Global Information Assurance Certification Paper

Web Page designed with PHP Nuke 3.0 exploit

SANS Institute Incident Handling and Hacker Exploits Practical Assignment

Prepared by
Marc Morissette
Network Engineer

Executive Details

Name: PHP Nuke 3.0 exploit
Variants: N/A
Operating System: Linux
Protocols/Services: Apache Web Server, PHP & MySQL
Brief Description: When installed on a web server, the software allows administrator access by typing in URL string commands

What is PHP Nuke?

PHP Nuke is a "Web Portal System, storytelling software, News system, online community or whatever you want to call it. The goal of PHP-Nuke is to have an automated web site to distribute news and articles with users system. Each user can submit comments to discuss the articles, just similar to Slashdot and many others."

PHP Nuke is a shareware program, and can be downloaded free under a GPL license from its website http://www.ncc.org.ve/php-nuke.php3?op=english. The operating system that is used on is Linux, thus making this web portal very attractive as a low cost server solution. No knowledge of HTML is required, as all layouts and designs are done via an administrative menu. Users use the standard HTTP TCP port 80 to access a PHP-Nuke web site

PHP Nuke is written with PHP, and requires Apache Web Server, PHP3 and MySQL. And many of its features include: web based admin, surveys, top page, access stats page with counter, user customizable box, themes manager for registered users, friendly administration GUI with graphic topic manager, option to edit or delete stories, option to delete comments, moderation system, Referrers page to know who link us, sections manager, customizable HTML blocks, user and authors edit, an integrated Banners Ads system, search engine, backend/headlines generation (RSS/RDF format), Yahoo like search engine, Comments option in Polls, 9 themes and a lot more. Support is available for 9 different languages. As you can see, it a very powerful and useful tool for a small business or non-profit organization. Other products that are similar are Slash, PHPweblog, Thatware, Sips, and NewsPro.

As mentioned earlier, administrators design and create their web site via an administrative menu, an example is shown below.

Once an administrator is logged in, they have access to the entire web page/portal, along with the server and its services. The purpose of this menu is to create the web site with little or no knowledge of HTML, and to get the site up and working in as short as time and money as possible. This especially includes training for an administrator. As the administrator gets up to speed, they can change the look and items found in the administrative menu.

So, what's the Exploit?

The software has a bug that allows non-administrative users (the public) administrative rights by using the affected web site's URL string. There are slight variations on the string, but they start from one single URL string.

To gain administrative access to the web site using PHP Nuke, all a user must type is the following in their favorite web browser

http://www.targetsite.com/admin.php3?admin

This will bring up a login and password screen as shown below on the *Stop Domestic Violence* web site, http://www.stopdv.org/admin.php3?admin. (PHP Nuke 3.0).

From this point, the user must know the Admin ID and password to gain access to the system. This is useful tool for system administration functions to the web site. System administrators are confident that without this info, their site is safe. However, by using some session hijacking or social engineering, a hacker can obtain this information and log into the web site with administrator privileges. In addition, the administrator's page contains menu items that, while are inaccessible without the ID/password authentication, can be useful in a hacker's later attacks. It is a case of giving away too much information to the public.

So, unless the hacker has the admin ID and password, this web site is useless to them. However, by adding additional text to the URL, we can circumnavigate around the administrator login screen. This is as follows,

http://www.targetsite.com/admin.php3?admin=anything&op=PostAdminStory&introtext=whatever%20you%20want%20to%20say

where "whatever you want to say" is either string of text or HTML code or pointer to another site. Using the %20 HTML code will separate the text to be typed in. This will post the hacker's message on the site's main web page. Or it will re-direct traffic to the hacker's site. Whatever the hacker chooses.

Now, by using a slight deviation of the above URL, we can perform any of the admin tasks on the menus. Let's take another look at the Stop Domestic Violence web site admin page

You will notice on the Main Menu there are items ranging from Home to Create Account, from Sections to Stats for the server. By issuing the following URL, a hacker can access any of these items using the administrator account

http://www.targetsite.com/admin.php3?admin=anything&op=task

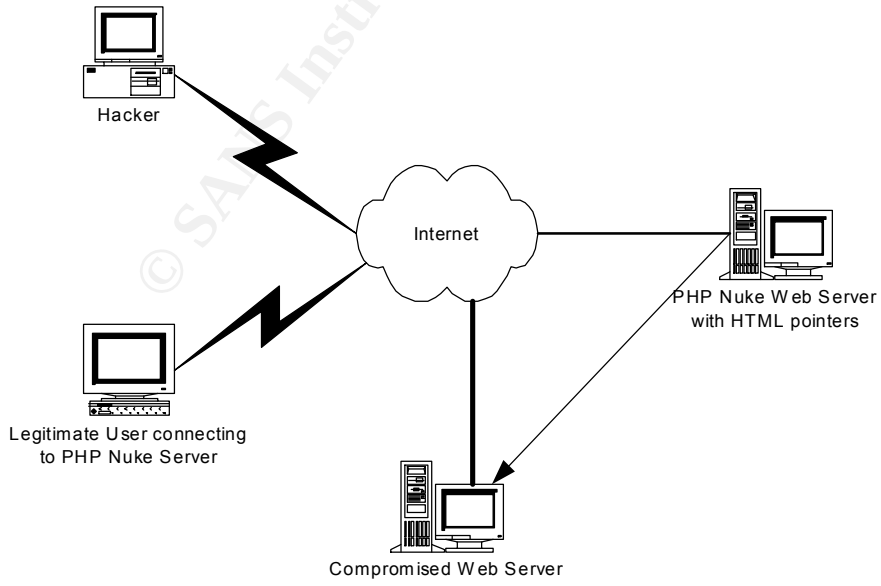
where "task" is any item on the menus. As you can imagine, this is a very serious threat, especially when user account creation and rights are issued from the menu!

Typical Hacker Attack Pattern

A typical attack on this type of web site would consist of a hacker obtaining the URL of the main page, and determining it is created with PHP Nuke. Or they can look it up on PHP Nuke's web site listed above. They have some of the sites linked to their page. Once they have the URL, they issue the URL http://www.targetsite.com/admin.php3?admin. This will get them a look at the administrator's page, and a listing of the administrator's menu items. Next they issue the command http://www.targetsite.com/admin.php3?admin=aything&op=task, where the task listed would allow them to create a backdoor account with administrator privileges, or if listed on the menu, a root level Linux account. The hacker can then add, change or redirect users to obscene, offensive, material, or can set up a web page that "collects" credit card numbers to be used or sold off.

The hacker would be accessing the server from over the Internet, possibly from a spoofed IP address. If they decide to re-direct Internet traffic to another site, this server will probably, but not always, be a server that has already been compromised using another vulnerability. Please refer to the following diagram.

Hacker Attack



What are the safe guards

Unfortunately, since the attack does look legitimate to your web server and network, there is no real fast fix for the solution. However, the good news is the author of PHP Nuke, Francisco Burzi, has put published a patch to his program that will shut down the hole used to bypass the administrator login. (http://www.ncc.org.we/php-nuke.php3?op=download&location=http://download.sourceforge.net/phpnuke&file=PHP-Nuke-3.0.tar.gz). Any system administrator running PHP Nuke 3.0 must download this patch and apply it to secure their web page. The problem is that it the exploit and patch are not well published, and system administrators may not be aware of the problem. The patch does not change the Administrator's page, so the menu choices are still visible for the public to see.

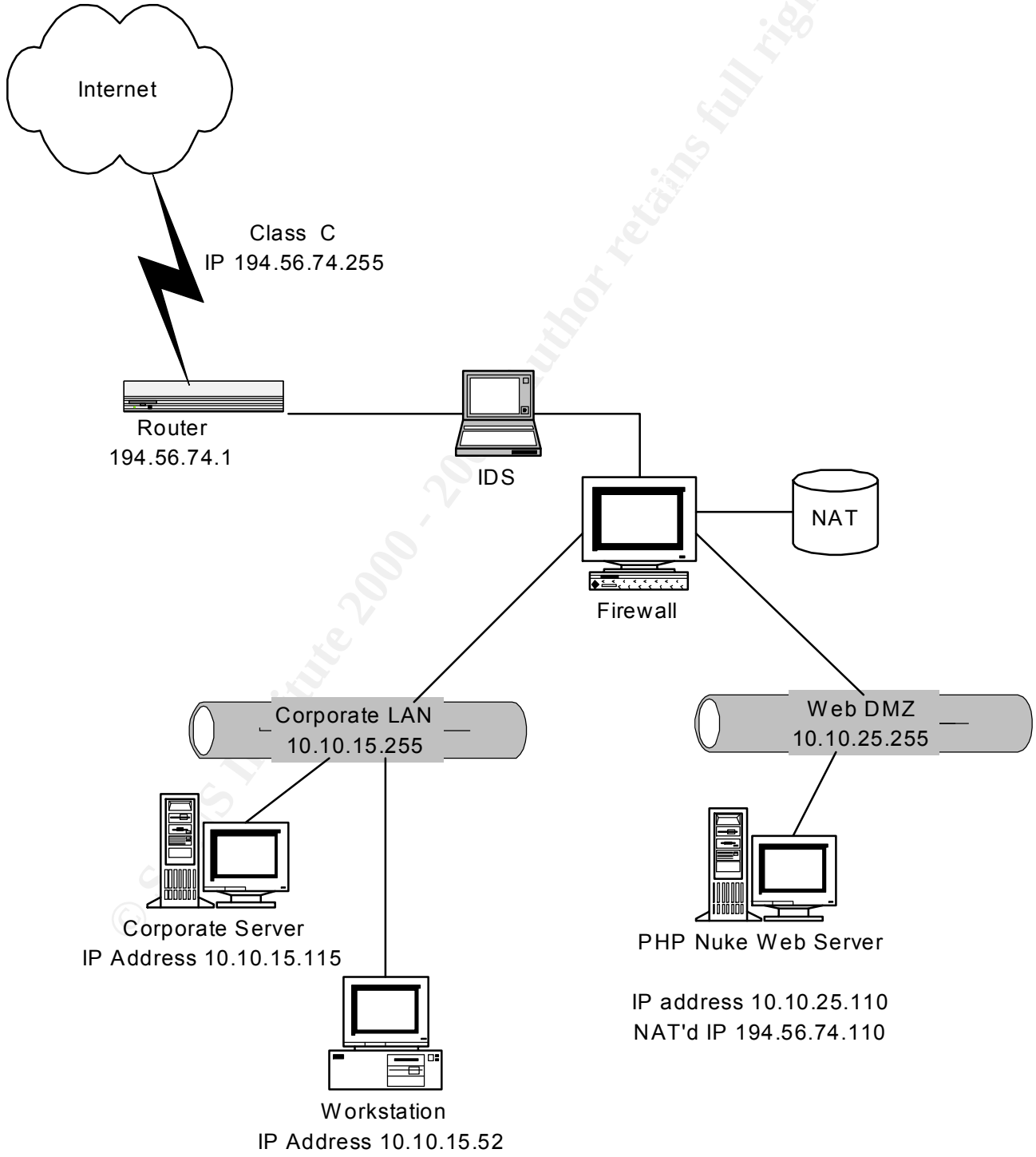
However, a patch that would not reveal the administrator menu until after authentication would provide more security. And as always, know your system. What files are there, what accounts are created, etc. If an account shows up that you are not familiar with, this is a good sign that an incident has occurred. Isolating your web server on another segment or DMZ would offer added protection from the rest of your servers, and do not establish trust relationships with the Web servers and "Corporate" servers. A firewall that can identify a "spoofed" IP address between the DMZ and the Internet connection would help identify legitimate users and hackers

Although the goal of this software is to add web page functionality to a small or non-profit organization, training of system administrators on web design and HTML, so they can by-pass the administrator's web-based menu for system administration functions, would then eliminate the need for this menu, and can be thus eliminated from the application.

One final thought for safeguarding against this and similar types of this vulnerability. The use of a separate TCP port for admin functions can identify traffic through the use of an intrusion detection network filter. If packets are being sent from an outside or unknown IP address on the specific port for admin functions, a "red flag" is identified and can be dealt with quickly. Only known or inside IP address can also only be allowed through a firewall rule for the admin TCP port. Let's look at the example on the next few pages.

Example

Non-profit organization GoodHeart has the following network.



The firewall has the following configuration;

Objects

Web Server
Name: PHPWS
IP: 10.10.25.110 NAT: 194.56.74.110

Workstation
Name: MGMT
IP: 10.10.15.52

RuleSet

Rule No.	Source	Destination	Service	Action	Log
1	Any	PHPWS	http	Allow	Long
2	MGMT	PHPWS	http_admin	Allow	Short
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
11	Any	Any	Any	Deny	Long

Services

http_admin
Protocol: TCP
Port: 44000

http
Protocol: TCP
Port: 80

Using this network configuration, the system administrator sets up the PHP Nuke admin page to be accessible only on port 44000. This is done via the administration menu item, *Admin Block*.

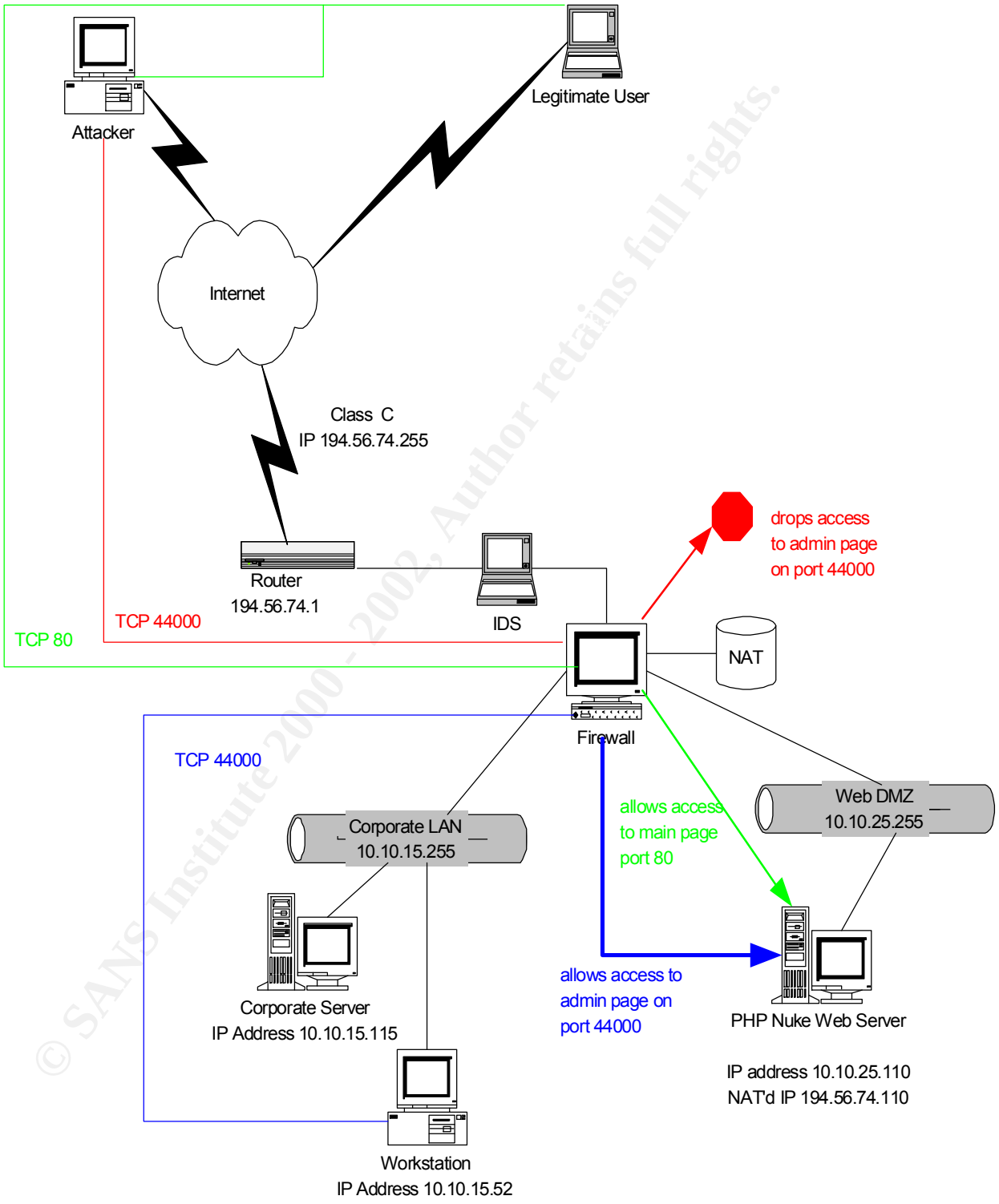
The firewall ruleset only allows an internal IP address to access this port on the web server. Any attempts from an outside IP address are denied and logged to the firewall log.

The IDS box on the outside of the firewall listens to the network, and if any traffic from the Internet comes on port 44000 to the web server, an alert is triggered. The alert simply tells the system administrator that a non-authorized IP address is trying to access the Admin Page. The system administrator can then determine if this is an incident or not.

By using an internal IP address scheme, the real IP address of the web server is hidden from the general public. This will help prevent any IP spoofing, protecting the IP address of the administration workstation.

The firewall ruleset will protect the admin page, but will allow legitimate users through to the main web page, as shown in the following diagram

Firewall permissions network schematic



Summary

As you can see, PHP Nuke 3.0 is a powerful, low-cost web portal program that is easy to use. First time web administrators will like the ease of use to maintain and design award winning web pages. However, as with most things, the easier to use, the more dangerous it can become. First time hackers, Script kiddies and advanced hackers can cause some major damage to the organizations with simple but effective URL strings.

With the patch, a web site is somewhat secured, but until the menus are placed on the page *after* the authentication page, web sites with the software are open for attack. By placing the web server in a DMZ that can be filtered through a firewall and IDS, and accessing the admin page on a different TCP port, a system administrator can reduce the security risks, and still maintain a high profile, high user profile web server.

Sources

1. Many thanks to Starman_Jones, a regular contributor to the BUGTRAQ mailing list, for his input and for actually trying out the exploits.

2. http://www.stopov.com; This site was used in a few scenarios, and actual screen shots of their pages are contain in this document.

3. http://www.hotscripts.com; Quotes and research.

4. http://www.ncc.org.ve/php-nuke.php3; Research and a copy of PHP Nuke

5. Francisco Burzi; Again, help with research and the patch to the application.