A New Look at Security Education: YouTube as YouTool

Laurie Werner
wernerla@muohio.edu

Charles Frank
frank@nku.edu

Department of Computer Science,
Northern Kentucky University
Highland Heights, Kentucky 41099 USA

Abstract

Teaching a computer security course which includes network administration and protection software is especially challenging because textbook tools are out of date by the time the text is published. In an effort to use lab activities that work effectively, we turned to the internet. This paper describes several resources for teaching computer security found on YouTube. We describe the media that worked well in the class/lab environment, and present some ideas for evaluating the YouTube materials. Using this popular web site has the added benefit of engaging students in computer security in an entertaining way.

Keywords: computer security, port scanner, YouTube, intrusion detection, password cracker, packet sniffer, security education, security tool

1. Introduction

Software security tools are an important part of a computer security course as well as a necessary component of the career preparation for a security professional. Software tools are used for defense of computer systems and for learning how attackers use them to gain unauthorized access to computer systems. Vulnerability and penetration testing, port scanning, trap and trace simulations are just a few of the hands-on activities that students work with in a computer security course. (Frank, 2009)

Skoudis and Liston (2006) offer a sufficiently thorough presentation of hack and defend software for a Securing Computer Systems course. They approach a broad range of security tools utilized during different phases of computer attacks and defense. This favorably reviewed volume is excellent for familiarizing students with a career-style resource. It can provide a practical central text. However, as educators, we are left with designing hands-on exercises based on practical information that will work in class. Designing and testing pedagogically meaningful laboratory activities for a computer security course is like chasing a moving target for several reasons. One is that any book we select for a security course is outdated before it is published. A second reason is that a security update on Wednesday can render a lab activity ineffective on Thursday. A third is that the security tool will change significantly, shortly after you write your lab activity and test it, or worse, be unavailable for download when lab time comes. Thus, we must adjust our approach to the lab practicum portion of a security course, and consider it a continuing journey rather than a destination. In the remainder of this paper, we present some ideas for enlivening this journey with a resource that our students

are likely to be far more familiar with than we are, YouTube (2009). Considering that YouTube is the world's most popular video sharing site (Rutledge, 2008), we decided to investigate it as a vehicle for computer security instruction.

2. YouTube as *YouTool*

A text or trade book can describe security tools in operation, and provide the rationale and benefit of a security tool. We educators can demonstrate the tools in class. We often do so in teaching security, especially where a tool is dangerous in the hands of students, or where the computing environment is not amenable to running it. An alternative to or enrichment for prepared security lab activities and in-class demonstrations is finding YouTube (2009) videos that illustrate the security tools in action. The YouTube videos range from professional to amateur. We can play a video in class and follow with discussion, or students can preview a video prior to working in lab, and testing the features the video presents.

A simple YouTube search for a particular security tool yields both relevant and irrelevant links. Amongst pertinent links, some videos will be poorer quality. Computer screens shown in the video may be illegible. The audio may be defective. The pace may be too rapid to follow. Some videos are sales pitches. A few are of hackers boasting about their alleged prowess. Yet some videos present a security professional applying a specific tool in an environment that would take a lot of time and effort to replicate in a lab setting.

The remainder of this section describes videos we have found appropriate for teaching about seven well-known computer security tools. Their quality ranges from excellent to superior.

Honeynets

The original idea to use videos in teaching computer security occurred to us when we were developing an activity to describe the function of and rationale for creating a honeypot. Skoudis and Liston (2009) portray a honeypot as a "sacrificial host designed to attract and distract attackers." A honeynet is a network of honeypots.

Our universities would not allow us to set up a honeypot for security and legal reasons. We actively discuss the legal issues surrounding honeypots in class, spurred on by Spitzner's (2002) long term experience in the honeynet project (2009), so that students understand the gravity of participating in a honeypot. We used Google to search for honeypots and found the video Honeynet Web (2009) produced by the Honeynet Project (2009). We assigned our students to view this video and to answer questions about honeynets. This video is entertaining while being informative. It stimulated our appetite for more videos, and piloted us to a YouTube security tool search.

Nmap

The nmap website (2009) provides free and open source port scanning software. Nmap is available in Windows and UNIX versions. Skoudis and Liston (2006) describe nmap in 25 pages of detail. We found only two suitable videos on YouTube which describe nmap. *NMAP port scanning tool* (2009) is a short introductory video by a Cochise College instructor that demonstrates installing and running nmap in a Windows environment. A nine minute video, *EXCELLENT How to use nmap* (2009), introduces two types of port scans and operating system fingerprinting with nmap. This video has background music and provides a description of a few command line flags and their meaning. Many users gave it five stars.

Netcat

Netcat is often used for file transfer between the attacker and a victim's computer**.** Skoudis and Liston (2006) devote 20 pages to netcat, illustrating an assortment of ways to use it. The YouTube video *Hacking and Your Computer Penetrate Your Own Network* (2008) demonstrates installing netcat on a Windows system. At this writing, the URL provided in this video contains no netcat software, but it can be found at the Netcat (2004, 2006) ftp sites. *Netcat Tutorial* (2008) provides a short demonstration of the tool at the Windows command line. In both videos, netcat listens on a port and opens a command window backdoor for an attacker.

There were other netcat videos on YouTube, but they were either not in English or of poor quality. Since netcat is often referred to as the Swiss Army knife of network tools, and in 2006 was ranked the 4th most popular tool

in a survey run by Insecure.org (Lyon, 2006), it is unfortunate that there are not more in-depth videos of such an important tool.

Snort

Snort (2009) is a widely used open source network intrusion detection tool. Snort is rule-based, which is a different implementation than students see in the aforementioned tools. We found three videos to introduce Snort to students. *Snort IDS with Kevin Rose* (2008) is a six minute introduction to IDS and Snort. *How to install and configure SNORT on an XP machine* (2008) shows how to install, configure, and run Snort. This video is rather fast paced and lasts ten minutes. Students can replay it as often as desired. The video *How to create a SNORT rule and test it* (2008) experiments with Snort's detection of nmap (2008) FIN and XMAS scans. Additionally, it programs a snort rule to alert for someone visiting www.youtube.com. This clever video astutely connects the port scanner nmap with the intrusion detection ability of SNORT. As the videos demonstrate, Snort detects but does not thwart an intruder. Its advantage is that it provides more details about intrusions, and thus enables the network administrator to prevent future intrusions. Skoudis and Liston classify the free version of SNORT as a network sniffer, but describe the paid version as a sophisticated tool that can detect an attacker's subtle attempts to sneak past intrusion detection software such as SNORT. SNORT ranked 3rd in popularity as a security tool in the Insecure.org survey (Lyon, 2006).

John the Ripper

John the Ripper (2009) is a well known free password cracking tool that runs on UNIX and Windows systems. We use it to show that weak passwords are vulnerable to a password cracker. Skoudis and Liston (2006) explain John the Ripper in some detail. For a laboratory exercise, we have our students download John the Ripper from the Open-Wall website (2009) and run it on a UNIX password file.

The video *John the ripper* (2008) cracks a Window's password to the sound of Rap music. Another video also entitled *John the Ripper* (2008) and the *Cracking Linux/Unix passwords using John the Ripper* (2008) show un-shadowing a UNIX password file and running John to crack passwords. John the Ripper ranked 10th in popularity as a security tool in the Insecure.org survey (Lyon, 2006).

EnCase

EnCase (Guidance, 2009) is the standard computer forensics tool used by law enforcement. The product is expensive even with a discount for university instruction. Since it takes significant time to learn to use EnCase, we demonstrate some of the tool's capabilities and leave in-depth analysis of EnCase to a computer forensics course. Although Skoudis and Liston (2006) do not explicitly mention EnCase, they discuss the role of forensic software in incident handling and investigation. YouTube videos enhance the EnCase software demonstration.

Although the YouTube video *EnCase Computer Forensics Demo* (2007) introduces EnCase dynamically; it moves quickly and requires some instructor explanation, as do most of the others discussed here. The YouTube video *Recovering Deleted Files With Encase* (2008) deletes a file on a USB drive and then recovers it with EnCase. This video clearly demonstrates that deleted file contents are not removed from the disk and may be retrievable by forensic software. *Examining a Wiped Drive* (Examining, 2009) demonstrates that wiping a drive with zeros prevents EnCase from finding any information on the drive. *Examining File Slack with EnCase* (Examining, 2008) shows how bits of information survive in file slack, the unused part of the last cluster in a file. File slack may contain bytes of information from a previously deleted file. These videos affirm important concepts in a relatively short amount of time. If no version of EnCase is available for a class demonstration, the videos offer a beneficial supplement to reading about incident handling.

Wireshark

Wireshark (2009) is packet capture and network protocol analyzer software. Orebaugh (2007) offers a through description of this free product. Skoudis and Liston (2006) applaud this software as well, under its former name of Ethereal. The Wireshark interface is slightly different from Ethereal.

The wireshark videos are the best of those we have examined so far. *Introduction to Wireshark (Part 1 of 3)* (2008) is an excellent video introduction to installing and using wireshark. This video is an example of a high-quality security tools video. The screen images are clear. The explanations are lucid, both in wording and audio.

Intro to Wireshark: Packet Capture and Protocol Analysis (2008) is another excellent video. It demonstrates sniffing a password during a telnet login. *Wireshark - IP Address, TCP/UDP Port Filters* (2008) is a good video for showing students how to do port and IP address filtering.

3. Summary and Reflection

The seven security tools mentioned in this paper represent a broad range of significant security tools extensively used by professionals. There are several more highly regarded security tools that we have yet to explore on YouTube.

At this point, we have decided that there are several factors to consider when selecting a YouTube video for enhancing instruction. One key advantage of all the YouTube videos is that they are publicly available and free. There is always the chance that a video is removed by the author or by YouTube, but that is a possibility with all web-based resources that are not your own. A second factor to consider is the impact of the information in the video. Does viewing the video make a point that works with the course material? A third aspect to take into account is the significant time required to review the videos and to determine whether to use them in class/lab or to assign them for outside of class viewing. The introductory demo style of video is well suited to homework. If you find that you need to clarify what the video is describing when you view it, then it is likely that students will need some guidance with it. A fourth element to consider is the length of the video. In our opinion the shorter YouTube videos are preferable since their quality tends to be only fair to good. A superior video that is informative, has excellent sound and a fine picture, is more likely to engage students for a longer viewing time. The wireshark videos (Wireshark, 2009, 2008) (Intro, 2008) were the best we found thus far, and are our benchmarks for either a short or long lesson. Content, audio and video were very good to excellent on all four that we introduced above. A fifth feature to consider when reviewing videos is the overall quality. Some videos may have solid information, but be difficult to hear or see. Since students can review them as often as they wish to, a short video of only fair sound or visual impression, yet with solid information may still be an acceptable choice.

Our students liked the video assignments, and we plan to continue using them, and increase the number of tools demonstrated via YouTube. We liked the variety that they added to the material. So far, all of the videos reviewed for this paper have been available since March, 2009 when first used in class. Many were posted in 2008. They were successfully accessed again on September 25, 2009. We feel that it is worth the effort to augment regular security lab material with the YouTube videos, despite the risk that they could disappear overnight. Students and instructors alike expect web resources to be dynamic. We believe that using YouTube as an educational resource is inevitable. Benkler's (2006) argument that society is in the midst of a drastic change in how we produce and consume services, including obtaining information, surely views education as a service. "Commons-based peer production…is the rise of effective, large-scale cooperative efforts—peer production of information, knowledge, and culture…We are beginning to see the expansion of this model…into every domain of information and cultural production." (Kazman, 2009)

We would like to encourage computer security professors and professionals to produce videos of security tools and to share them with others. There is a need for high quality video to illustrate security tool functionality.

4. References

Benkler, Y. (2006) The Wealth of Networks: How Social Production Transforms Markets and Freedom. Yale University Press, New Haven, CT.

Cracking Linux/Unix passwords using John the Ripper (2008) http://www.youtube.com/watch?v=s85YeRO4DmE accessed on September 25, 2009.

EnCase Computer Forensics Demo (2007) http://www.youtube.com/watch?v=O4ce74q2zqM accessed on September 25, 2009.

Examining a Wiped Drive (2009) http://www.youtube.com/watch?v=qDgc3fXtiho accessed on September 25, 2009.

Examining File Slack with EnCase (2008) http://www.youtube.com/watch?v=E17PIdJ7HAM accessed on September 25, 2009.

EXCELLENT How to use nmap (2008) http://www.youtube.com/watch?v=Y96zgdmIJyU accessed on September 25, 2009.

Frank, Charles (2009) CIT380 Securing Computer Systems Fall 2008 website, http://www.nku.edu/~frank/cit380Fall2008.html retrieved on June 30, 2009.

Guidance Software website (2009) http://www.guidancesoftware.com accessed on June 30, 2009

Hacking Your Computer Penetrate Your Own Network (2008) http://www.youtube.com/watch?v=cFlGKpEPSFw&feature=related accessed on September 25, 2009.

Honeynet Project web site, (2009) http://www.honeynet.org/ accessed on September 25, 2009.

Honeynet Web (2009) http://www.youtube.com/watch?v=HuKmUjRGV54&feature=related accessed on September 25, 2009.

How to create a SNORT rule and test it (2008) http://www.youtube.com/watch?v=BZCwyjfz5x4&feature=related accessed on September 25, 2009

How to install and configure SNORT on an XP machine (2008) http://www.youtube.com/watch?v=nAWN989WA0A&feature=related accessed on September 25, 2009

Intro to Wireshark: Packet Capture and Protocol Analysis (2008) http://www.youtube.com/watch?v=U6ZveV0nDpk accessed on September 25, 2009.

Introduction to Wireshark (Part 1 of 3) (2008) http://www.youtube.com/watch?v=NHLTa29iovU accessed on September 25, 2009.

John the Ripper password cracker (2009) http://www.openwall.com/john/ accessed on June 30, 2009.

John the Ripper tutorial (2008) http://www.youtube.com/watch?v=4ZpzZsGCG9I accessed on September 25, 2009.

Kazman, R. and H. Chen (2009) "The metropolis model a new logic for development of crowdsourced systems." Communications of the ACM 52, 7 (Jul. 2009), pp. 76-84. DOI= http://doi.acm.org.proxy.lib.muohio.edu/10.1145/1538788.1538808

Lyon, Gordon Fyodor (2006) "Top 100 Network Security Tools" http://sectools.org/index.html accessed on September 25, 2009.

Lyon, Gordon Fyodor (2009) Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, http://nmap.org/book/ online portions retrieved on June 30, 2009

Netcat download (2004) http://joncraton.org/files/nc111nt.zip retrieved on September 25, 2009

Netcat download (2006) http://www.filewatcher.com/m/nc111nt.zip.61440.0.0.html retrieved on September 25, 2009

Netcat Tutorial (2008) http://www.youtube.com/watch?v=YkEbz9x1oh4&feature=related accessed on September 25, 2009

NMAP port scanning tool (2008) http://www.youtube.com/watch?v=4WuglJA9H6o&feature=related accessed on September 25, 2009.

Nmap website (2009) http://nmap.org/ accessed September 25, 2009

Orebaugh, Angela, Gilbert Ramirez and Jay Beale (2007) Wireshark & Ethereal Network Protocol Analyzer Toolkit, Syngress, Burlington, MA.

Password cracking using John the ripper (2008) http://www.youtube.com/watch?v=hdDA8zh3l78 accessed on September 25, 2009.

Recovering Deleted Files with EnCase (2008) http://www.youtube.com/watch?v=33HS50gQOEQ&feature=related accessed on September 25, 2009

Rutledge, Patrice-Anne (2008) The Truth about Profiting from Social Networking, FT Press, Upper Saddle River, New Jersey.

Skoudis, Ed and Tom Liston (2006) Counter Hack Reloaded, 2nd Edition, Prentice Hall, Upper Saddle River, New Jersey

Snort IDS with Kevin Rose (2008) http://www.youtube.com/watch?v=eYp8O19Xtu4 accessed on September 25, 2009.

Snort website (2009) www.snort.org accessed on September 25, 2009.

Spitzner, Lance (2002) Honeypots: Tracking Hackers. Addison-Wesley Professional, Boston, MA. ISBN-10: 0-321-10895-7

Wireshark - IP Address, TCP/UDP Port Filters (2008) http://www.youtube.com/watch?v=__SR6JO6l-A&NR=1 accessed on September 25, 2009.

Wireshark website (2009) http://www.wireshark.org/ accessed on September 25, 2009.

YouTube website (2009) http://www.youtube.com/accessed on September 25, 2009.