Penetraciono testiranje

Nmap (the Network Mapper) Alat

Testiranje ranjivosti sistema je izvršeno uz pomoć Nmap alata i to sa komandom *nmap --script vuln*. Ova komanda pokreće skripte koje testiraju odnosno traže ranjivost sistema koji se nalazi na ip adresi proslijeđenoj komandi.

Glavni dijelovi izvještaja dobijenog testiranjem **admin aplikacije** (komanda *nmap -p 8080 -v -v --script vuln localhost*):

PORT STATE SERVICE REASON

8080/tcp open http-proxy syn-ack ttl 128

|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php

|_http-jsonp-detection: Couldn't find any JSONP endpoints.

|_ssl-dh-params:

| VULNERABLE:

| Diffie-Hellman Key Exchange Insufficient Group Strength

| State: VULNERABLE

| Transport Layer Security (TLS) services that use Diffie-Hellman groups

| of insufficient strength, especially those using one of a few commonly

| shared groups, may be susceptible to passive eavesdropping attacks.

| Check results:

| WEAK DH GROUP 1

| Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

| Modulus Type: Safe prime

| Modulus Source: RFC2409/Oakley Group 2

| Modulus Length: 1024

| Generator Length: 8

| Public Key Length: 1024

| References:

|_ https://weakdh.org

|_http-slowloris-check:

| VULNERABLE:

| Slowloris DOS attack

| State: LIKELY VULNERABLE

| IDs: CVE:CVE-2007-6750

| Slowloris tries to keep many connections to the target web server open and hold

| them open as long as possible. It accomplishes this by opening connections to

| the target web server and sending a partial request. By doing so, it starves

| the http server's resources causing Denial Of Service.

|

| Disclosure date: 2009-09-17

| References:

| http://ha.ckers.org/slowloris/

|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750

Glavni dijelovi izvještaja dobijenog testiranjem **myhome aplikacije** (komanda *nmap -p 8081 -v -v --script vuln localhost*):

PORT STATE SERVICE REASON

8081/tcp open blackice-icecap syn-ack ttl 128

|_ssl-dh-params:

| VULNERABLE:

| Diffie-Hellman Key Exchange Insufficient Group Strength

| State: VULNERABLE

| Transport Layer Security (TLS) services that use Diffie-Hellman groups

| of insufficient strength, especially those using one of a few commonly

| shared groups, may be susceptible to passive eavesdropping attacks.

| Check results:

| WEAK DH GROUP 1

| Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

| Modulus Type: Safe prime

| Modulus Source: RFC2409/Oakley Group 2

| Modulus Length: 1024

| Generator Length: 8

| Public Key Length: 1024

| References:

|_ https://weakdh.org