CTF Cheatsheet
Yelling at PCs since 2006

About this event: EnoIntro 2019

Time	12:00 - 20:00 **(UTC)**
Flag format	`ENO/^\w{31}=$/`

Network

IP	Host	Network Type
Team<int>.enoctf.enoflag.de	Vulnboxes	Game
———	———	———
172.16.1.1	Moloch Server	Internal
10.10.10.10:1337	Flaggenabgabe	Internal

Directories

Directories we use to share data from/about the services and sniffer data. They reside on Team<int>.enoctf.enoflag.de

Directory	Description
/services/	service data (in subdirs) and moloch
/pcaps/	sniffer data as pcap files

Connectivity, SSH & Co

Authentication

- Best use public/private key pairs to authenticate
  → **private keys** should never leave your machine
- Windows users can use Putty (but mind the SSH key config options)

```
# ssh -p <port> <ip> to specify port if not standard
ssh -p 22 root@<VulnboxIP>
```

SSH config

It is advisable to create and maintain a SSH config (`/.ssh/config`) where you define configurations for commonly accessed hosts.

```
# SSH config @ ~/.ssh/config
Host vulnbox
  User root
# Port <vulnbox-ssh-port>
  Hostname <vulnboxip>
  IdentityFile ~/.ssh/<my-private-key>
#Usage with this config: 'ssh vulnbox'
```

SSHFS

- Used to mount directories located on a remote host in your own file system (may need to be installed first: `sudo apt install sshfs`)
- Commonly used by us to access access network traces from our sniffer and share files / service backups from the vulnbox.
  To mount the remote /sniffer dir at <ip> in your local file system:

```
mkdir -p ~/enointro/pcaps ~/enointro/sshfs
# '\' indicates linebreak, command is a one liner
sshfs -o allow_other root@<vulnboxip>:/pcaps/  \
  ~/enointro/pcaps
sshfs -o allow_other root@<vulnboxip>:/services/  \
  ~/enoflag/sshfs
```

```
# To delete local dir, first unmount with
# fusermount -u ~/enointro/
```

- On Windows, it's possible to use WinSCP to browse a remote directory and up/download files.

Surviving on the vulnbox

Try to get familiar with some *nix commands to navigate the vulnbox. **Be aware** of the consequences of the commands you run, especially deletions and such. especially since your user on the vulnbox may be `root`.
Some useful examples (that should be extended):

```
# Find every file named cat.* in /searchdir
find /path/to/searchdir -iname cat.*
# search for 'foo' directory from /etc on
find /etc -type d -iname foo # see also: -type f|s|..
# Check enabled service files
systemctl list-unit-files | grep enabled
# List running processes
ps aux
# Show list of listening network services
netstat -tulpen # ss -tulpen, if no netstat available
# Search history of executed commands for 'foo'
history | grep -i foo
# Copy contents of file 'foo' to clipboard
xclip -sel c < foo
# Show all aliases in current shell
alias
```

Misc tips:

- Use `<CTRL>+r` to start a bash reverse search and type some part of a command to find last used instances and use `<CTRL>+r` again to scroll trough them.
- Search in man pages by typing `/` and then entering your search term (regexes also work). Press `<Enter>` to start searching, type `n` to search forward and `N` to search backwards.

Patching and restarting services

Make sure you know what to do to make sure your changes/patches are actually taking effect. Some services will need to be rebuilt, while others consist of interpreted scripts. Even if you just have to change a python script, make sure it is the one that is used by the running service (check what is actually executed).

Systemd

Systemd services may be used to start a service directly, or act as a trigger to start docker builds and/or running of containers.

```
systemctl status nginx # can also show useful files
# Restart the systemd service ngnix
systemctl restart nginx # also: stop|start|etc
# Tail the systemd log of the nginx unit from now on
journalctl -u nginx.service -f
```