

## Step-By-Step Hacking Video

digg\_url = 'http://digg.com/security/Step-By-Step\_Hacking\_Video';

| del.icio.us

Discuss in Forums {mos\_smf\_discuss:Hoffman}

By Daniel V. Hoffman, CISSP, CWNA, CEH

Everyone talks about the ability to hack computers via wireless technology, but have you ever actually SEEN someone do it? Well you're about to. The Step-By-Step Hacking Video will show exactly how a laptop without the proper security protection can be attacked and exploited. In a manner of mere minutes, we can own an unprotected or out-of-date system. The video actually shows the exact procedures that a hacker could utilize to gain access to a mobile system and eventually a corporate network. Steps and technologies to prevent such an attack are presented throughout the video and are the focus of this article. NOTE: While it may seem that the first few minutes of the video are unexciting &ndash; just wait &ndash; you are being setup!

This article is broken up into two sections. The first section quantifies the different threats to which mobile computer systems are susceptible. The second portion defines the fundamental methodological steps that hackers take in trying to exploit computer systems directly and details how each step could be thwarted. These fundamental steps are also used in the video.

Today's mobile workforce poses significant security challenges to corporations. With workers accessing corporate resources from public wi-fi hotspots, hotels, home wi-fi and broadband networks, etc., the need for a comprehensive mobile workforce security solution is becoming a necessity. This is an extraordinary challenge considering the additional complexity of the mobile workforce being a moving target and with security budgets and personnel constantly being downsized.

To implement an ideal mobile workforce solution, it is important to understand the actual threats. These threats fall into three main categories:

#### Malware

Most consumers think of viruses when it comes to malware and believe that an antivirus software solution will address all malware threats. Those of us in the industry realize that it is much more complex. For antivirus solutions to be effective, they need to be running and the virus definitions need to be up-to-date. This can be a significant challenge with a mobile workforce that is not always online when automatic updates are performed. To protect yourself from malware, please consider the following:

-

In addition to antivirus software, antispymware applications are necessary to address the malware threat. Keeping these applications running and up-to-date poses the same difficulty as antivirus updates.

-

Another important tool to combat malware is an enterprise-grade personal firewall with IDS/IPS capability. This is important because antivirus and antispymware applications are reactive and based upon recent definition files. Conversely, an enterprise-grade personal firewall with IDS/IPS capability has the ability of performing zero day protection, where malicious behavior can be intelligently identified and stopped as it occurs.

-

An often-overlooked means to prevent the risk from malware is ensuring that the remote endpoints have the latest operating system and application security patches and that the remote system is properly configured from a security perspective. This is important because malware will often take advantage of system and application vulnerabilities that would not be present if the system were up-to-date with patches and properly configured.

-

It is also important to note that there is a significant risk that anti-antivirus and anti-personal firewall malware will disable the security applications that corporations put into place. Consequently, it is important to have a check take place to ensure that these applications are running and up-to-date and if they are not, access to the Internet, corporate network,

etc. should be denied and the deficiency remediated. The logic for such checking and remediation should reside on the remote endpoint, as today's systems need to be in compliance with security policies at all times. In the past, corporations have relied upon VPN Concentrators or Cisco NAC-type functionality to check the security posture of the remote endpoint as it is gaining access to the corporate network. With today's mobile workers spending 80% of their time not VPN'd into a corporate network, this way of checking the state of the system's security posture is inadequate.

## Sniffing

A mobile worker constantly has the threat of their data being sniffed. Sniffing can fall into two fundamental categories:

-

**Sniffing of Credentials** &ndash; Corporations are moving to a model where a single application is being used to provide dial-in, wi-fi, broadband, mobile data (CDMA, EVDO, etc.) access. In doing so, there is an advantage to having authentication for all of these different transports proxied back to a central location, commonly the corporation's network. Often, these authentication credentials are the remote user's network credentials, or some other credentials that have significant value to the end-user and corporation. Consequently, it is very important to ensure that these credentials are protected during the proxy process. With standard RFC Compliant RADIUS Proxy (A commonly used authentication protocol), the username is always sent in the clear and the password is hashed with MD5, then un-hashed and re-hashed on each RADIUS server through which the credentials pass.

-

**Sniffing of Data** &ndash; With workers using public and private wi-fi and hotel broadband Internet access, the threat of an unwanted party sniffing application traffic is a very real concern. In virtually all cases, public wi-fi locations and hotel broadband locations do not offer any forms of inherent encryption for data leaving a system on these networks, while at the same time making these networks readily available to a number of simultaneous users. The best way to protect against the sniffing of data is to ensure that a VPN tunnel is active throughout the life of the public wi-fi and hotel broadband network connection. Doing this and disabling split-tunneling will ensure that all data leaving the remote system will be encrypted via the VPN client, which commonly would use DES, 3DES or AES encryption.

## Direct Attack

The most dangerous form of attack is a direct attack. This is because a hacker can use their cognitive skills to exploit a remote system and to leave the remote system vulnerable in the future. They can also consciously dissect and analyze data on the remote system. There are a number of key security steps to implement to protect against a direct attack:

-

Remote systems need to be up-to-date with security patches and properly configured. Hackers gain direct access to remote endpoints by running exploits that take advantage of vulnerabilities on the remote system that would not be present if the system were properly patched and properly configured. Ensuring a mobile workforce has the latest patches

and is properly configured is one of the biggest security challenges to organizations. Virtually all of the patching systems in place today do not provide a means to remediate the remote system by actually pushing the necessary patch or configuration to the system when the endpoint is not connected directly to or VPN'd into the corporate network. With end-users spending 80% of their online time not VPN'd into the corporate network, that leaves a significant gap.

-

Ensuring the remote endpoint has an enterprise-grade personal firewall that is running, properly configured and up-to-date. This firewall would not only prohibit a hacker from accessing the remote systems, it would also provide stealth capabilities to help make the endpoint invisible to scans.

-

Being purposely redundant, antivirus and antispyware applications need to be running and up-to-date. An outdated security application will not provide protection against newly developed malware. Commonly, a hacker will place malware on a victim's machine to either further exploit it, or to provide a means to exploit it in the future. An endpoint that is constantly scanning for the existence of such malware will be able to detect when this takes place and perform the necessary actions to address the threat.

#### Step-by-Step Guide to the Fundamental Steps Performed in the Video and How to Combat Them Footprinting and Scanning

The first step is finding a live system. There are many tools available on the Internet to search for live targets. To protect against footprinting and scanning, use an enterprise-grade, properly configured and running personal firewall. This is the best means to protect your mobile systems from even being seen during a scan.

#### Enumeration

Once a target is found, more information needs to be gathered to determine the best approach for exploiting it. Just as there are many scanning tools available free on the Internet, there are many enumeration tools available. There are two main steps that should be implemented to prevent enumeration from taking place:

-

Ensuring that a properly configured enterprise-grade firewall is present and operational.

-

Ensuring that the remote operating system is properly configured, so that it does not disclose this type of information.

## Launching an Attack

Once a live system is found and information is gathered about it, a direct attack can be launched against the system. There are a number of steps that can be taken to prevent a direct attack:

-

Ensuring your remote systems have the latest operating system and application security patches. When hackers launch an attack against a system they do so using exploits that take advantage of vulnerabilities on the remote system that commonly would not be present if the remote systems was up-to-date with security patches.

-

Ensuring that a properly configured enterprise-grade firewall is present and operational.

-

Ensuring that antivirus and antiSpyware are running, utilizing real-time scanning and are up-to-date on your remote systems. It is a common tactic for hackers to place trojans and other malware on hacked systems and having these programs actively scanning would help catch situations where this malware is being transferred to the hacked machine.

## Leaving the Remote System Vulnerable to an Attack

Once a hacker has exploited the system, they will commonly take steps to leave it vulnerable to future attacks. This can be done by installing a trojan or remote control software, installing a key logger that routinely sends all keystrokes from the system, etc. To protect against this step:

-

Ensuring an enterprise-grade personal firewall is running, properly configured and up-to-date. This can stop a remote connection from taking place and sense when malicious activities are taking place.

-

Ensuring that antiSpyware and antivirus applications are running, and up-to-date. In doing so, these security applications would be able to find address and malware left behind to further exploit the system.

I hope this helps shed light on the hacking process and has given you ample information to help you protect your own corporate networks including those ever slippery mobile workforce machines.

Any questions or comments for the author may be sent to [dhoffman@fiberlink.com](mailto:dhoffman@fiberlink.com).