


Peer-graded Assignment: Foundation Course Project

Sukhvir Singh

Analyze: Identify one specific service / port / protocol that repeatedly displays as being attacked

Attacks reported as on December 14, 2020 Time 7:32 PM INDIA is approximately 23737 per minute & 1400638 attacks in 1 hour. The Source Target is PIR, Attack Type is Network (Dionaea) & Attack on Port 445/tcp is there.

LIVE TICKER					TOP ATTACKER 2020-12
DOMAIN	DATE	SOURCE	TARGET	ATTACK TYPE	
DTAG	19:38:04	CZ	PIR	Network (Dionaea)	
DTAG	19:38:03	SA	PIR	Network (Dionaea)	
DTAG	19:38:02	VN	PIR	Network (Dionaea)	
COM	19:38:01	US	US	RDP (rdpy)	
DTAG	19:38:00	SA	PIR	Network (Dionaea)	

This Target PIR is continuously being attacked. It's represented by T-SEC Radar System which represents Cyber Attacks worldwide

Research: Describe a real world scenario where that particular service would be required

We all know about SWIFT Code. It's an international bank code that identifies particular banks worldwide. It's a secure messaging service that enables financial transactions between 11,000 financial institutions in over 200 countries,

and handles 32 million messages goes up to some trillion dollars, every day. Trust & integrity is the main part of SWIFT's Business Model. But in 2015 over \$ 1 billion theft was there from a bank named Bangladesh Central Bank (BCB).

The bad actors used the SWIFT network to fool the US Federal Reserve into transferring those BCB funds. (It's not uncommon for the US Fed to hold international banking assets.) As a basic security check, SWIFT sends details of any transfer to the printers of the financial institution behind the request.

Under normal circumstances, with that added layer of review in place, when a BCB official sees a request of that size he or she would stay the transfer until confirmation can be had. (Especially if – as was the case here – the funds are being sent to an unknown account) In order to get the attack out of the gate successfully, therefore, the attackers cleverly used malware to disable the bank's printers.

In the end, the full attack was thwarted, but \$81 million still went missing!

Solve: Explain in your own terms a process (Solution) that would be used to setup a secured trust relationship between the server which delivers that service and a legitimate client requester.

1. Set up strong passwords
2. Enable your server to use SSH Keys which is a pair of public and private keys to login into your server
3. You can Disable SSH Password Login in the openssh config files in your operating system to completely stop such attacks.

References:

1. <https://www.cybermdx.com/blog/5-scary-real-life-cyber-attacks-you-never-heard-about>