SANS Penetration Testing

23 Jan **2019**

Web Application Scanning Automation

0 comments Posted by sanspentest
Filed under web pen testing

Some functions within penetration testing can be mundane and repetitive. To feed some life into these parts of the test, it can be fun and challenging to develop an automation script for these elements of an assessment. Furthermore, automating parts of a penetration test can help the output to be more consistent, reproducible, rigorous, and introduce some quality control as suggested by the OWASP Testing Methodology[1]. This article will introduce a few features of nmap and Nikto that support script automation, and walk through building a simple starter automation script.

Ready, Aim, FIRE!

To feed your automation, you will need a way to document your target information. Frequently a flat-text file with one target per line is sufficient. Other formats, such as XML, may be helpful depending on the tools you intend to use within your automated scripts.

Most command-line tools have features, such as reading target information from files, that facilitate automation nicely.

NMAP

The popular port scanning tool, nmap[2], can read a list of targets from a file through the "-iL" switch. For nmap, the file can specify targets in the same format that they can be listed on the command line, and multiple target designations can be placed on separate lines.

The following sample shows the flexibility nmap offers in the formatting of files it can read through the "-iL" switch:

```
192.168.17.34
10.23-25.0.0/24
172.16.1.1-10
```

Table 1: Sample nmap "targets.txt" File

The nmap tool also permits the results to be saved into several different formats:

- Normal: The same output as nmap sends to STDOUTXML:
- The results in XML data structure
- Greppable: Output with scan results for each host on a single line
- Script Kiddie: Results are in "L33T" speak

Using the "-oA" switch, nmap will output the results into three (3) separate files associated with the first three (3) output options listed above.

These file outputs will become the inputs for other tools to select targets.

Putting the input and output options together, the following nmap command will read in targets from the "targets.txt" file and output results to the three (3) useful file formats.

```
nmap -iL targets.txt -oA $(date +%Y%m%d)_nmap_tcp
```

Table 2: Example nmap Command

The "$(date +%Y%m%d)" portion of the filename in the previous command causes the current date to be prepended to the file names nmap creates.

Nikto

A tool commonly used to perform initial web application scans is Nikto[3]. Nikto looks for common web application vulnerabilities associated with outdated software, misconfigurations and dangerous files.

Nikto's ability to read an nmap greppable format file, a flat-text file with targets listed within, and the specification of a target on the command line makes target selection versatile. Each of these ways to target hosts can be specified by using the "-h" switch.

There are several conditions in which Nikto may prompt for further input, pausing the scan process until a response is received. To prevent a situation where Nikto is waiting for feedback, rather than scanning targets, the following switches can be used to disable prompts.

- -ask no: disables the prompt that asks if you want to submit new banners for software identified while scanning.
- -nointeractive: disables all other prompts.

Like nmap, Nikto has the ability to save results to multiple file formats by using the "-Format" switch. Some of the formats available include those in the following list:

- -Format HTM: Saves an HTML formatted report.
- -Format CSV: Saves Nikto's results in comma separated value format.
- -Format XML: Results are stored in XML format.

Multiple file types can be specified after the "-Format" switch by separating them with a comma.

Additionally, Nikto can save a replay file associated with each finding it reports, making it easy to jump in and verify findings or exploit the vulnerability.

The following example Nikto command reads the "nmap_output.gnmap" file for hosts for which the HTTP/HTTPS protocol was discovered, disables all interactive prompts, and saves a report in the "nikto_nmap-scans.html" file using HTML format.

```
nikto -host nmap_output.gnmap -ask no —nointeractive -Format htm -output nikto_nmap-scans.html
```

Table 3: Example Nikto Command

Automation: Bash Script Magic

Armed with script specific features of nmap and Nikto, it is time to build a basic automation script. This script can be used to begin the automation process, and expanded to include more tools.

Script Setup

To start the script out, it is best to define the path to the command interpreter you want the script to use, in this case we will point to bash. Afterwards, the definition of a couple variables, "ports" and "date", will be useful for this script.

- **ports**: Stores the list of ports Nikto will scan. For this starter script the focus will be on 80/tcp and 443/tcp.

- **date**: Stores the date to use as a timestamp in filenames.

The beginning of the script will look like this:

```
#!/bin/bash
ports="80 443"
curdate=$(date +%Y%m%d)
```

Table 4: Start of Automation Script

The $(date +%Y%m%d)is used to execute the date command with parameters to specify the format YYYYMMDD and its output will be stored in the $curdate variable.

Grab Those IPs

The tools run by the script will need the IP addresses of the targets to run. There are many tactics to provide the targeting details, some of which are dependent upon the tool's capabilities. Though Nikto can read a greppable nmap output file, for demonstration purposes let's look at how the addresses can be pulled from nmap's output.

Grep is a tool that searches through a file and returns the line that matches a specified query.

- The following grep command could return the results shown below:

```
grep '80/open' $curdate\_nmap_tcp.gnmap
Host: 10.10.10.10 () Ports: 80/open/tcp//http///
```

Table 5: Grep Command to Find Lines with Port 80/tcp

The cut command can extract a section of text using a delimiter.

- In the following example, a will be used as the delimiter, and the second "field" will be extracted. Based on the previous output from the grep command, this should isolate the IP address of the host with port 80/tcp available.

```
$grep '80/open' $curdate\_nmap_tcp.gnmap | cut –d ' ' -f2
10.10.10.10
```

Table 6: Grep + Cut to Return Only the IP Address for Systems Listening on Port 80/tcp

Another way to extract the IP address uses the tool awk.

- This command searches for instances where port 80/tcp are reported open, and then prints the second field within each of the search results. By default awk will use whitespace (tabs and spaces) as the field delimiter.

```
$awk '/80\/open/{print $2}' $curdate\_nmap_tcp.gnmap
10.10.10.10
```

Table 7: Another Way to Extract the IP Address using Awk

Note that in the previous commands the "$curdate" variable was used as part of the file name. The "_" in the filename uses the backslash to tell bash that the "_" is a literal underscore character and not part of the "$curdate" variable. Otherwise bash would look for the variable "$curdate_nmap_tcp.gnmap", which does not exist.

Throw Us for a Loop

Bash includes the ability to iterate through a set of items using the `for` loop. A simple example of the `for` loop is:

```
$for a in hello there; do echo $a; done;
hello
there
```

Table 8: Simple for Loop Example

The above loop iterated through the two items `hello` and `there`, then wrote each item to stdout using the echo command.

There are a few features of `for` loops that are useful in scripts.

- The loops can be nested inside of each other to iterate through multiple sets of data. As can be seen in the code snippet below, the script will loop through each of the ports specified in the $ports variable, as well as all the IP addresses inside the nmap output.
- The semicolon (";") can be replaced with a carriage return to make the loop easier to read in a script.
- The set of items the `for` loop will iterate through can be returned by a command.
  - As an example, the following command will loop through each of the results in the ls command, and print them to the screen.

```
for a in $(ls -1); do echo $a; done;
```

Table 9: FOR Loop Using a Command's Results as the Iterable Data

At this point, the details about pulling the IP addresses and the for loops can be combined.

```
for testport in $ports
do for targetip in $(awk '/'$testport'\/open/{print $2}' $curdate\_nmap_tcp.gnmap)
do nikto -host $targetip -ask no —nointeractive
done
done
```

Table 10: FOR Loop to Iterate through Ports and IP Addresses

NOTE: To expand the $testport variable in the search string, the string delimited by the single quotes must be terminated before the variable is referenced, and then resumed afterwards.

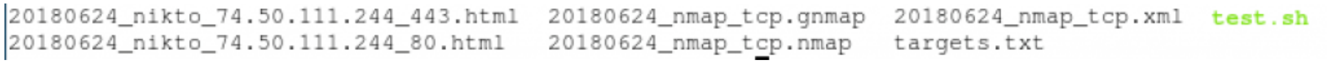
The Initial Automation Script

All the pieces necessary to build the initial automation script have been presented. The following code block puts everything together.

```
#!/bin/bash
ports="80 443"
curdate=$(date +%Y%m%d)
nmap —n -Pn -iL targets.txt -oA $curdate\_nmap_tcp —-reason
for testport in $ports
do for targetip in $(awk '/'$testport'\/open/{print $2}' $curdate\_nmap_tcp.gnmap)
do nikto -host $targetip:$testport -ask no —nointeractive -useragent "Mozilla/5.0 (Windows
NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1" -Format htm -output
$curdate\_nikto_$targetip\_$testport.html
done
done
```

Table 11: The Initial Automation Script

If a targets.txt file contains the target hack.me in the same folder as the automation script (test.sh in this case), the following files will be present in the directory from which the script is run.



```
20180624_nikto_74.50.111.244_443.html  20180624_nmap_tcp.gnmap  20180624_nmap_tcp.xml  test.sh
20180624_nikto_74.50.111.244_80.html   20180624_nmap_tcp.nmap   targets.txt
```

Screenshot 1: Files Created by the Initial Automation Script

An Alternative Path

Leveraging Nikto's ability to read target details from nmap's greppable formatted output, another way the script could be written is provided below.

```
#!/bin/bash
curdate=$(date +%Y%m%d)
nmap —n -Pn -iL targets.txt -oA $curdate\_nmap_tcp —reason
nikto -host $curdate\_nmap_tcp.gnmap -ask no —nointeractive -useragent "Mozilla/5.0 (Windows
NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1" -Format htm —output .
```

Table 12: An Alternative Initial Automation Script

The alternative version of the script differs from the first script in the following ways:

All of Nikto's results for every target will be stored in the same file.
Nikto identifies other ports that nmap reports as using http/https protocols, and scans those systems as well.A small amount of flexibility is lost, as the tools are making decisions about what to scan; but, the script is easier to read.

Homework

This article focuses on starting an initial script. Be like the crew members of the Enterprise and go where no hacker has gone before? Change the script, add in your favorite tools, and enjoy the productivity gains from introducing automation to improve your pen test methodology.

More Information

Related Webcast

"Web Application Scanning Automation"

- available: ondemand
- presenter: Timothy McKenzie

Abstract: *Many functions within a penetration test are routine, and using a script to automate portions of the process can provide a consistent, repeatable and auditable process. This presentation will begin with a walk through the command-line switches of a couple well-know tools that aid automation. By the end of the hour, attendees will have an automation script that they can use to run their own tests, and grow to incorporate more of their own tools and methodology.*

Related Course

SEC542: Web App Penetration Testing and Ethical Hacking

Upcoming classroom opportunities with instructor Tim McKenzie include

- Austin, TX - Apr 29
- San Diego, CA - May 9
- Amsterdam - May 20

For the course syllabus, additional classroom opportunities, and online training options, visit the SEC542: Web App Pen Testing and Ethical Hacking course description.

[1] https://www.owasp.org/index.php/Testing:_Introduction_and_objectives

[2] https://nmap.org/

[3] https://github.com/sullo/nikto

Permalink | Comments RSS Feed - Post a comment | Trackback URL

Post a Comment

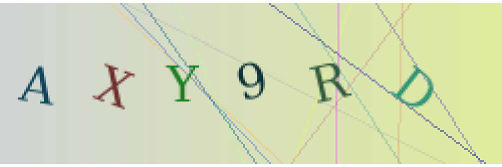
***Name**

***Email**

Website

***Comment**

Captcha



***Response**

Post Comment

* Indicates a required field.

Subscribe to SANS Newsletters

Join the SANS Community to receive the latest curated cyber security news, vulnerabilities and mitigations, training opportunities, and our webcast schedule.

Enter email address...

Enter country...

Subscribe

Share

Categories

- Advanced Web App Pentesting (2)
- Anomaly Analysis (1)
- Anti-Virus Evasion (7)
- Backdoor (2)
- Bash (11)
- Challenge Coins (1)
- Challenges (27)
- Cheatsheet (9)
- cloud (2)
- Command Line Kung Fu (17)
- Conferences (4)
- Cryptography (4)
- CyberCity (1)
- Databases (1)
- Enumeration (2)
- Exploit Development (4)
- File Analysis (2)
- fuzzing (1)
- Infrastructure (4)
- Introduction (3)
- Legal Issues (1)
- Linux (2)
- Metasploit (9)
- Methodology (48)
- Mobile (21)
- Network Devices (3)
- Nmap (2)
- Passwords (7)
- Post Exploitation (13)
- Posters (23)
- PowerShell (8)
- Presentations (10)

- Protocol Analysis (1)
- Python (20)
- Quiz (2)
- Recon (1)
- Reporting (4)
- Scanning (7)
- scapy (3)
- Shell Fu (5)
- Summit (1)
- web pen testing (18)
- Welcome (2)
- wireless (5)
- Writing (2)

Recent Posts

- Tips for Creating a Strong Cybersecurity Assessment Report
- Web Application Scanning Automation
- Secrets to Successful Cybersecurity Writing: Hack the Reader
- Using gdb to Call Random Functions!
- SANS Pen Test Poster: Pivots Payloads Boardgame

Archives

Select Month ▾

Links

- Log in
- Entries RSS
- Comments RSS

Latest Blog Posts

Tips for Creating a Strong Cybersecurity Assessment Report
January 23, 2019 - 11:57 AM

Web Application Scanning Automation
January 23, 2019 - 4:03 AM

Secrets to Successful Cybersecurity Writing: Hack the Reader
January 11, 2019 - 2:00 PM

Latest Tweets @SANSPenTest

Demonstrate how your organization maximizes the value of its [...]
April 19, 2019 - 6:40 PM

SANS #PenTest Pivots &amp; Payloads Poster/Board game is ava [...]
April 16, 2019 - 1:35 PM

Join @lennyzeltser in NYC starting 6/1 to learn how to break [...]
April 14, 2019 - 6:55 PM

Latest Papers

Security Monitoring of Windows Containers
By Peter Di Giorgio

Cyber Threats to the Bioengineering Supply Chain
By Scott Nawrocki

PDF Metadata Extraction with Python
By Christopher Plaisance

"This is the best hands-on course available anywhere."
- Whitney Janes, FedEx

"Ed Skoudis is the best teacher I've ever had. He is 100% competent and professional."
- Petra Klein, FRA

"This was by far the best course I have ever taken."
- Peter Lombars, Intrucom Inc.