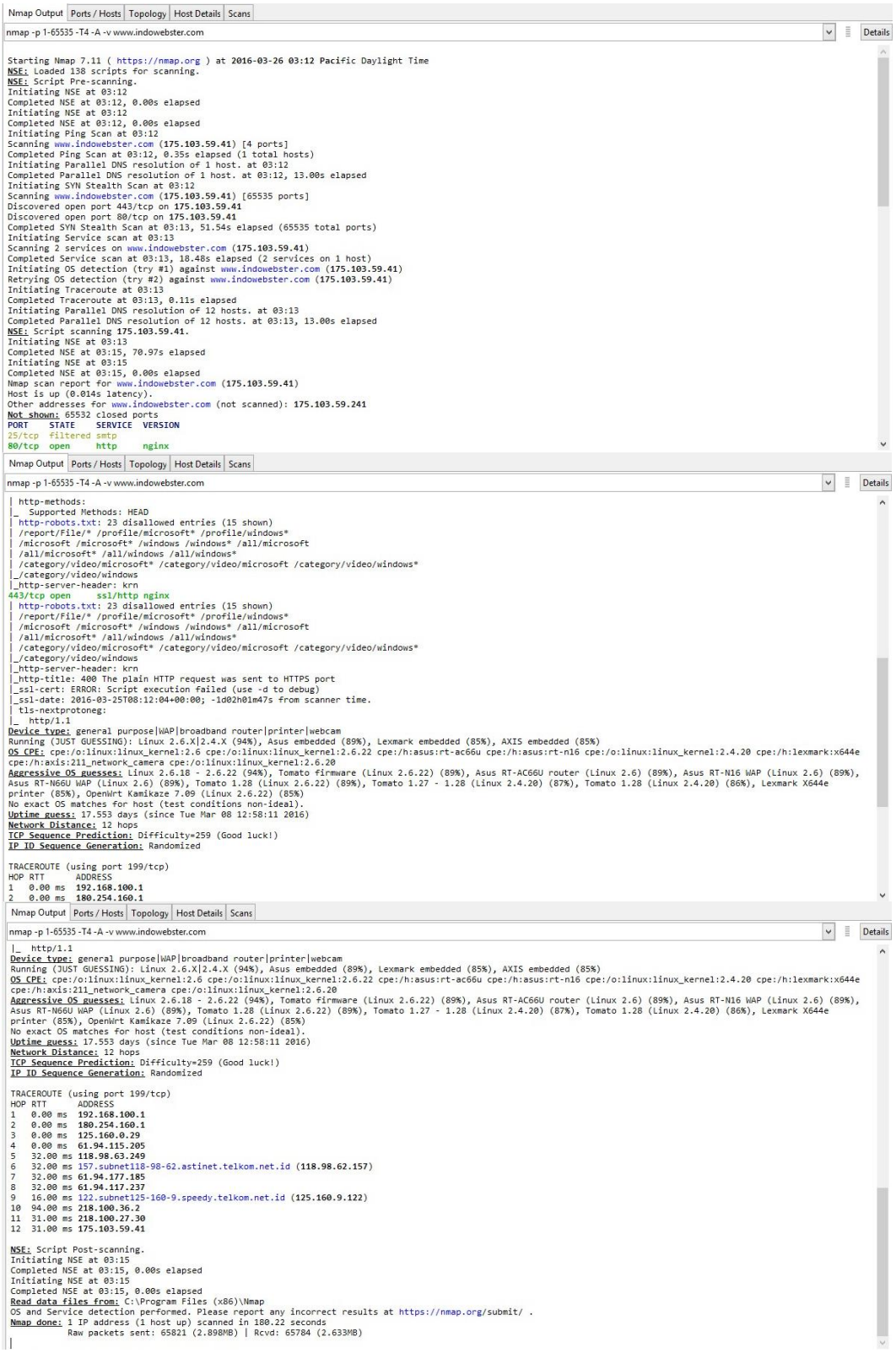
TUGAS

Oleh :

Romi Bagaskara
09121001015

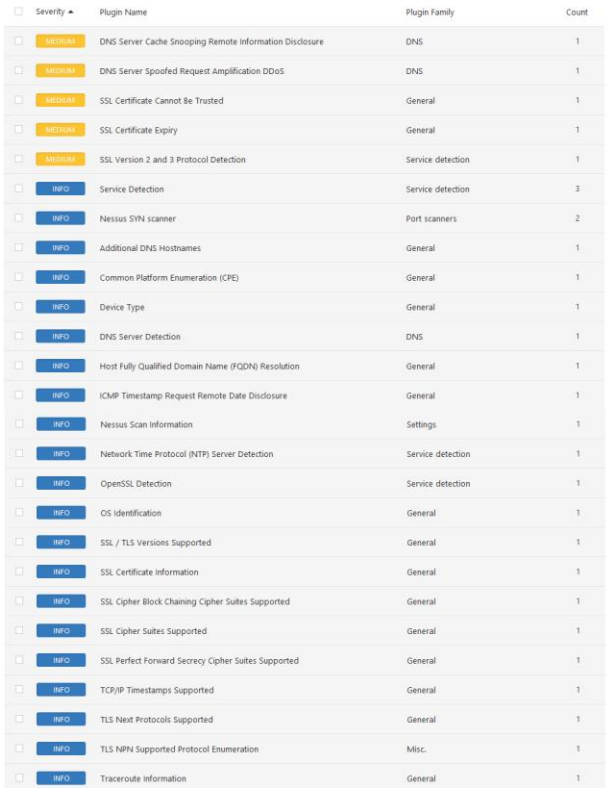
SISTEM KOMPUTER
UNIVERSITAS SRIWIJAYA
PALEMBANG
2016

Berikut ini adalah hasil Scanning pada domain www.indowebster.com menggunakan Nmap – ZenMap GUI :



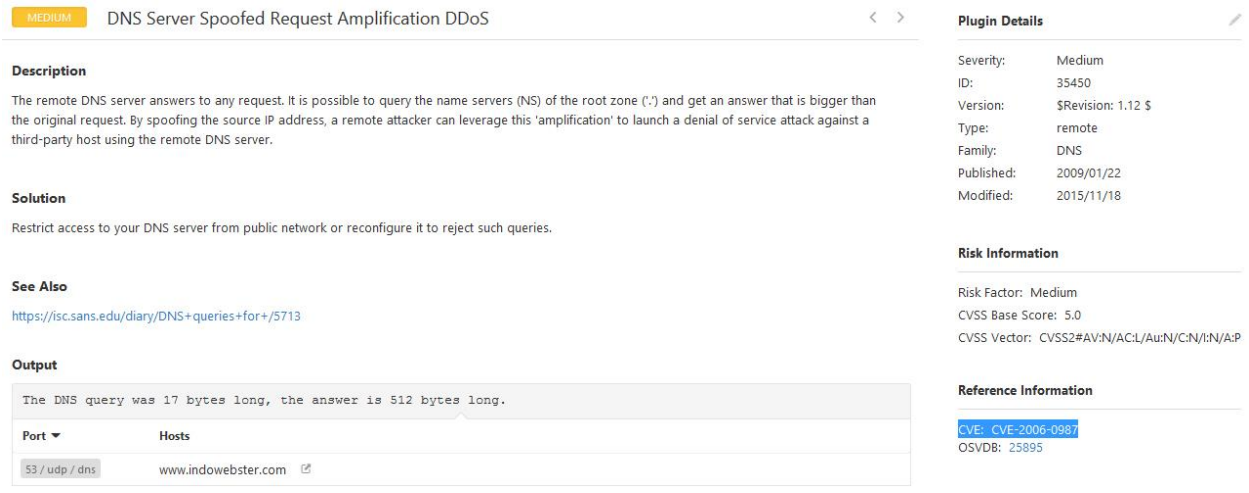
Dari hasil scanning diatas, domain www.indowebster.com menggunakan OS Linux Kernel 2.2 dan memiliki dua buah port yang terbuka, yaitu port 80/tcp dan port 443/tcp. Port 80/tcp merupakan port HTTP World Wide Web dari domain itu sendiri dan port 443/tcp adalah protokol yang didefinisikan untuk berkomunikasi tergantung pada aplikasi.

Untuk scanning domain www.indowebster.com menggunakan Nessus, berikut ini adalah hasil scan pertama melalu Nessus :



Severity	Plugin Name	Plugin Family	Count
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	DNS	1
MEDIUM	DNS Server Spoofed Request Amplification DDoS	DNS	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Certificate Expiry	General	1
MEDIUM	SSL Version 2 and 3 Protocol Detection	Service detection	1
INFO	Service Detection	Service detection	3
INFO	Nessus SYN scanner	Port scanners	2
INFO	Additional DNS Hostnames	General	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	DNS Server Detection	DNS	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	Nessus Scan Information	Settings	1
INFO	Network Time Protocol (NTP) Server Detection	Service detection	1
INFO	OpenSSL Detection	Service detection	1
INFO	OS Identification	General	1
INFO	SSL / TLS Versions Supported	General	1
INFO	SSL Certificate Information	General	1
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1
INFO	SSL Cipher Suites Supported	General	1
INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1
INFO	TCP/IP Timestamps Supported	General	1
INFO	TLS Next Protocols Supported	General	1
INFO	TLS NPN Supported Protocol Enumeration	Misc.	1
INFO	Traceroute Information	General	1

Setelah mendapatkan hasil scan kemudian memilih “DNS Server Spoofed Request Amplification DDoS”, telah didapat CVE nya yaitu “CVE-2006-0987”



MEDIUM DNS Server Spoofed Request Amplification DDoS

Description

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

Solution

Restrict access to your DNS server from public network or reconfigure it to reject such queries.

See Also

https://isc.sans.edu/diary/DNS+queries+for+/5713

Output

```
The DNS query was 17 bytes long, the answer is 512 bytes long.
```

Port	Hosts
53 / udp / dns	www.indowebster.com

Plugin Details

Severity:	Medium
ID:	35450
Version:	$Revision: 1.12 $
Type:	remote
Family:	DNS
Published:	2009/01/22
Modified:	2015/11/18

Risk Information

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

Reference Information

CVE: CVE-2006-0987
OSVDB: 25895

Berikut adalah mapping CVE dari domain www.indowebster.com :

CVE-ID	
CVE-2006-0987	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
The default configuration of ISC BIND before 9.4.1-P1, when configured as a caching name server, allows recursive queries and provides additional delegation information to arbitrary IP addresses, which allows remote attackers to cause a denial of service (traffic amplification) via DNS queries with spoofed source IP addresses.	

CVE-ID	
CVE-2007-0987	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Directory traversal vulnerability in index.php in Jupiter CMS 1.1.5 allows remote attackers to include and execute arbitrary local files via a .. (dot dot), or an absolute pathname, in the n parameter.	

CVE-ID	
CVE-2008-0987	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Stack-based buffer overflow in Image Raw in Apple Mac OS X 10.5.2, and Digital Camera RAW Compatibility before Update 2.0 for Aperture 2 and iPhoto 7.1.2, allows remote attackers to execute arbitrary code via a crafted Adobe Digital Negative (DNG) image.	

CVE-ID	
CVE-2009-0987	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Unspecified vulnerability in the Upgrade component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.3 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	

CVE-ID	
CVE-2010-0987	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Heap-based buffer overflow in Adobe Shockwave Player before 11.5.7.609 might allow remote attackers to execute arbitrary code via crafted embedded fonts in a Shockwave file.	

CVE-ID	
CVE-2011-0987	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
The PMA_Bookmark_get function in libraries/bookmark.lib.php in phpMyAdmin 2.11.x before 2.11.11.3, and 3.3.x before 3.3.9.2, does not properly restrict bookmark queries, which makes it easier for remote authenticated users to trigger another user's execution of a SQL query by creating a bookmark.	