Jameel Alsalam
Somnath Banerjee
Grant Musick
Rares Saftoiu

CSE P 590TU / UC Berkeley PP 190/290-009 / UCSD CSE 291

One-page summary of topic:

A rootkit is loosely defined as one or more computer programs that let an outside party control what the administrator of a computer system sees on that system. Although usually harmless in and of themselves, they allow an outside party to effectively control or monitor a computer system.

Our paper will detail the types of rootkits in existence for Windows, Linux, Unix and OSX, how they get deployed to a computer system and the types of activities they hide from that system's administrator. We expect it will mostly focus on the user of device driver rootkits since these seem to be the most common ones these days.

In the paper we will also discuss the types of losses that can occur when a system has been compromised by a rootkit in the home and in the enterprise environment. It will include a discussion of privacy issues, financial losses and co-opting systems for attacks on other computer networks. It will also discuss how it can be used to slip through the security on other systems because of a trusted relationship one computer has with the next.

We will examine ways to prevent a rootkit from being deployed or how to minimize the damage once it has made it onto a system. This will include anti-virus softare, firewalls, intrusion detection programs and the various utilities in existence that attempt to check for these programs. It will also discuss whether technology can replace end-user knowledge to avoid this problem.

And, lastly, it will discuss how cost effective each of these countermeasures are. What it would cost to make our systems totally safe from this exploit and what is actually feasible.

Work division and schedule:

Chief Editor: Grant

Describe the threat (due 11/16)
Grant Musick

Assess current vulnerabilities (due 11/16)

Somnath Banerjee and Grant Musick

Assess possible losses in an attack (due 11/23)
Somnath Banerjee and Jameel Alsalam

Present possible responses (due 11/30)
Rares Saftoiu

Evaluate cost effectiveness (due 11/30)
Jameel

Final editing and assembling of paper(due 11/07)
Grant Musick

Guess-timate for work in each section and minimum number of pages:

Describe the threat
* Generic description of what is a rootkit
    - 1 page

Assess current vulnerabilities
* Windows vulnerabilities (2k/2k3/XP/64-bit)
    - 1 page
* Linux vulnerabilities (2.2/2.4/2.6)
    - 0.5 pages
* Unix vulnerabilies (AIX/HPX/FreeBSD)
    - 0.5 pages
* Mac vulnerabilities (OSX variants)
    - 0.5 pages

Assess possible losses in the event of an attack
* Windows
    - Home users
        - 1 page
    - Corporate users
        - 1 page
* OSX
    - Home users
        - 1 page
* Linux/Unix

- Corporate users
    - 1 page

Present possible responses
* Home users
    - Windows
        - 0.5 pages
    - OSX
        - 0.5 pages
* Corporate users
    - Windows
        - 0.5 pages
    - Linux
        - 0.5 pages
    - Unix
        - 0.5 pages
    - OSX
        - 0.5 pages

Evaluate the cost effectiveness of each
* Home users
    - Windows
        - 0.5 pages
    - OSX
        - 0.5 pages
* Corporate users
    - Windows
        - 0.5 pages
    - Linux
        - 0.5 pages
    - Unix
        - 0.5 pages
    - OSX
        - 0.5 pages

Summary
* Summarize findings
    - 1 page

Minimum total pages: 14.5

Possible questions for this topic:

1) What is a rootkit?
2) How does a rootkit work?
3) Which operating systems/platforms are vulnerable to a rootkit?
4) When are rootkits used?
5) Who uses them?
6) Where do they come from?
7) What proportion of the attacks are from rootkits?
8) Why do people use them?
9) How much of a security violation is it to have one installed?
10) Can they be stopped?
11) Are they an intrinsic vulnerability of existing platforms?
12) What kind of damage can be done with a rootkit?
13) Are there legitimate uses for a rootkit?
14) Which laws do rootkits violate?
15) How easy/hard is it to create a rootkit?
16) Is it ethical for a third party to hide files on your computer system?
17) What equipment/knowledge is required to create a rootkit?
18) ...

Useful Link:

http://en.wikipedia.org/wiki/Rootkit

Random Notes:

There are the obvious attacks where somebody puts a rootkit on your system
to hide their presence from you, but there are also ways a hacker can exploit this by changing his/her system to keep 3rd parties interested in fairness from detecting cheats. For instance, there were reports of people using the Sony sys DRM scheme to cheat at World of Warcraft by hiding bot programs.