Linux ECONET exploit to work on FreeBSD? Don't jump at trolls!

Few days ago, the Linux ECONET exploit was uncovered.

Not long afterwards a customer contacted us at work to know, if he was vulnerable or not.

His arguments: Someone posted to the mailing list that FreeBSD would be exploitable as well - not to mention that the customer indeed uses FreeBSD.

I instantly replied, that FreeBSD would _not_ be vulnerable, otherwise a security advisory would have been posted on their site.

Grieving in unbelief? Well, despite of being very unlikely, that a Linux-specific exploit would run without modification on FreeBSD, would it not be required to also have the ECONET symbols available in the sources and additionally also a network driver for it?

Let's check on the full source tree:

```
[root@sandbox ~]# grep -rile econet /usr/src/*
/usr/src/contrib/ipfilter/bpf-ipf.h
/usr/src/contrib/ipfilter/pcap-bpf.h
/usr/src/contrib/ipfilter/lib/ipft_pc.c
/usr/src/contrib/libpcap/savefile.c
/usr/src/contrib/libpcap/pcap/bpf.h
/usr/src/contrib/openbsm/libbsm/bsm_domain.c
/usr/src/contrib/openbsm/sys/bsm/audit_domain.h
/usr/src/sys/bsm/audit_domain.h
/usr/src/sys/net/bpf.h
/usr/src/sys/security/audit/audit_bsm_domain.c
```

This much ends up in the system's include directory:

```
[root@Vigor65 ~]# grep -rile econet /usr/include/
/usr/include/bsm/audit_domain.h
/usr/include/net/bpf.h
/usr/include/pcap/bpf.h
```

However nothing of this all seems directly related to an ECONET driver, but instead to the Berkeley Packet Filter.

So to speak, trying to compile the exploit raises expected errors about undeclared symbols.

```
exploit.c: In function 'main':
exploit.c:217: error: 'PF_ECONET' undeclared (first use in this function)
exploit.c:217: error: (Each undeclared identifier is reported only once
exploit.c:217: error: for each function it appears in.)
exploit.c:250: error: 'MAP_ANONYMOUS' undeclared (first use in this function)
```

exploit.c:261: error: 'CLONE_VM' undeclared (first use in this function)
exploit.c:261: error: 'CLONE_CHILD_CLEARTID' undeclared (first use in this function)

To summarize this: The exploit does not apply to FreeBSD - not even after loading linux.ko and installing linux_base-f10 or a similar linux compatibility port.

As for the reporter, I feel this is indeed a fake because auf several reasons.

His posting reflects a FreeBSD host as from the 'uname' output being exploitable. But looking at his post and the previous post, the memory addresses are absolutely identical. It is very unlikely that memory addresses for two different operating systems ever be identical, that much is sure. This all looks indeeded copy-pasted and rewritten.

- The guy posted further comments to the topic which makes me feel that he's just a troll trying to bash around

Not to mention the domain name, which exists, but was registered using absolute fake data as seen on the screenshot. This indeed looks trollish to mee. If he was serious about this, he would stand with his name. Period.

So, this is a perfect example of how people jump at trolls. As if we all didn't have better things to do ....