Kerberos Username Enumeration – Top 500 Common Usernames

Low Privilege Active Directory Enumeration from a non-Domain Joined Host

JAN
18

Cracking Cisco ASA SHA-512 Hashes with Hashcat

By matt in Passwords

I haven't seen too much detail around about how to crack Cisco ASA PBKDF2 (Password-Based Key Derivation Function 2) SHA-512 hashes, which I believe have been supported in some ASA versions from as early as March 2016.

As always the hashes can be recovered from the appropriate Cisco ASA config file.

Here are some examples of how the hashes can appear in the ASA config files. In the examples below all 3 sample hashes can be easily cracked using any respectable word-list:

```
enable password $sha512$5000$vlCP+V07DGEJ9TcSV/GpuA==$2S8SLoECmbtb/o17ZhXuKg== pbkdf2

username admin password $sha512$5000$SvZkzlRDO115YrLXsZuWCg==$Yu0w7sFjhLnbtZQJ/nyp+A== pbkd

username admin password $sha512$5000$OZ45Ro7002bnyFGXlIghqg==$T9oP1zKSTmv74Nizd8ku3A== pbkd
```

Some modification of the hashes is required before they can be imported into hashcat. Basically the first $ needs to be removed and all subsequent $'s need to be replaced with colons.

For example:

```
$sha512$5000$SvZkzlRDO115YrLXsZuWCg==$Yu0w7sFjhLnbtZQJ/nyp+A==
```

Becomes:

```
sha512:5000:SvZkzlRDO115YrLXsZuWCg==:Yu0w7sFjhLnbtZQJ/nyp+A==
```

This hash can now be fed into hashcat as a single:

```
hashcat64.exe -m 12100 sha512:5000:SvZkzlRDO115YrLXsZuWCg==:Yu0w7sFjhLnbtZQJ/nyp+A== c:\Too
```

```
sha512:5000:SvZkzlRDO115YrLXsZuWCg==:Yu0w7sFjhLnbtZQJ/nyp+A==:cisco

Session..........: hashcat
Status...........: Cracked
Hash.Type........: PBKDF2-HMAC-SHA512
Hash.Target......: sha512:5000:SvZkzlRDO115YrLXsZuWCg==:Yu0w7sFjhLnbtZ...yp+A==
Time.Started.....: Thu Jan 18 14:49:19 2018 (0 secs)
Time.Estimated...: Thu Jan 18 14:49:19 2018 (0 secs)
Guess.Base.......: File (c:\Tools\wordlists\pw_topten.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:        0 H/s (1.61ms)
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 80/80 (100.00%)
Rejected.........: 0/80 (0.00%)
Restore.Point....: 0/80 (0.00%)
Candidates.#1....:  -> hashcat
HWMon.Dev.#1.....: Temp: 41c Util: 85% Core: 928MHz Mem:2505MHz Bus:4
```

Or via a file:

```
hashcat64.exe -m 12100 sha512.txt c:\Tools\wordlists\pw_topten.txt
```

```
sha512:5000:SvZkzlRDO115YrLXsZuWCg==:Yu0w7sFjhLnbtZQJ/nyp+A==:cisco
sha512:5000:vlCP+V07DGEJ9TcSV/GpuA==:2S8SLoECmbtb/o17ZhXuKg== :

Session..........: hashcat
Status...........: Cracked
Hash.Type........: PBKDF2-HMAC-SHA512
Hash.Target......: sha512.txt
Time.Started.....: Thu Jan 18 14:51:03 2018 (1 sec)
Time.Estimated...: Thu Jan 18 14:51:04 2018 (0 secs)
Guess.Base.......: File (c:\Tools\wordlists\pw_topten.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:      207 H/s (1.60ms)
Recovered........: 2/2 (100.00%) Digests, 2/2 (100.00%) Salts
Progress.........: 160/160 (100.00%)
Rejected.........: 0/160 (0.00%)
Restore.Point....: 0/80 (0.00%)
Candidates.#1....:  -> hashcat
HWMon.Dev.#1.....: Temp: 41c Util: 37% Core: 928MHz Mem:2505MHz Bus:4
```

Cracked hashes:

```
sha512:5000:vlCP+V07DGEJ9TcSV/GpuA==:2S8SLoECmbtb/o17ZhXuKg==: (i.e. blank)

sha512:5000:SvZkzlRDO115YrLXsZuWCg==:Yu0w7sFjhLnbtZQJ/nyp+A==:cisco
```

I leave the final hash (below) to be cracked as a challenge for the reader (it can be cracked with any respectable word-list):

```
$sha512$5000$OZ45Ro7002bnyFGXlIghqg==$T9oP1zKSTmv74Nizd8ku3A==
```

Thanks to my colleague Marius for the initial pointer on the hash type.

Leave a Reply

Your email address will not be published.

Your message

Name

Email

Website (optional)

Notify me of follow-up comments by email.

Notify me of new posts by email.

Submit Comment

Search

Follow @attackdebris

RECENT POSTS

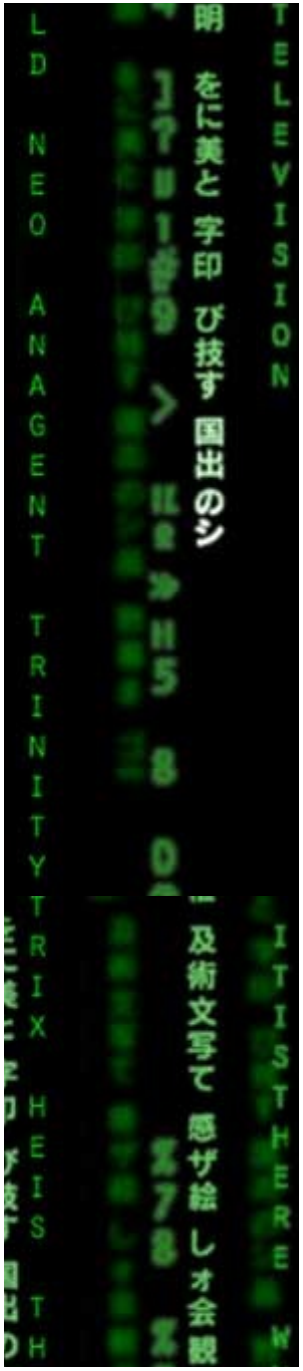
- Troubleshooting Empire and PoshC2_Python HTTPS Connections
- Low Privilege Active Directory Enumeration from a non-Domain Joined Host
- Cracking Cisco ASA SHA-512 Hashes with Hashcat
- Kerberos Username Enumeration – Top 500 Common Usernames
- Auto-sslscan (Automatic SSL Scanning)

USEFUL LINKS

- Hack, Whack and Smack
- Phillips321
- rewt dance
- Scriptmonkey

ARCHIVES

- December 2018
- February 2018
- January 2018
- June 2017



CATEGORIES