Security Engineering Masterclass
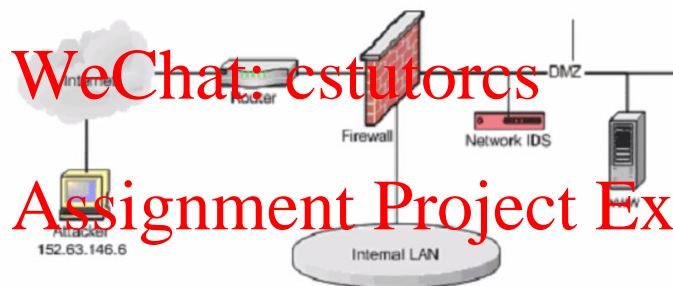
SIEM:

In SIEM systems, we _____ logs, so knowing how to read and interpret information from logs _____ the below image, it shows that possible logs can come from all sorts of places _____ firewall etc.

SCENA

Note: we will assume the devices have been configured with full logging capabilities such that maximum visibility is attained. For example, the firewall is configured to log both accepted and denied attempts.

© AARNet Pty Ltd | 4

Consider this log from the router, what is it saying?

INDEPENDENT ANALYSIS

- What can we observe with the below Router Logs (Cisco):

```
May 31 09:27:44 router.company.com 1410875: May 31 09:27:43: %SEC-6-IPACCESSLOGP: list from-internet denied tcp
152.63.146.6(1459) -> xxx.yyy.zzz.1(80), 1 packet

May 31 09:27:50 router.company.com 1410880: May 31 09:27:50: %SEC-6-IPACCESSLOGP: list from-internet denied tcp
152.63.146.6(1673) -> xxx.yyy.zzz.2(80), 1 packet

May 31 09:27:54 router.company.com 1410883: May 31 09:27:53: %SEC-6-IPACCESSLOGP: list from-internet denied tcp
152.63.146.6(1750) -> xxx.yyy.zzz.3 (80), 1 packet

May 31 09:27:57 router.company.com 1410885: May 31 09:27:56: %SEC-6-IPACCESSLOGP: list from-internet denied tcp
152.63.146.6(1722) -> xxx.yyy.zzz.5(80), 1 packet

May 31 09:27:58 router.company.com 1410886: May 31 09:27:57: %SEC-6-IPACCESSLOGP: list from-internet denied tcp
152.63.146.6(1930) -> xxx.yyy.zzz.6(80), 1 packet

May 31 09:28:01 router.company.com 1410888: May 31 09:28:00: %SEC-6-IPACCESSLOGP: list from-internet denied tcp
152.63.146.6(1976) -> xxx.yyy.zzz.7(80), 1 packet

May 31 09:28:05 router.company.com 1410891: May 31 09:28:04: %SEC-6-IPACCESSLOGP: list from-internet denied tcp
152.63.146.6(2167) -> xxx.yyy.zzz.8(80), 1 packet

<data pruned>
```

- Router access control lists have been configured to allow inbound TCP port 80 traffic with ephemeral source ports to xxx.yyy.zzz.4 because this is our company web server.
- Can we answer the Five 'W's (Who, What, When, Where, Why)

- Who: 152.63.146.6. But no user attached to IP.
- What: Broad scanning of xxx.yyy.zzz.0/24
- When: May 31 <time>
- Where: DMZ company
- Why: brute forcing ip addr

- What can we observe with the below Firewall Logs (Gauntlet):

```
Jun 1 06:08:50 firewall.company.com [29142]: log host=nodnsquery/152.63.146.6 protocol=http cmd=get
dest=xxx.yyy.zzzz.4 path=/cgi-bin/phf ID=29142174970

Jun 1 06:08:54 firewall.company.com http-gw[29142]: log host=nodnsquery/152.63.146.6 protocol=http cmd=get
dest=xxx.yyy.zzzz.4 path=/cgi-bin/form...

Jun 1 06:08:58 firewall.company.com [...]        ...63.146.6 protocol=http cmd=get
dest=xxx.yyy.zzzz.4 path=/cgi-bin/surve...
```

- What number of the 5 Es identified?
- Can we answer the Five 'W's (Who, What, When, Where, Why)

- Who: 152.63.14...
- What: Attempt ... scripts.
- Where: DMZ company trying to gain access still.
- Why: Research shows that phf, formmail and survey.cgi are all exploitable scripts. Attempts malicious activity because if accessed, these scripts would allow remote execution. The access in isolation is a poor move on the red team because it flags it as malicious activity.

What can we observe with the below IDS Logs (Snort):

```
[**] [1:886:3] WEB-CGI phf access [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/01-06:08:50.764332 152.63.146.6:3308 -> xxx.yyy.zzzz.4:80
TCP TTL:52 TOS:0x0 ID:61884 IpLen:20 DgmLen:280 DF
**AP*** Seq: 0x591AF831 Ack: 0x92D23FAF Win: 0x16[..] TcpLen: 32
TCP Options (3) => NOP NOP TS: 59902357 300726
[Xref => http://www.securityfocus.com/bid/629]
[Xref => http://www.whitehats.com/info/IDS128]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0067]

[**] [1:884:2] WEB-CGI formmail access [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/01-06:08:54.411065 152.63.146.6:3309 -> xxx.yyy.[...]
TCP TTL:52 TOS:0x0 ID:15383 IpLen:20 DgmLen:285 D[.]
**AP*** Seq: 0x85C51FD8 Ack: 0xC004B803 Win: 0x16[..] TcpLen:
TCP Options (3) => NOP NOP TS: 59974615 372988
[Xref => http://www.securityfocus.com/bid/1187]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0172]
[Xref => http://www.whitehats.com/info/IDS226]

[**] [1:871:2] WEB-CGI survey.cgi access [**]
[Classification: Attempted Information Leak] [Priority:
06/01-06:08:58.609416 152.63.146.6:3310 -> xxx.yyy.zzzz.4[.]
TCP TTL:52 TOS:0x0 ID:32890 IpLen:20 DgmLen:295 DF
**AP*** Seq: 0x8B55C63C Ack: 0xC624745D Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 59983434 381809
[Xref => http://www.securityfocus.com/bid/1817]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0936]
```

- What alerts do we see? What are these alerts known for?
- Below are the Snort rules that triggered these alerts.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI phf access";flags: A+; uricontent:"/phf"; nocase;
reference:bugtraq,629; reference:arachnids,128; reference:cve,CVE-1999-0067; classtype:attempted-recon; sid:886;

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI formmail access";flags: A+; uricontent:"/formmail";
nocase; reference:bugtraq,1187; reference:cve,CVE-1999-0172; reference:arachnids,226; classtype:attempted-recon;
sid:884; rev:2;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI survey.cgi access";flags: A+; uricontent:"/survey.cgi";
nocase; reference:bugtraq,1817; reference:cve,CVE-1999-0936; classtype:attempted-recon; sid:871; rev:2;)
```

- Can we answer the Five 'W's (Who, What, When, Where, Why)

- Who: 152.63.146.6
- What: Attempt to leak info about the vulnerable scripts.
- Where: DMZ company trying to gain access still.
- Why: Attempting to leak information from the scripts to exploit them.

Note: Parsing the logs (which are in different format) is required in order to stitch together this information.

Limitations of single device analysis:
- False positives,
- Incomplete info
- Missing the 'why'
- Miss lateral movement or other activities (e.g. exfiltration)

Summary:
- Analysing single devices is the computerised version of tunnel vision.
- Security events should be analysed from as many sources as possible.

- Security Awareness of an environment can be attained by listening to what its devices are saying.

程序代写代做 CS编程辅导

WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

https://tutorcs.com