SETH

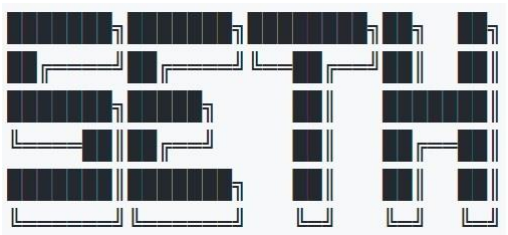
Information Security Inc.

Contents

- About SETH
- SETH Features
- Requirements
- Demo setup 1
- Demo setup 2
- Installing SETH
- Demo and Countermeasures
- References

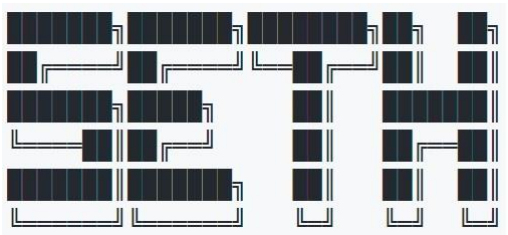
About SETH

- Seth is a tool written in Python and Bash to MitM RDP connections by attempting to downgrade the connection in order to extract clear text credentials



SETH features

- The script performs ARP spoofing to gain a Man-in-the-Middle position and redirects the traffic such that it runs through an RDP proxy



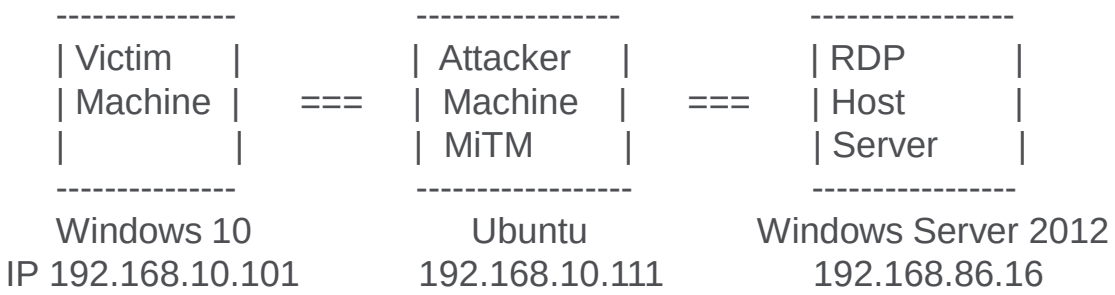
Requirements

- python3
- tcpdump
- dsniff (arpspoof)
- openssl < 1.1.0f

OpenSSL should not be too recent, as it does not support older versions of the SSL protocol and thus may be incompatible with older version of the Windows RDP client

Demo Setup 1

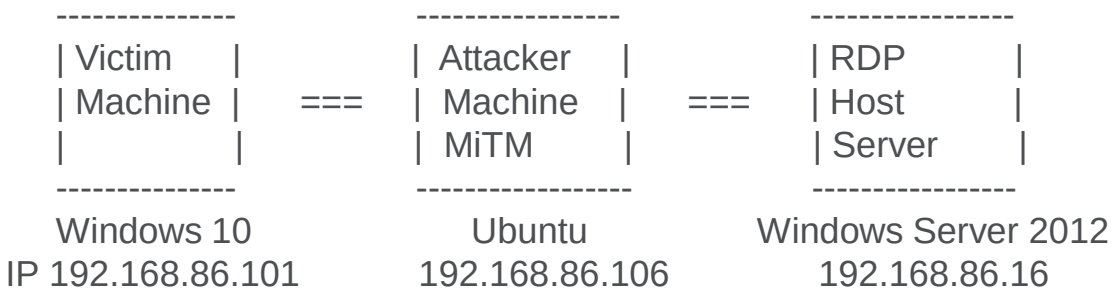
- RDP host ***is not*** on the same subnet as the victim machine



Gateway IP = “192.168.10.105”

Demo Setup 2

- RDP host ***is on*** the same subnet as the victim machine



Installing SETH

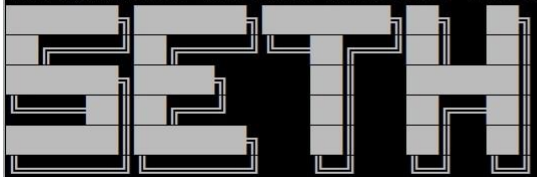
- Installing SETH on the attacker machine

```
root@admin1-virtual-machine:~# git clone https://github.com/SySS-Research/Seth.git
Cloning into 'Seth'...
remote: Counting objects: 244, done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 244 (delta 0), reused 1 (delta 0), pack-reused 241
Receiving objects: 100% (244/244), 1.75 MiB | 848.00 KiB/s, done.
Resolving deltas: 100% (120/120), done.
Checking connectivity... done.
```

Installing SETH

- SETH usage

```
root@admin1-virtual-machine:~/Seth# pwd
/root/Seth
root@admin1-virtual-machine:~/Seth# ./seth.sh -h
```

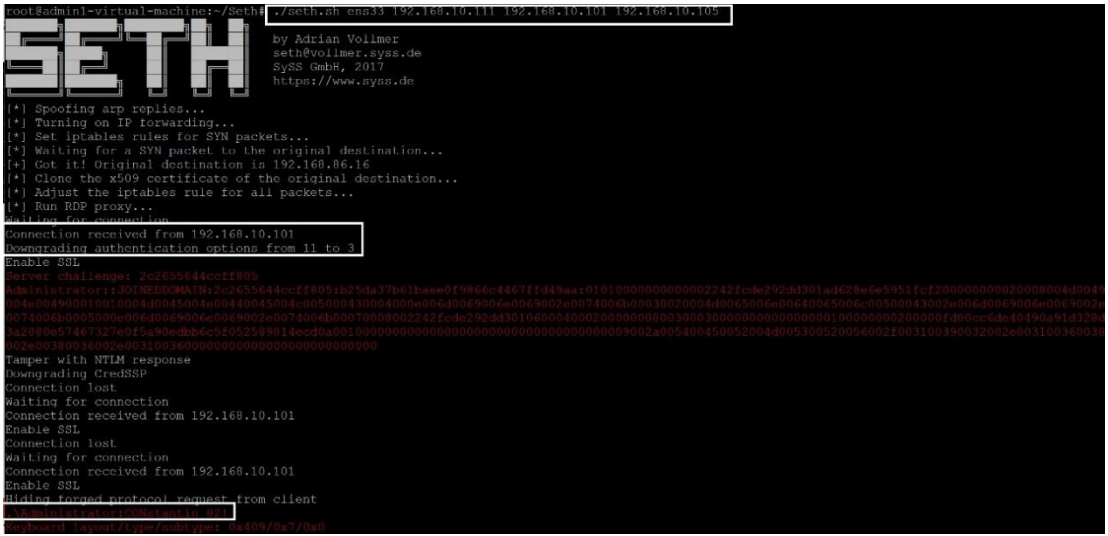


```
by Adrian Vollmer
seth@vollmer.syss.de
SySS GmbH, 2017
https://www.syss.de

Usage:
./seth.sh <INTERFACE> <ATTACKER_IP> <VICTIM_IP> <GATEWAY_IP|HOST_IP>
```

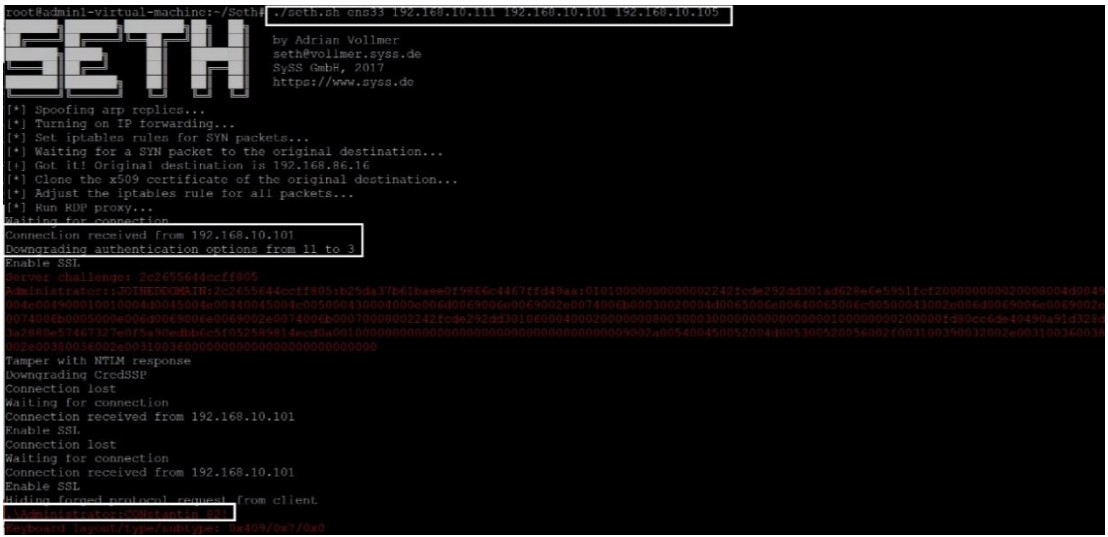
Demo and Countermeasures

- **Demo using Setup 1 : RDP host (server) *is not* on the same subnet as the victim machine**



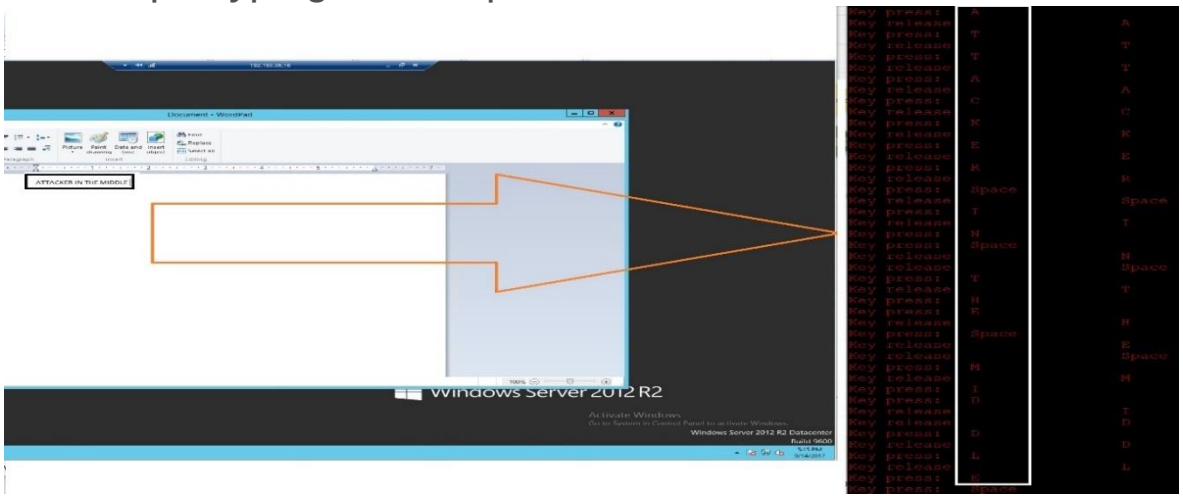
Demo and Countermeasures

- Seth sniffs an offline crackable hash as well as the clear text password



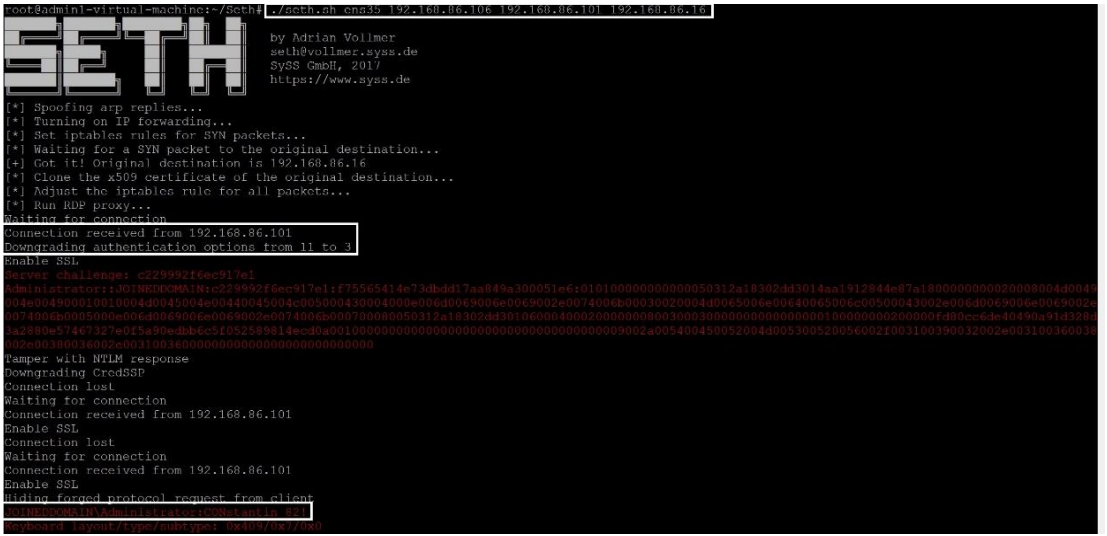
Demo and Countermeasures

- From the attacker machine we can see what the victim is doing inside the RDP session by capturing the keystrokes
- For example typing in Wordpad



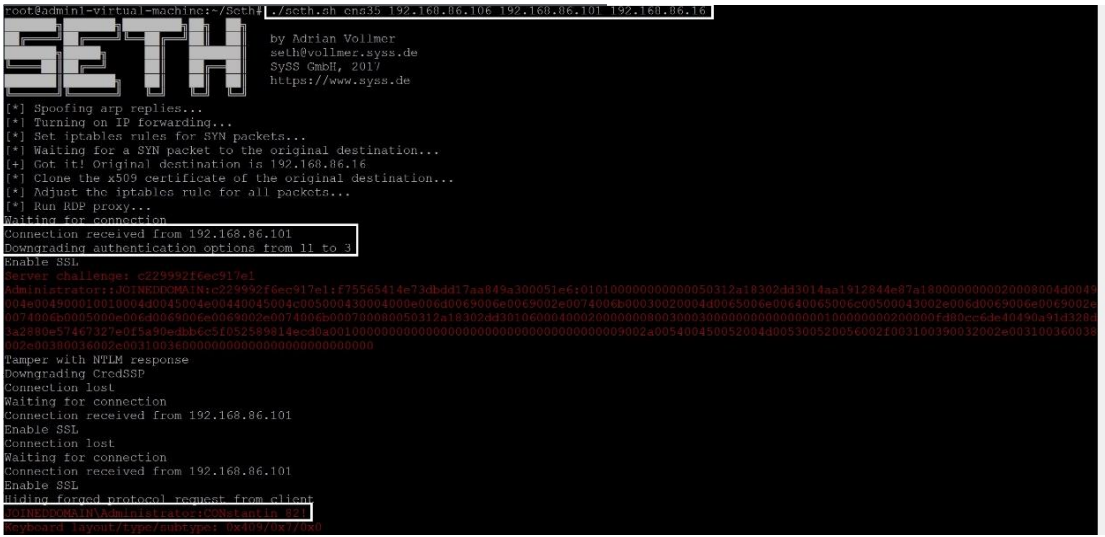
Demo and Countermeasures

- **Demo using Setup 2 : RDP host (server) *is on* the same subnet as the victim machine**



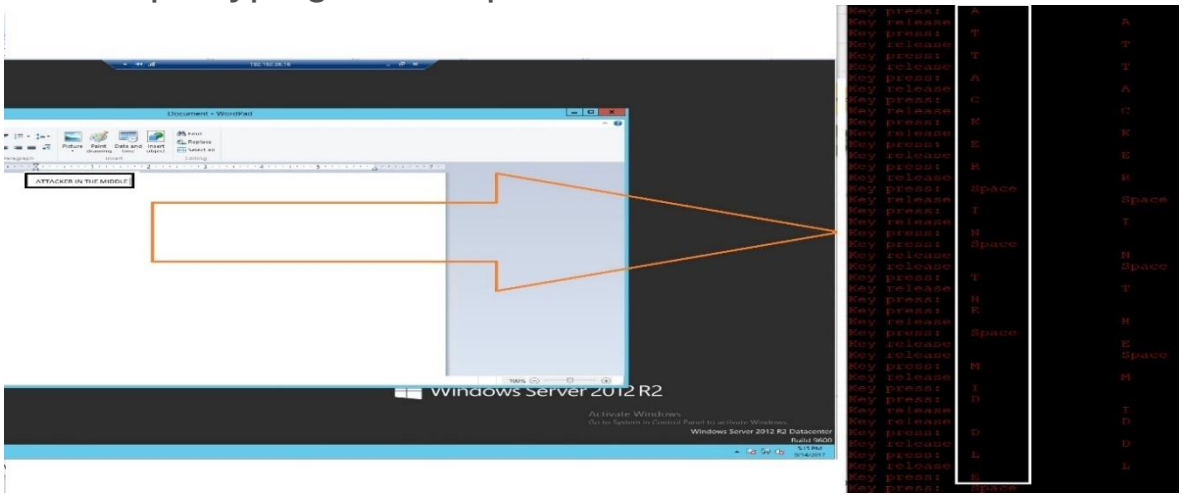
Demo and Countermeasures

- Seth sniffs an offline crackable hash as well as the clear text password



Demo and Countermeasures

- From the attacker machine we can see what the victim is doing inside the RDP session by capturing the keystrokes
- For example typing in Wordpad



Demo and Countermeasures

• ***Countermeasures***

◎ RDP connections cannot happen if the server's identity cannot be verified (if the SSL certificate is not signed by a trusted CA). Sign all servers certificates with the enterprise CA

◎ Use a seconds factor besides user credentials

◎ SSL warnings are not to be taken lightly. Client systems need to have the root CA in their list of trusted CAs

References

- Github

https://github.com/SySS-Research/Seth

- ARP spoofing

https://en.wikipedia.org/wiki/ARP_spoofing