Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Remote Access White Paper

The increasing mobility of today's workers supports the need for corporate dial-in solutions. Many business users have Internet connectivity at their homes for personal use. This may suggest the use of Virtual Private Networks (VPN) for everyone. Unfortunately, users do not often have access to their local connections when traveling far from home. Additionally, VPN technology is not yet consumer ready. Wide scale deployment often requires a large technical staff capable of debugging often-difficult problems. Technicall...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Wargames - You've seen the movie, maybe you experienced it, but that was 20 years ago, certainly things have improved since then, haven't they?

History

As we enter the new security paradigm many fear we are faced with resourceful threats and exposures. While this is certainly true, companies need to address some age-old exposures in addition to looking into the future. Currently, many companies are concerned with Internet connectivity, spending large sums of money securing these connections to the world. As more and more companies secure this avenue, hackers begin to look for other ways to break-in. Often this other way is the same old way they used before, just with a few new twists. This makes securing your remote access[1] crucial.

"**Wargames"** - You've seen the movie, maybe you experienced it, but that was 20 years ago, certainly things have improved since then, haven't they? Don't be too sure. Now more than ever companies need to understand all of their threats and vulnerabilities, coupled with their high value business objectives. Addressing dial-in risks, as part of any total security architecture makes good business sense.

This stuff doesn't happen in real life, does it? The movie was based on a true story, as was Clifford Stoll's now famous hacker book **"The Cuckoo's Egg"**. More importantly these techniques are still being mimicked today.

War Dialing Case Study

Just how do hackers break into a network through a phone line? It is a fairly simple technique known as war dialing (gaining the very name from the movie itself). The following case study was based on an actual company, a Healthcare provider, although the results are representative of findings across several industries. The case study will demonstrate the ease and effectiveness of using a war dialer to break into a corporate network.

Note: the following paragraphs are for educational purposes only, any use of this information for other purposes is forbidden and possibly illegal.

The company's name has been changed to protect the innocent, in this case ABC. When performing a war dialer, there are a few necessary requirements. First and foremost the hacker needs to obtain the company's exchange. An exchange is the company's registered phone extensions, for example 216-555-0000 through 216-555-9999; indicating the company owns approximately 10,000 numbers. Obtaining this information can be as trivial as looking in the phone book, referencing a business card or using the public accessible resources of the Internet. For our case study we will assume that ABC Company has three locations, all of which are in the same geographic location, thus

[1] Remote access for this paper will be defined as- access to the company's internal resources through a location outside of the company's control, specifically relating to communications involving phone or dialup access.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

having the same area code. Once we have obtained ABC's exchange and range we next determine the phone numbers that have devices[2] connected to them. Certain fax machines may carry the same characteristics as a modem; the war dialer can filter out these devices. A war dialer[3] in simple terms will take the input range or exchange, which we have already obtained, in this instance 216.555-0,9999, 216.556-0,2000, and 216.557-1234-1244, and dial each number attempting to connect to any devices that answer.

Software Used

There are a variety of software programs available to perform a war dial test. The most popular commercial package is PhoneSweep (http://www.sandstorm.net/phonesweep). Shareware tools Toneloc and **T**he **H**ackers **C**hoice (THC) are the most popular for hackers. For this case study we will be using THC. THC can be downloaded freely off any number of security web sites including http://www.6Ft-Under.com. Originally, THC was based off of Toneloc's design and functionality. However, a newer version of THC has recently been released which has some added features making it the current hacker's choice, surpassing Toneloc in ease-of-use and in functionality. Phonesweep, a commercial product is extremely functional and eliminates the need to analyze long cumbersome reports produced by the shareware products. This functionality is not inexpensive, Phonesweep can cost up to $2,500 depending on your specific needs.

Running the War Dialer

The hardware needed to run a war dial is surprisingly minimal. Any PC running DOS 6.2 and a modem card, or external modem will suffice. Boot your machine, and configure the modem to live on COM2 and THC will do the rest. Configuring THC is also relatively straightforward, for the example above the following command will initiate and run the war dialer:

C:\THC\thc-scan /m:216-555-xxxx /r:0000-9999 /c /q

This will dial the 10,000 numbers selected; the default setting on the war dialer will dial a number and wait to detect a carrier for 30 seconds. This represents approximately 6 rings per number, not including dial and connect time. If you are dialing through a PBX and testing long-distance numbers, this may need to be increased. Running the war dialer continuously twenty-four hours a day will take approximately 3.5 days to complete a full exchange. In our case we have three ranges to dial. Using the above syntax modify the exchange to /m:216-556, the range to /r:0000-2000 for the next range, thus dialing 216-556-0001,0002,0003 etc until it reaches 2000. Finally run the last segment changing the exchange to /m:216-557, and the range to /r:1234-1244.

Once the war dialer has been configured and started as shown above, it will randomly dial each number looking for devices or carriers. When the war dialer connects to a device it immediately captures the information displayed and stores the banner in a text

[2] A device in this instance will be anything that answers with a modem connection for example a Cisco Router, Windows NT RAS or Windows 95 with PC-Anywhere running.
[3] A War-Dialer is a program that systematically dials a predefined list of phone numbers and categorizes the results as being Busy, Carrier, No Carrier, or Timeout.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

file for later viewing. The war dialer would classify this connect as a *carrier*. The war dialer will place each number into one of four categories as described below:

- **Busy's** are numbers that, during dialing, were in use; these numbers are placed into a pool of numbers to be redialed. Periodically during testing the dialer will pull busy numbers from the busy pool and redial them. This process will be continued until the number is categorized as a *Carrier*, a *No Carrier* or a *Timeout*. After 8 attempts with the number being continuously busy, the number is marked as *busy*, and no further automated attempts are made.
- **Carriers** are numbers that had a device on the remote side to auto-answer and attempt to negotiate a data session, i.e. PC-Anywhere, Windows NT Remote Access Service (RAS). *Note: any device that responds with a carrier, is a concern to the organization as they may provide a "gateway" into the internal network.*
- **No Carriers** are numbers that answered, but did not attempt to negotiate a data session, these are typically voice response, or other non-machine oriented pickups, including any automated attendant-type phone numbers.
- **Timeouts** are numbers that were dialed with no response of any type.

War Dialer Results

Hackers are only interested in carriers found, or devices that answered with a data session. As noted earlier war dialers can determine fax machines from a true data connection. Once the war dialer is finished, the next step would be to view the banners that were captured. Below are examples that were captured during the case study:

Example of a machine running PC-Anywhere

11-09-99 16:49:00 Dialing... /216-555-2213

CONNECT 9600/ARQ/V32/LAPM/V42BIS

*X_ }_*

._Please press <Enter>..._I PAPPS _ TEL1 _ w‹ _ __I PAPPS _ TEL1 _ w‹ _ __I PAPPS _ UHTEL1 _ w‹ _ __I PAPPS _ TEL1 _ w‹ _ __I PAPPS _ TEL1 _ w‹ _ __E

[CARRIER LOST AFTER 33 SECONDS]

Example of Shiva

11-09-99 21:13:53 Dialing... 216-555-3921

CONNECT 9600/ARQ/V34/LAPM/V42BIS

@ Userid:

@ Userid: HELP

Password?

Login incorrect

@ Userid: GUEST

Password?

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Login incorrect

@ Userid:

@ Userid: LOGIN

Password?

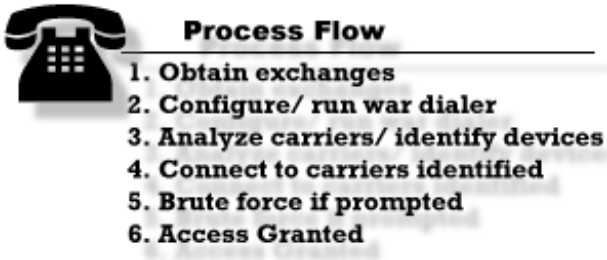
Did the war dialer break in? No. The war dialer is only a tool in this overall process. There still needs to be some level of expertise involved to understand and analyze the war dialer results.

The first example is a banner captured from a machine running PC-Anywhere. Although not easily recognized by the naked eye, this banner is distinguishable by the:

Please press <Enter>…

Evident in Any PC-Anywhere banner.

Why is the banner so important? Without knowing the system you have connected to, it may be impossible to properly connect to that system. In this example the host is running PC-Anywhere software, thus in order to establish a proper connection the hacker must use the PC-Anywhere client. In this instance the host machine is not requesting any form of authentication. Once a hacker connects he has free access to the machine and possibly the entire network. For our case study, we were able to connect to five (5) machines running PC-Anywhere. These machines were all logged in as *Administrator* and we were able to map the internal network to identify additional targets. Further, we were able (using the file transfer feature of PC-Anywhere) to download and crack the *SAM*[4] files and eventually take over the entire internal network. No one from the network security staff knew that we were connected and there were no logs of our activity. The security ramifications of this breach can be quite far reaching. Unrestricted access to the connected machines, and ABC's entire internal network can obviously have serious consequences.



The second banner displays a Shiva remote access server, a very common centralized device used to authenticate users onto the network. This device can be recognized by the banner:

@Userid:

As demonstrated above the war dialer will attempt some very basic commands to try to gain access to the device or generate more information that may be used to identify the device in later steps.

That's it, are we done? As demonstrated from the above example, running a war dialer is fairly simple, however understanding and analyzing the results takes some more detailed knowledge and understanding of remote access services. The war dialer can identify possible devices that may be used to gain entry into a company, but it is up to the

[4] NT's password file containing all users accounts and their respective passwords.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

perseverance and the expertise of the hacker to gain entry. The next step is to review the carrier logs and determine, using the method described above, what the device is.

Is there anything that can help me identify these devices? There is always an easier way. PhoneSweep has the potential to identify over 250 devices automatically while running the war dialer. It uses the same techniques described above matching known banner signatures to ones that have been preprogrammed. For our example we used a reference from a well know hacking magazine called Phrack (Volume Six, Issue Forty-Seven, File 6 of 22).

From our example we were able to connect to ABC's network without authorization to over seven (7) different devices and from that we had the potential to download/modify/delete patient identifiable information.

Legal Issues

Of course war dialing is illegal, right? As alluded to earlier, running a war dialer may be illegal. Some states restrict dialing a sequential range of numbers, hence the above example could possible be illegal. However, the hacking community, more specific THC, has worked around this by randomizing the numbers dialed in the range. This serves two purposes, one it eliminates or reduces the risk of legal liability, but more importantly stealth's the war dialing activity. It is not long before employees notice phones ringing in sequential order from one cubical to the next and when they answer no one is there. This may seem strange but these laws were primary instituted to stop tele-markers from using similar methods to sell you stuff. It does not stop them, nor does it stop the hackers.

Stop the Insanity

How can war dialing be prevented? While it is extremely difficult to stop war dialing, it is possible to make the practice less fruitful. When planning to secure remote access there are a several points that should be addressed:

Inventory existing dial-in lines

Using the method described above war dial your particular organization. Keep in mind that war dialing is not 100%. It does not guarantee that you have found all of your dial-in lines. Depending on when you run the war dialer, some lines may be inactive (often users will only enable their desktop dial devices when they leave for the day) or in use (this is why the war dial software will attempt a connection 8 times before giving up).

Regularly monitor existing log features of your dial-in architecture

Monitor for failed logon attempts and successful logons during unusual business hours. Most centralized dial facilities have a method for logging activity. Unfortunately, the logs are often not reviewed, or not configured to capture essential information, such as failed attempts. If your dial-in equipment provides the capability you should keep any caller-id logs as well as the caller's user name, connect time, and connect duration. This can then be reviewed with users should the need arise.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Consolidate all dial-in connectivity to a centralized device

By consolidating dial-in connectivity into one area, it will allow connections to be monitored as recommended above. By centrally administering dial-in lines you will be placing control of vital resources in network administrators hands. These administrators typically have a greater concern for security than an average user installing PC-Anywhere on their desktop. Additionally, overall administration time will be reduced (although this benefit will be difficult to quantify).

Distribute analog lines throughout various exchanges

Although a simple example of security by obscurity, if someone has selected your company as a target, they will likely use common numbers from business cards, web home pages and the like. By placing your dial-in pool on a separate exchange, it may help to prevent an attack from a war dialer. As with all aspects of security, each small action raises the bar a little bit. Making the successful attack less likely.

Disable any banners that do not need to be present

As noted above the easiest way to identify a carrier is by the banner that is displayed. Certain prompts cannot be modified, however all references to your organization should be removed. At times a hacker is simply sweeping numbers looking for something interesting. If you have your company's name appear on a banner it may increase the likelihood of further attacks.

Require two-factor one-time authentication

The primary system that is rapidly becoming an industry standard is the use of SecurID cards. SecurID cards present a token-based approach to dial security. It uses a small LCD card to generate a unique number every 60 seconds. When the card is first configured, the user must select a PIN (Personal Identification Number) this is then combined with the token generated by the card to form a complete *passcode* used to enter the system. This combines something you know (the PIN) and the something you have (the Card), both items must be present to gain access. There are several variations on this theme of something you know and something you have. More information about SecurID cards can be found at: http://www.rsa.com/.

Policies

Develop remote access policies and procedures to address a variety of security and procedural issues.

Continuous assessments

Did someone call an auditor? Although war dialing is not a solution to remote access security, it can determine if policies are being followed or if rogue modems are being used.

Conclusion

Any remote access solution must be reliable, easy-to-use and secure. Does remote dial-in connectivity have a place in today's fast paced Internet driven economy? The answer is an emphatic yes. There is no need to throw away your old dial-in solution for newer technologies. Solutions exist to allow users requiring PC-Anywhere access the ability to use the centrally controlled and monitored dial-in pool. The increasing mobility of

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

today's workers supports the need for corporate dial-in solutions. Many business users have Internet connectivity at their homes for personal use. This may suggest the use of Virtual Private Networks (VPN) for everyone. Unfortunately, users do not often have access to their local connections when travelling far from home. Additionally, VPN technology is not yet consumer ready. Wide scale deployment often requires a large technical staff capable of debugging often-difficult problems. Technically savvy users will have an easy time making connections. Others may find the technology difficult to use. There are other hurdles to entering the VPN game. Not all Internet Service Providers (ISP) provide the types of connections that can be leveraged to use VPN technology. This may limit choices for your users. Understanding this and other future needs and expectations will reduce the risk of rogue remote access points across the company. Consolidation of these access points into one centralized secure location is a win-win situation for users and for corporate security. As noted throughout this paper, having a centralized remote access solution can reduce administration time, increase security and overall *enable* business to perform at peak levels.

CITATION OF SOURCES

Cavalier and DisordeR. Phrack, General Source " Volume Six, Issue Forty-Seven, File 6 of 22", Internet Outdial List v3.0
Link: http://www.6ft-under.com/Tools/index.htm

Minor Threat & Mucho Maas. "ToneLoc v0.98 User Manual"
Link: http://www.textfiles.com/hacking/tl-user.txt

Dan Powell, Steve Schuster and Ed Amoroso, AT&T Labs. "Local Area Detection of Incoming War Dialer Activity". Columbia, MD.
Link: http://www.att.com/isc/docs/war_dial_detection.pdf

Stoll, Clifford. Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage
Amazon Link: http://www.amazon.com/exec/obidos/ASIN/0743411463/qid=1006294548/sr=8-1/ref=sr_8_19_1/102-2960351-1015308

Mandia, Kevin and Prosise, Chris. Incident Response. New York. Osborne/ McGraw-Hill. 2001.
Amazon Link: http://www.amazon.com/exec/obidos/ASIN/0072131829/qid=1006295463/sr=8-1/ref=sr_8_3_1/107-8423942-1846913

Stuart McClure, Joel Scambray, George Kurtz. Hacking Exposed: Network Security Secrets & Solutions. New York. Osbonre/ McGraw Hill. 2000.
Amazon Link: http://www.amazon.com/exec/obidos/ASIN/0072193816/qid=1006296197/sr=8-1/ref=sr_8_7_1/107-4007216-1010936

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**