Intro to Penetration Testing: Enumeration

October 11th, 2017
Brown Bag Talks

Friday at 11:00 AM
What is Enumeration

Gathering the follow:

- Usernames, Group names, Hostnames
- Network shares
- Services and Versions
- DNS, SNMP, SMB

Reason for gathering:

- To get initial access
- To perform lateral movement
- To make exploitation easier
Tools for Enumeration

- Nmap -- Network mapping and port scanner
- Nessus/Openvas -- Services, vulnerability, leak scanner
- gobuster/dirb -- Directory bruteforcer
- Nikto -- Web server scanner
- WPScan -- WordPress scanner
- Searchsploit -- connected to exploit.db to search for exploits
WARNING!!!

- Enumeration can get you banned from services and can be considered illegal activity

For practice
Nmap

- Nmap -sP <IPADDRESS>/<SUBNET> = Ping scans the networks, listing machines that respond to ping
- Nmap -p 1-65535 -sV -sS <IPADDRESS> = Full TCP port scan finding services and versions
- Nmap -v -sS -A <IPADDRESS> = Prints verbose output, runs stealth syn scan, finds OS and detects version
- Nmap -sV -Pn -oX target.xml <IPADDRESS> = Scans for open ports and service version with no pings sent to target then saves output to target.xml
Searchsploit

- Searchsploit --nmap target.xml = Search for exploits with the nmap output
- Quick and easy way to see exploits without scanning the target twice
Nessus / Openvas

Pros:

- Scans everything you specified
- Can show vulnerabilities and types
- Multiple ip’s at once

Cons:

- Sends a lot of data to target
- Can be slow depending on target
- Target can block your IP
Nikto / WPScan
+ Target IP: 74.217.87.87
+ Target Hostname: websccontest.com
+ Target Port: 80
+ Start Time: 2014-03-16 13:23:30 (GMT0)

+ Server: Apache
+ Cookie SESSIONID_VULN_SITE created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.3
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use `-C all` to force check all possible dirs)
+ Server leaks inodes via ElTags, header found with file /robots.txt, inode: 4920
56, size: 101, mtime: 6x4f135f9b82c00
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microso
ft.com/en-us/library/e8z01xch%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X ST
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals poten
tially sensitive information via certain HTTP requests that contain specific QUERY st
ings.
+ OSVDB-3092: /cart/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 6544 items checked: 6 error(s) and 13 item(s) reported on remote host
+ End Time: 2014-03-16 13:43:12 (GMT0) (1182 seconds)

+ 1 host(s) tested
URL: http://192.168.0.13/wordpress/

Started: Mon May 11 04:00:23 2015

The WordPress 'http://192.168.0.13/wordpress/readme.txt' exists exposing a version number
Full Path Disclosure (FPD) in: 'http://192.168.0.13/wordpress/wp-includes/rss-functions.php'
Interesting header: SERVER: Apache/2.4.12 (Ubuntu)
Interesting header: WP-SUPER-CACHE:
Interesting header: X-POWERED-BY:
XML-RPC Interface available under: http://192.168.0.13/wordpress/xmlrpc.php
This may allow the GHOST vulnerability to be exploited, please see: https://www.rapid7.com/db/m
Upload directory has direct access enabled: http://192.168.0.13/wordpress/wp-content/uploads

WordPress version 4.2.2 identified from meta generator

WordPress theme in use: twentyfifteen - v1.1

Name: twentyfifteen - v1.1
Location: http://192.168.0.13/wordpress/wp-content/themes/twentyfifteen/
Readme: http://192.168.0.13/wordpress/wp-content/themes/twentyfifteen/readme.txt
Style URL: http://192.168.0.13/wordpress/wp-content/themes/twentyfifteen/style.css

Title: Twenty Fifteen Theme <= 1.1 - DOM Cross-Site Scripting (XSS)
References: https://www.nbdc.org/vulnerabilities/2055
One user: root

<table>
<thead>
<tr>
<th>Id</th>
<th>Login</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>root</td>
<td>root</td>
</tr>
</tbody>
</table>
Gobuster / Dirb / Dirbuster

Pros:

- Finding obscure directories
- Finding information quickly
- Enumerating the entire file server

Cons:

- Very Loud
- Can cause IP Ban
- Can often prove to be useless
Questions?