

Pitfalls of a Home Based Ethical Hacking Business

del.icio.us

Discuss in Forums {mos_smf_discuss:/root}

By EH-Net Member Cutaway, GSEC-G, GSNA-G, GCUX-S, GAWN-C, and CISSP

Self-employed security professionals, or those who are involved with small businesses, will invariably find themselves conducting security assessments and penetration tests of Internet facing systems and services. These activities will happen through resources that are generally not as robust as those supplied to security professionals in medium and large organizations. The following is a list of a few items that a security team should take into consideration before performing security related activities under these conditions.

Small Office/Home Office (SOHO) DSL/Cable Routers

Network and service enumeration, vulnerability scanning, or automated exploitation can pose a significant challenge to SOHO Routers. These embedded devices have limitations due to memory, CPU, and firmware. A good example of the challenges these devices will present to a security consulting effort is the fact that the outgoing connections of these devices are limited. For instance, a Linksys WRT54G with DD-WRT installed can only handle 512 simultaneous connections. Default Nessus configurations scan 10 hosts at a time and perform 2 tests per system after an initial port scan of 8800+ ports. Combine that with NMap, Paros, Wikto, Metasploit or any other automated enumeration, vulnerability or exploitation tools, and these devices are going to be strained to function efficiently. Rather than using a SOHO router for protection and connection to the Internet, the team should consider building and deploying a Linux based router and firewall system. These systems are much more robust and can provide a significant amount of necessary flexibility when connecting the team's resources to the Internet.

Scanning Hosts

Projects that include a large target base and a team of people are going to require a location to consolidate resources and data output from a plethora of information gathering tools. A team of scanning hosts can be created, so that security tools can be consolidated and maintained more efficiently. One deployment configuration that should be considered is setting up one system to house tools that require a Graphical User Interface (GUI), another system without a windowing interface for command line tools, and servers that do not require a GUI. The main reasons for doing this is so that 1) all team members are using the same version of each tool and 2) so that the generated output is stored in one place. Since multiple people will be using these servers they also need to be tuned to handle the load that occurs during scanning and

enumeration. Memory is very important. Running without a windowing interface, limiting the use of browsers, and monitoring the memory usage of other programs will help these systems operate with optimum efficiency and limit lost or incomplete data during periods of heavy loading. Another idea, if possible, is to keep these systems on a separate network or Virtual LAN. Avoiding normal network activity like Internet browsing, file sharing, and Instant Messaging will have a positive impact on the consistency and reliability of the information collected by these systems.

Network Problems

Network problems can be a hassle to track down and mitigate while the team is trying to focus on target discovery and exploitation. These problems can stem from hardware, software, or the Internet Service Provider (ISP). Checking hardware for connectivity is usually easy in a small office or home network. Unusual and ongoing network issues might be caused by an ISP. These businesses can be contacted via their customer support to see if there is an issue on their network. Special attention should be made to all applications running on each system connected to the team's network, as they can adversely affect bandwidth. Here are a few examples:

-

Media Software - iTunes and similar applications can create quite a few network connections depending on the number of feeds and radio stations to which they have been configured to automatically create a connection.

-

Firefox - This browser has a plethora of plugins that, once installed, will automatically check for information. Examples: Sage periodically updates RSS feeds, ForecastFox automatically polls the weather every minute or two, Google Browser Sync will automatically upload and download bookmarks and OPLM files, ShowIP performs DNS queries for each webpage, etc. Fortunately, Firefox Plugins can be disabled very easily through the Add-ons window.

-

Instant Messaging (IM) - Communication is a necessity for any team. This is often accomplished via iChat, AIM, Trillian, Skype, or any number of other IM or Voice over Internet Protocol (VoIP) clients. Some IM clients include video on top of chat. All of these can start affecting bandwidth.

-

Email Clients - Email clients can be configured to automatically poll for new messages. Message size can increase when the team starts sending report documents, tool outputs, images, and other information as encrypted attachments.

-

Automatic Updates - Although highly recommended, automatic updates can adversely effect reconnaissance, enumeration, and exploitation efforts. Suddenly checking for updates to Microsoft Windows, OS X, Adobe, Java, or any number of other operating systems and applications can directly impact network and system resources.

VMware

Although many consider this program to be the great resource equalizer, it can only operate in this fashion if it is configured to provide the resource requirements of assessments and penetration testing. If the team's scanning system is going to run out of a VMware image, then it will be necessary to evaluate the amount the memory assigned to the image. Using Network Address Translation (NAT) to get an IP address for the interface is very convenient, but to effectively handle enumeration and vulnerability scanning, the interface should be set to operate in Bridged mode. NAT is controlled by a size restricted NAT table. Each connection is stored in this table and when the table reaches its size limitations it starts dumping packets (thank you Ed Skoudis for point this out to me during one of his classes). Bridged mode means that the VMware interface gets its own IP address on the network. Of course, this interface may still be affected by a host based firewall. Firewall configuration settings should be pre-tested to determine how it will affect tools and connections running out of the VMware image.

Team Collaboration

Work and communications in a distributed team is always a challenge. Protection of sensitive client and team information is very important. Determining how the team will communicate via secure IM, VoIP, email, and file exchange should be determined at the beginning of the effort. The team should exchange and verify public encryption keys. Predetermined and documented file and directory naming conventions and permissions will avoid a lot of confusion. Connections to remote resources should also be addressed. Setting up secure Virtual Network Computing servers and clients, Remote Desktop, Secure Shell, Virtual Private Networking, and other secure communications should be addressed early, so that the team can focus on work instead of administration.

Network Address Translation

SOHO deployments are often NAT environments. NAT is easy to deploy, and it offers a necessary layer of security. Unfortunately not all software and scripts are NAT compliant. They were never intended to be. So the team is going to have to figure out a way to allow connections through border routers and other protection systems to the waiting applications. Good examples of tools that will require these considerations are Netcat listeners and Metasploit exploits. Fortunately most routers these days support port forwarding so this is a problem that can be fixed by a few simple steps. While making the configuration changes to the border router, the IP address assigned to the router should be noted. This IP address may be dynamically assigned by the ISP and could change. Periodically making a note of the address assigned will come in handy when setting your connection options for the tools that are going to be deploying code to initiate return connections.

Conclusion

Security assessments and penetration testing can be challenging and time consuming just by their very nature. By addressing these issues before initiating a project, the team can maximize the amount of time that is devoted to the project specific tasks instead of administrative problems. As usual, be sure to get written permission prior to conducting any assessment or penetration testing efforts.

Go forth and do good things.

Cutaway

Cutaway is an Information Technology Security Manager for a medium-sized university in South Texas. In his spare time he also performs numerous duties as an Information Security Consultant for Cutaway Security. He has been in the security industry since 2002 where he started out in the security field performing system accreditation and certification, assessment, and penetration testing for a prominent defense contractor. In 2005 Cutaway earned his Masters in Network Security from Capitol College in Laurel, Maryland while also achieving his GSEC-G, GSNA-G, GCUX-S, GAWN-C, and CISSP certifications. In March of 2006 Cutaway started the Security Ripcord Blog and Podcast (<http://blog.cutawaysecurity.com/>) which is used to help further professional and personal security education through Internet media.