UNIVERSITY OF ALASKA FAIRBANKS

Linux Logs

Arsh Chauhan

11/4/17

Logging?

Logging is basically keeping track of all transactions that take place.

Important?

Logs are important for security since they keep a history of everything that has happened.

Important?

Logs are important for security since they keep a history of everything that has happened.

This is important when responding to or confirming a breach

Can logs be trusted?

Logs exist on the compromised machine. So the first question is:

Can logs be trusted?

Logs exist on the compromised machine. So the first question is: Can they be trusted?

Can logs be trusted?

Logs exist on the compromised machine. So the first question is: Can they be trusted?

It depends...

Can logs be trusted?

Logs exist on the compromised machine. So the first question is: Can they be trusted?

It depends...on the access the attacker achieved.

Can logs be trusted?

Logs exist on the compromised machine. So the first question is: Can they be trusted?

It depends...on the access the attacker achieved.Lets get more meta and ask...

Can logs be trusted?

Logs exist on the compromised machine. So the first question is: Can they be trusted?

It depends...on the access the attacker achieved.Let’s get more meta and ask...If the machine itself can be trusted?

Can logs be trusted?

Logs exist on the compromised machine. So the first question is: Can they be trusted?

It depends...on the access the attacker achieved.Let’s get more meta and ask...If the machine itself can be trusted?

LAB

Find FSociety

You're a security analyst at E-Corp. Tyrell Wellick suspects there has been an intrusion and has tasked you with figuring out if F-Society has managed to get into your web- server. From experience you know this webserver is running SSH, Nginx and UFW. Your task is to figure out if an intrusion has occurred or not. Write a short report for Tyrell giving him:

1) Did an attack happen
2) Initial attack vector (how the attacker got in)
3) The attacker's IP
4) What access did the attacker gain
5) Was data exfiltrated
6) How can this attack be prevented in the future