18, 2001 the Global Incident Analysis Center (GIAC) reported the existence of the Ramen worm. The Ramen worm consists of generally available hacking tools that have been put together to infect Red Hat Linux systems that have not been properly secured. It is believed that this was the work of script kiddies since it only attacks known vulnerabilities. The developers of this worm did modify some of the tools they used. In particular, the scanner they used is a modified version of the synscan program.

In short, the Ramen worm takes advantage of numerous well-known flaws of Linux servers using the default installation options of Red Hat Linux. It appears that both versions 6.2 and 7.0 are vulnerable to attack. The worm is able to identify these by using their release dates. The Ramen worm is somewhat intelligent in its attacks in that it customizes the attack based on the particular version of Red Hat Linux it finds. For version 6.2, it will use the RPC.statd and wu-FTP flaws. For version 7.0, the worm tries to compromise the system by swamping the error logging function of the system's printer service with data. When the Ramen worm gains access, it installs a root kit that patches the security holes and installs new software that replace common system functions and replace the main page on Web servers with a Ramen provided HTML file. Finally the "new" copy of the Ramen worm sends an e-mail to two Web-based accounts, boots up, and starts scanning the Internet again.

When Ramen is scanning, it uses simple methods to determine which systems to attack. For example, when Ramen is scanning port 21, FTP, it records the response of the potential target. The FTP banner that is transmitted by the target system is analyzed to see if it contains a particular date. If it does, then Ramen executes a propagation script based upon what vulnerability it believes might be present in the target system. When doing this, it does not stop scanning. It performs both processes in parallel.

Once in the target system, Ramen creates a working directory for itself, namely /usr/src/.poop. Next Ramen requests a copy of itself, ramen.tgz, from the attacking system using the Linux Web browser and the Web-like service it installs on compromised systems. Ramen uses TCP port 27374 for this purpose.

Next Ramen performs a global search and replace of all files named index.html. (Be aware that the contents of the Ramen version of this file vary. The individuals distributing this worm are continually refining what the Ramen worm does to the target system.) Then Ramen disables existing FTP services and disables rpc.statd so that this system will not be infected again.

An interesting aside is that Ramen is extremely efficient in scanning for targets. Ramen does nothing to control network traffic and will consume a significant amount of network bandwidth. The scanning is extremely fast. According to an interview of Mihai Moldovanu, a Romanian network administrator, in a ZDNet News story, dated January 23, 2001 written by Robert Lemos, "the Ramen worm scanned two B-class networks (about 131000 IP addresses) in less than 15 minutes." Obviously, the Ramen developers have targeted specific vulnerabilities to look for and can thus minimize the scan time. Another interesting fact about Ramen is that it does not try to hide itself and does not appear to do anything in a stealthy manner.

We need to all remember that the Ramen worm can be extended by just adding new exploits to the Ramen toolkit as they become available. This allows the Ramen worm to "stay current" and remain a threat to Linux systems as new vulnerabilities are found.

Detection of the Ramen Worm

Due to the Ramen worm not trying to hide, it is easy to detect. The visible signs that a system has been compromised are listed in CERT Incident Note IN-2001-01 Dated January 18, 2001. These signs include:

- The Ramen toolkit is installed in the "/usr/src/.poop" directory.
- All "index.html" files are replaced with a Ramen provided "index.html" file.
- The system file "/etc/hosts.deny" is deleted.
- The file "/usr/src/.poop/myip" is created and contains an IP address of the local system.
- A script is added to the end of "/etc/rc.d/rc.sysinit" to initiate scanning and exploitation during system startup.
- Usernames "ftp" and "anonymous" are added to "/etc/ftpusers"
- A service named "asp" is created using TCP port 27374.

For other details, please read the above-mentioned CERT IN-2001-01 article.

Another sign that you may be under an active attack is that you experience a time of little or no bandwidth on the network or on your Internet link. Also, if you are on a network utilizing multicast, the scanning that Ramen does could cause network problems to surface. As always, any anomalous activity should raise a red flag for you or your system administrator to take action and analyze the situation.

Eradication of the Ramen Worm

In order to minimize the spreading of this worm, the GIAC put out a warning to turn off LPRng and disable wu-ftpd if you are running Linux on January 18, 2001. The GIAC further indicated that if either service needed to be run that you should apply all patches and run the latest versions of each. The GIAC also put out a request for someone to develop a script that would help system administrators in determining if their systems were infected.

As a result of the GIAC request, on January 23, 2001 Mr. William Sterns of ISTS at Dartmouth College responded with a script that could detect the existence of the Ramen worm. Initially, this tool, entitled ramenfind, was being distributed via email. Now ramenfind can be downloaded from several sites. I chose to use www.packetstorm.securify.com/distributed/indexdate.shtml. At this site, there are 2 versions of the ramenfind script, 0.3 and 0.4. Ramenfind seems to work fine when I have executed it on my own systems. In addition, Mr. Stern has included tests for some variations of the Ramen worm.

If you want to test your Linux system for the Ramen worm, just download and execute the ramenfind script. Remember that you will have to modify the file permissions to include execute before you can run the ramenfind script.

For those system administrators that want to rid your systems of the Ramen worm manually, perform the following steps :

- Delete /usr/src/.poop and /sbin/asp
- Delete /etc/xinetd.d/asp if it exists
- Remove all lines in /etc/rc.d/rc.sysinit that refer to any file in /etc/src/.poop.
- Remove all lines in /etc/inetd.conf that refer to /sbin/asp.
- Reboot the system.
- Do not enable ftp, rpc.statd, or lpr until the current patches have been installed.

Please remember that the above signatures are for the initial version of the Ramen worm. As the Ramen worm evolves in what systems are attacked and what the results of the attack are, the signatures of the worm will likely change as well.

Finally, be aware that the Ramen worm is driven by scripts that can be easily modified to attack other versions of Linux or other UNIX systems. We should make sure that we follow good security practices on all of our systems, especially the Linux and UNIX systems.

Significance of the Ramen Worm Attack (Lessons Learned)

Personally, I have learned several lessons from the Ramen worm. The most important delusion I had was that if you used a commercial distribution of Linux like Red Hat, that

you didn't need to be as concerned about security patches. I also believed that using the latest distribution would minimize your risk without doing anything else. As this worm has shown, both of these ideas were just plain wrong. The commercial distributions of Linux are just a staring point and one must perform several tasks in order to be secure. From just the Ramen worm attack, I am going to be more pro-active in:

- installing all security patches
- only running services that are needed
- read and study the SANS digest to keep current with the latest attack
- make security a priority
- never depend on the distribution to represent a secure installation

I realize that the above is a reaction to a problem, but I'm sure that others of you have fell into the same trap. You are directed to get a system up and running in very little time. Something has to give, and it is usually security. I have learned over last several months that if you can ever get up to date with patches on the services that your systems must provide, you can keep them current and minimize your risk.

Concerning the Ramen worm itself, I like the idea of the worm patching the security holes so that the system is not re-infected. It seems to me that this would be a good idea on possibly how to secure Linux systems in the future. If done properly, it seems on the surface that this would result in a very secure network if a tool like this were run periodically on your network. This way you would catch any new unpatched systems that found their way to your network automatically.

An interesting view is presented in an interview of Lance Spitzner, coordinator for the Honeynet Project (a group of well-known security experts who study how hackers attack servers) by Robert Lemos in ZDNet News, dated January 23, 2001, :

> "The worm is dangerous in that it is an automated tool that exploits widely known vulnerabilities," said Honeynet's Spitzner. "Since it is automated, it can quickly scan for and exploit vulnerable systems at an exponential rate (that makes) the most dangerous element of this worm bandwidth consumption." Spitzner also said the worm could have been far more dangerous. "It leaves very easy-to-identify signatures on the compromised system, making it very simple to find. It appears to do little damage to the system itself, only replacing a Web page and creating a small Web instance for self-replication."
>
> Ironically, the Ramen worm could make the Internet more secure, said Honeynet's Spitzner. "It even secures the systems by eliminating the same vulnerabilities it used to exploit the system," he said. "I have seen far more destructive acts than this by the black hat community."

Based on the above comments, it appears that we all may have been given a "second chance" to secure our systems and networks. Mr. Spitzner is correct in that the developer of the Ramen virus could have been very destructive. The Linux community was fortunate this time, but what if the Ramen worm mutates into a destructive strain? By then, I hope that all of our systems will be secure and that we are all adhering to best security practices of the day.

In addition, because of the Ramen worm, I would hope that the vendors producing the various Linux distributions will take notice and provide us with a secure distribution of Linux. At a minimum, we should be made aware of tools and services that are provided with a distribution that are outdated or are unpatched. In addition, I would suggest that the vendors deactivate most services by default. This alone would have limited the effects of the Ramen worm because most systems do not need to be set up as FTP servers. Nevertheless, we can't place all the blame on the distributors. Most Linux systems that I manage have other software installed on them that did not come from the Linux distribution. We should keep all software on the system up to date. On a positive note, I was able to locate one vendor, E-Smith Inc., who takes the Red Hat distribution of Linux as a starting point and modifies it. According to E-Smith, Inc., their customers are not vulnerable to the Ramen worm. I trust that other Linux Distributors will follow suite.

As a final word, please remember that you are responsible for the security of your systems and that they are only as secure as you make them. You also must remember that the environment we operate in is continually changing and we must all be proactive and diligent concerning the security of our systems.

References:

1.Dratch, Sharon. "The Ramen worm: Not a Problem for E-Smith Users." E-Smith, Inc.18 January 2001. URL: http://www.esmith.com/article.php3?sid=27&mode=threaded&order=0 (01 March 2001)

2.Feamow, Matt. "SANS GIAC Detects Summary." SANS/GIAC. 18 January 2001. URL: http://www.sans.org/y2k/011801.htm (15 February 2001)

3.Feamow, Matt. "SANS GIAC Detects Summary." SANS/GIAC. 23 January 2001. URL: http://www.sans.org/y2k/012301.htm (15 February 2001)

4.Houle, Kevin. "CERT Incident Note IN-2001-01." CERT Coordination Center. 18 January 2001. URL: http://www.cert.org/incident_notes/IN-2001-01.html (16 February 2001)

5.Lemos, Robert. "Net Worm Hobbles Linux Servers." ZDNet News. 23 January 2001. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2675147,00.html (16 February 2001)

6.Steams, William. "Ramenfind, Ramen Worm Detection and Removal Tool." Beyond Security, Ltd. 12 February 2001. URL: http://www.securiteam.com/tools/Ramenfind__Ramen_Worm_detection_and_remova

l_tool.html (04 March 2001)
7. Steams, William. "Ramen Worm." SANS/GIAC. 15 February 2001. URL: http://www.sans.org/y2k/ramen.htm (15 February 2001)
8. Warfiled, Michael. "The Ramen Linux Worm is Propagating." Beyond Security, Ltd. 22 January 2001. URL: http://www.securiteam.com/securitynews/The_Ramen_Linux_Worm_is_Propagating.html (01 March 2001)

Last Updated: May 22nd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event