Net Admin Weekly

59,000 Subscribers Worldwide

October 9, 2002
Issue #12

CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters

CramSession

Feature

Web Spoofing: Not Just Harmless Fun — Read it

Q & A

NAT Problems — Read it

Same Domain Name for Internal Network and Internet Resources — Read it

Security Advisories

Symantec Provides Free Bugbear Removal Tool — Read it

Apache Fixes Flaw in Web Server — Read it

SANS/FBI Top 20 Security Vulnerabilities List — Read it

News Headlines & Resources

Any Port in a Storm: Understanding Buses and Ports — Read it

Microsoft Polishing Off .NET Server Software — Read it

Windows 2000 Cluster Service Reduces Maintenance Downtime — Read it

Systems Management Server 2003 Reviewer's Guide — Read it

Microsoft Operations Manager 2000 Operations Guide — Read it

How to Increase Outlook Web Access Performance — Read it

Windows 2000 Service Pack 3: Notes from the Field — Read it

Download of the Week

PostCast Server — Read it

Feature

Web Spoofing: Not Just Harmless Fun

to top

Spoofing – it sounds so whimsical. Just a joke. Just for fun.

But web spoofing, the act of representing a web page or site as something it's not, is no laughing matter when the intent is to con innocent web users into giving away confidential information such as credit card numbers or account passwords.

The thing that inspired me to write about this topic in this week's newsletter was an email that I received a few days ago. Sent in HTML format, the body of the message said the following:

"Dear PayPal Customer,

This e-mail is to inform you of a recent update we have made to our systems. To avoid service interruption, we require that you confirm your account as soon as possible. Please click here ("Click here" was hypertext) and take a moment to confirm your account.

Please note: if you fail to update your account, it will be flagged with restricted status.

Thank you,
The PayPal Staff."

Now there were a couple of problems with this message for me, right off the bat. First, I don't have a PayPal account. But even if I did, I'd have been suspicious of this message because the "From" field was empty. That's possible, but unusual, for a legitimate business email. The mail header showed a return path of <service@paypal.com> but I wasn't convinced.

The "Click here" link pointed to the following:
http://www.paypal.com@%77%77%77.%61%7A.%72%75/%70%70%64

Someone who doesn't know much about how URLs work might think the site was on the www.paypal.com web server, but this is a common spoofing trick. When you see an @ sign in a URL, everything that comes prior to the @ sign is disregarded by the web browser. So the REAL URL is the seeming garbage that follows the @ sign. Another trick is that those % signs are disregarded, too. When you get rid of them, you find yourself with the IP address – in hexadecimal format. And that link takes you to a web page that looks for all the world like a PayPal page, nice logo and all. Except that if you're paying attention and take a look at the address bar, you'll see that you aren't at www.paypal.com at all; you're at www.az.ru/ppd/. In other words, this "PayPal" page is residing on a server somewhere in Russia (you know that because of the .ru top level domain).

This should be smelling very fishy to you by now. On the fake PayPal site are (who would have guessed?) form fields to fill in your account information and password. I don't think so. This is a typical case of URL spoofing – using knowledge of browser technology to make a URL appear to be legitimate. Some spoofers go a step further, and use JavaScript to obscure the real address in the address bar, covering it with a fake address bar that shows the address the user would expect to see.

PayPal has been a favorite target of scam artists who have used this and other methods to obscure their real web addresses. A slightly different version was reported in September in an internet.com article that offered users free transfers for re-entering their credentials, supposedly made necessary due to a "troubled computer system." That one used a CGI script to redirect users to www.paypalsys.com. In this case, even if the user does scrutinize the address bar in the browser, the domain name looks as if it could belong to PayPal. Previous variations have asked users to "verify" their account info because of a server upgrade. Another simple method of spoofing URLs is to substitute a 0 (zero) for the O (letter 'O') character, or interchanging similar appearing characters such as the lowercase l, uppercase I and 1.

Unicode characters can also be used to simulate English letters of the alphabet. For example, it was reported that a group of students registered the domain Microsoft.com with Verisign using the Russian Cyrillic letters for "o" and "c." The two domains were different, because the Cyrillic letters are different technically, but they appeared to be alike.

Other scammers just use the IP address instead of the server and domain name, so all the user sees is something like 207.46.230.220 instead of the domain name (this particular IP address actually resolves to www.microsoft.com).

If a link has only an IP address, is there a way to find out the domain with which it's associated? Sure – you can use the nslookup TCP/IP utility (type nslookup at the command line, followed by a space, then the IP address). This will show you the domain name associated with the IP address. There are also online tools at sites such as www.samspade.org that will let you do the same thing.

Another favorite method of spoofing is to put false links in a web page. Because the page displays only the hypertext itself (for example, the words "Chase Manhattan Bank"), the user doesn't immediately know that the link points to www.scamsite.com instead of www.chase.com. You can view the URL of a link without clicking it by hovering over it and checking the browser's status bar (at the bottom), but clever scammers use JavaScript to hide the real URL there and replace it with a fake one.

SSL (the Secure Sockets Layer protocol) is designed to provide for authentication of servers on the Internet, but hackers can use various techniques to persuade the user's web browser to connect to a fake server and still give the appearance of a secure session. So don't be fooled into thinking all is well just because the site appears to be secure. It may even actually be a secure site – but the secure connection is not to the server that the user thinks he/she is connecting to.

Later that same day, I received almost the identical email message from "Western Union" with a link to "http://www.westernunion.com@az.ru/wuc." This time they didn't try to obscure the real URL (az.ru/wuc) with a hex IP address, but did use the old @ sign trick to fool those who don't know better into thinking the link pointed to the westernunion.com domain. I don't have an account with Western Union either, but I have to give these scammers points for persistence, at least.

How many unsuspecting users have been taken in by these scam artists? There's no way of knowing, but there's no doubt that many have dutifully followed the instructions and exposed their accounts to hackers who can then make fraudulent charges to the accounts. While most of the readers of this newsletter may be savvy enough to recognize these scams for what they are, it's important to educate the users we support – as well as members of our families and friends who are less tech-oriented – that these scams are out there.

This week's feature article by
Deb Shinder,MCSE, etc.
Net Admin Weekly Editor
deb@shinder.net

Q & A

NAT Problems

to top

Question:

Dear Sgt. Deb,

I have been using NAT successfully on my home network, but just recently a problem has cropped up. No computers, not even the NAT box, can access the Internet either by DNS or by IP address. I can ping my default gateway, but nothing works after that. The event log message is below:

"The DNS proxy agent was unable to bind to the IP address 192.168.0.1. This error may indicate a problem with TCP/IP networking. The data is the error code."

I have NAT set-up to do DHCP and DNS. I have tried setting up a DHCP server and not using NAT but it still doesn't work. Client computers are able to obtain a DHCP address but not access the Internet. I have tried disabling RRAS and reconfiguring it but it still doesn't function. When I disable the RRAS service and disable the internal network NIC, I have full Internet functionality. The NAT box has two NIC's. One public, one private. The only other weird thing is when I do an ipconfig/all on the NAT box, the default gateway for the public NIC is blank, even though there is an entry in the TCP/IP properties. I have tried technet and MS support site. Anybody encounter this before? --John B.

Answer:

Hi John,

The Windows 2000 RRAS NAT is very handy, but you have to play by its rules. A key element in configuring the RRAS NAT is the type of interface using to connect to the Internet. If you have a dedicated connection, then all you have to do it enable RRAS, install the NAT Routing Protocol, and let 'er rip. But if you use a dial up interface, then you need to configure the demand dial interface and create a static route to 0.0.0.0 so that the demand dial interface is triggered when requests are made for non-local hosts.

The error regarding the DHCP Relay Agent is interesting. First, why is it enabled? Do you have VPN clients that need to obtain DHCP options from an internal network DHCP server? If not, remove the DHCP Relay Agent Routing Protocol from the RRAS console.

Make sure ICS is not enabled on the computer, as that can cause some conflicts. I mention this because your internal interface uses the same IP address that ICS assigns. Let RRAS take care of the NAT, not ICS.

Do you have a DHCP server on the internal network or are you allowing the RRAS NAT service's DHCP allocator to take care of address assignment? If you have a DHCP server, disable the DHCP allocator. Do you have a DNS server on the internal network that can resolve Internet host names? If so, disable the RRAS NAT proxy DNS feature.

One more thing – I notice you say the default gateway for the public interface is blank when you do an ipconfig, but there is an address in the TCP/IP properties dialog box. How does the external interface receive its address? If you use a static address on a permanent link, ipconfig will show the address. If you use PPPoE, then the external interface provides an Ethernet transport for the PPPoE Internet link. The PPPoE interface will have to be used for your dial on demand interface.

Configuring an ISA Server Test Lab for Exam 70-227

to top

Question:

Dear Dr. Tom,

Ok! What might be the ramifications if one has a (Domain name) site e.g. "mysite.com" hosted with their ISP provider and they set up a server at home and name it "mysite.com?" Will there possibly be problems if they also use the ISP's DNS?

Can one name their server "mysite.com" and still have their ISP host a site called "mysite.com?"

Anyone have any input? Would it possibly be better if they just

acquired another domain name? They could possibly change it and host they current "mysite.com" domain from their server home site, but then the ISP requires them to use their own site for e-mail. They do not have Exchange or any or mail program. I am aware of the capability to set up

IIS, but what about the mail issue?

Are there some alternatives some of you may suggest? If possible could you maybe keep it on the serious side, with some good suggestions?

Thanks,
Pseudomind

Answer:

Dear Pseudomind,

You can use the same domain name for internal and external network resources. In fact, Microsoft often recommends this configuration because it makes management easier. However, in order to make this work, you need to create a split DNS.

A split DNS allows internal network clients to access resources on the internal network without being dependent on a public DNS server. Only Internet hosts should use the public DNS zone. Internal network clients need to use the internal network zone, even though the two zones have the same domain name and may even have the same resource records.

In your situation, it sounds like you have a Web site hosted by an ISP that uses the same domain name as your internal network domain. You need to create your own DNS server and then enter the public IP address for the site in your private DNS. For example, if the internal network domain is mysite.com, then you need to put an entry in the DNS for www.mysite.com and enter the public address of the server. Other resources on the internal network would have private IP address entries that are valid on your internal network.

This is an even more important issue when you choose to publish resources on the internal network so that Internet users can access them. You do not want internal network users looping back through the firewall to access resources on the internal network. You can avoid this by creating a split DNS, so that internal network clients use a DNS server that resolves these publicly accessible servers to their IP addresses on the internal network.

For more information on split DNS configuration, **check this out**.

Security Advisories

Symantec Provides Free Bugbear Removal Tool

to top

The Bugbear virus is making the rounds on the Internet. If you haven't been stung, consider yourself lucky. If you have been nailed by the virus, you can get a free Bugbear removal tool from Symantec.

Read more...

Apache Fixes Flaw in Web Server

to top

There is a vulnerability in the Apache shared memory scoreboard which is stored in a shared memory segment. Any user who can obtain execution permissions under the Apache UID can send commands to any process as root and, in many cases, terminate the process causing a DoS condition. The Apache Software Foundation has released a fix. Check out the article for details.

Read more...

The SANS/FBI Top 20 Security Vulnerabilities List

▲ to top

You might be aware of the FBI's most wanted list. It's a list of the most dangerous criminals the FBI is looking for. But the FBI has teamed up with SANS to create a most wanted list of security vulnerabilities. They have a top ten Windows list and a top ten UNIX list. A must read for all network admins.

Read more...

News Headlines and Resources

Any Port in a Storm: Understanding Buses and Ports

▲ to top

What's the different between a serial port, a parallel port and an iLink port? There are so many ports on modern computers, it's sometimes hard to tell the players without a scorecard! In this article, Deb Shinder reviews the current state of computer ports and helps make sense of them all.

Read more...

Microsoft Polishing Off .NET Server Software

▲ to top

Microsoft .NET Server is quickly approaching RC2 status. Chances are there will be an RC3 version, and then final release sometime in the first quarter of next year. If you're thinking .NET is in your future, you might want to get on board with the corporate preview program.

Read more...
Read more...

Windows 2000 Cluster Service Reduces Maintenance Downtime

▲ to top

Uptime, uptime, uptime! The Microsoft Cluster service is one of the key components of your Windows 2000 Server's fault tolerance configuration. Getting it to work isn't a no-brainer, but Carol Bailey does a great job on walking you through the tough parts in this article. A definite must read if you plan on using Windows 2000 in a highly available datacenter.

Read more...

Systems Management Server 2003 Reviewer's Guide

▲ to top

Do you use Systems Management Server (SMS)? If so, you might be interested in the next version, SMS 2003. The next version adds a lot of cool tools and features that will help your network management go more smoothly and reliable than ever! If you're thinking of participating in the beta, or are participating it in now, then check out the Reviewers Guide.

Read more...

Microsoft Operations Manager 2000 Operations Guide

to top

Microsoft Operations Manager (MOM) allows you to monitor key servers and server services on your network. It's a fairly new product, so information on how to get it up and running is pretty sparse. Microsoft helps you out with a nine chapter operations guide on how to get MOM purring like a kitten.

Read more...

How to Increase Outlook Web Access Performance

to top

Outlook Web Access (OWA) allows you to use your browser to connect to an Exchange Server. It's a great tool for users who don't have a copy of Outlook easily available. But a major complaint users have is poor performance. This article gives you many tips and tricks you can use to speed up that OWA site!

Read more...

Windows 2000 Service Pack 3: Notes from the Field

to top

No one likes to install service packs without seeing what's happened to other people first. In this article, Christopher Rick has collected a number of notes from people who took the plunge and installed SP3. Makes for some very interesting reading!

Read more...

Download of the Week

PostCast Server

to top

Do you need to send a newsletter, an announcement, or a flyer to thousands of people? No, I'm not talking about spamming! This program allows you to send messages to your own SMTP server, rather than depending on a third party. It gives you more control over the source domain, and you don't need a dedicated Internet connection for it to work. If you need to do some legit mass mailings, the PostCast Server may be just what you're looking for. Best of all, it's FREE.

Read more...

□ □ A+ Weekly

□ ● ByteBack!

□ □ Cisco Insider

□ □ Developers Digest

● □ Exam Tips 'N Tricks

□ ● IT Career Tips

● □ Linux News

□ ● Must Know News

□ ● .NET Insider

● □ Script Shots

□ □ Security Insider

● □ Trainers News

Enter your Email

Subscribe Now!

CramSession
Prepare for Success!

Your subscribed e-mail address is:steven.thode@toadworld.net
To unsubscribe, simply click here and hit "send" in your e-mail reader.