Cyber Security In High-Performance Computing Environment

Prakashan Korambath
Institute for Digital Research and Education, UCLA
July 17, 2014

Introduction:

Cyber attack is an unauthorized access to a computer information system or infrastructure with a malicious intent to steal sensitive document, compromise network, vandalize the resources or use the resources for further malicious actions by individuals or organizations or nations. For this discussion, we define a high-performance compute (HPC) environment as a compute resource running Linux operating system (OS) with around at least 500 to 1000 compute nodes having approximately 4000 to 12000 compute cores. They all invariably have high speed, low latency, high bandwidth interconnect network fabric such as Infiniband. They also have attached storage arrays of the order of hundreds of terabytes to petabytes. These kinds of resources are used simultaneously by an average of 200 to 300 users mostly from academic research environments in universities at any time although they may have over 1000 overall users. The complexity of securing the system increases with number of users, as there will be more cases of lost or compromised passwords. Usually in HPC clusters only few login nodes are open to the public network as the compute nodes are in a private network. Security breach involving computer viruses such as Trojan viruses or computer worms usually associated with Windows OS will not be discussed here. We will only discuss proactive mitigating steps to minimize interruptions in the operation of the resource.

The expectation in HPC environment is that the research done are mostly open and the resources should be easily accessible and the policy should accommodate the need of researchers who are collaborating around the globe. There is a need for balance between security and convenience. Because of the convenience factor intrusion prevention is little bit harder on HPC systems and they are more vulnerable. However, there are a lot of positive benefits in operating an HPC environment in universities compared to the compute environments in financial institutions. Expectation is that typical researchers are not storing any personnel information such as social security number or private medical data on these systems. The biggest worry is that hackers may vandalize the system when they couldn't find any useful data or use this resource to stage criminal activities such as executing a distributed denial of service (DDoS). If the users are involved in any research with private medical data then they are required to do their research on HIPAA complaint compute environment. We will not address how to set up a HIPAA complaint system in this write up as it brings additional complexity of encrypting all the research data. HPC sites typically do not have to worry about attacks such as denial of service as these kinds of attacks are usually against high volume web portals such as news organizations or government web sites.

Protecting passwords and disabling unencrypted network protocols:

In the 1990s research compute environment used protocols such as telnet, ftp where the data between remote computers are communicated in clear text format. So, it was easy for anybody with reasonable expertise to intercept the communication and read the contents. It was easy to listen to an open port and record the keystrokes of users. None of the HPC sites that we know are running these kinds of protocols anymore. The traffic among HPC systems connected through public or private network now is exclusively through encrypted protocols using OpenSSL such as ssh, sftp, https etc. Since almost all HPC resources are running some version of Linux operating system they all invariably run Iptables based firewall at the host level, which is the primary tool to restrict access to service ports from outside network. Many of them open only few ports such as port 22 for ssh. Iptables also help in operating the system when there are known zero-day-vulnerabilities by isolating the resources from outside network.

Typical way the HPC systems compromised is through either users not protecting their password or using passwords that are easy to exploit such as 'test123'. By virtue of the design of the Linux OS, the exploit at the user level is often contained local to a particular user because regular users do not have elevated privileges and they do not have access to files of other users or users from a different group. Even though the security breach through compromised password is usually contained in a user environment, they become escalated in a situation where there is a flow in the Linux kernel itself, which will allow the hacker to trigger local root exploitation and elevate the privileges. In such situation the OS needs to be reinstalled with updated kernels. Linux kernels in the 2000s had frequent kernel flows and were susceptible to memory corruption (buffer overflow), which are becoming very rare these days. Another kind of problem is if the security package itself has flows such as Heartbleed bug (heartbleed.com) in OpenSSL, which was detected in 2014 even though the bug existed for many years prior to that.

In a scenario where users are hacked, often times owners of the accounts are unaware of the fact that they have been compromised. From our experience of running an HPC cluster for the past 12 years it is often the activity of the hackers that expose or alert the system administrators of the system about possible compromise meaning if somebody just login to the system and do nothing their actions are often overlooked. But as soon as the imposter or hacker start using the resources the monitoring tools that are often embedded in Linux OS can record the strange behavior of the system and an alert system administrator can execute remedial actions. Almost always the behaviors of hackers are completely different from that of the owner of the account. Activities such as sudden burst of network activity, increased network latency, over loading the system with CPU usage, unauthorized jobs bypassing the job scheduler etc. are good indicators of possible compromise. Typically the hackers are exposed in 8 to 10 hours in such scenarios. Often times the affected systems are quarantined from outside network for forensic activities and all the logs are examined to trace the origin of attack such as time, frequency of attack, source host, source port, destination host, destination port and the protocol or application that is used in attacking the system. System will be put back to service after remedial actions are taken such as notifying the appropriate authorities if necessary, upgrading or removing the faulty application or kernel as well as any other upgrades.

Some of the HPC centers do not rely on users in protecting their password. So they implemented what is called One Time Password (OTP) where users are given a small calculator like devices to generate a random key to login to the system. However, that is inconvenient for users, as they have to carry this device all the time with them and also add to the operating cost of HPC systems. Those centers that do not use OTP often limit the failed access attempts to three or four times and restrict access to the account for a period of one or two hours to minimize the brute force attempt to crack user password on the system. Other safeguards HPC centers deploy include running only the necessary applications with administrative privileges that open TCP/IP ports to external network. Even if there is a need to open up Apache port or Database port the connection to these ports are restricted to certain user groups or hosts using Iptables.

The HPC environment also has few privileged account for system administrators and user support staff. These accounts have access to all the resources on the system in the sense that these users can read, write, or delete the contents in any of the accounts. So the account holders of these account needs to take extra caution on all the devices and network they operate. They should access their privileged account from remote machines or untrusted network only after activating a virtual private network (VPN).

Other forms of attacks are little bit more sophisticated in the sense that hackers do a man-in-the-middle attack by making it appear the hacker controlled system to have similar credentials to the system that users are trying to access in that process tricking the users to give away their credentials. In other word hackers are trying to hijack the endpoints. Experienced hackers also try to cover their trails and continue their exploit by installing rootkits, modifying the RPM package repository, turning off or maneuvering the monitoring software and log files. The sophisticated hackers are usually capable of obfuscating their activities and disabling monitoring tools. In such situations system administrators have to rely on secondary effects such as unusual network bandwidth or unusual CPU load to detect the intrusion. It is possible that a sophisticated attack can remain undetected for months.

Phishing is another common way hackers get user credentials by enticing users to visit hacker controlled machines. Users who use popular social networking web sites are usually susceptible for this kind of attack and if they happen to use same password for their HPC accounts then they are inviting the hackers over from social networking sites to HPC systems. Social networking sites are usually good targets for hackers because they get access to the users contacts and access to their friends and continue their exploit. Intercepted e-mails are another source of compromise.

Safeguarding the resource

1. Always run Iptables (firewalls) on the machines with public network connections.
2. Check the operating system logs periodically or have it checked by an application and report any anomalies in user behavior such as logins, source host, network bandwidth, resource usage, time and frequency of login etc.

3. Enforce choice of passwords that contain certain number of characters and combination of alphanumeric characters as well as special characters.
4. Force password change once a year even though most users don't like to change passwords often.
5. Inactivate expired accounts, unused accounts and accounts of employees when they leave the organization.
6. Turn on Host based authentication if possible. This is almost impossible for HPC systems as the users can be on any host at any time.
7. Advise users not to store private keys such as ssh private keys for passwordless logins on HPC resources because hackers who obtained elevated privilege can use it to access other machines.
8. Allow only authorized machines with known MAC addresses in a network that issue DHCP IP addresses. This is also little bit impossible in today's world where people use all kinds of mobile devices such as smart phones to access the resources.
9. Use software that use PKI encryption by relying on public and private keys such as grid-ftp.
10. Allow only encrypted protocols such as ssh, sftp or https to access the system.
11. Activate tools such as SELinux that will control the access through predefined roles, but most HPC centers do not activate it as it breaks down the normal operation of the Linux clusters and it becomes harder to debug when applications don't work as expected.
12. When running a web-based application, add campus Shibboleth based authentication. This will serve at least as a spam filter and can curtail denial of service like attacks.
13. Enforce resource quota such as total storage capacity or compute time when applicable.
14. Issue one time password generating devices if possible.
15. Do not allow any HIPAA complaint research on HPC clusters with lots of users. Isolate any HIPAA type research within restricted networks.
16. Allow research with sensitive data only within restricted networks.
17. Prevent any mobile devices from going back and forth between open networks and restricted networks.
18. Compartmentalize networks so that it is easy to quarantine the compromised part of the network. This is also helpful in zero-day-vulnerability because the developers are still working on possible patches to fix those vulnerabilities.
19. It is not usually necessary to upgrade the OS to the latest because it takes a while for the community to test for various flaws. Upgrade the OS only if necessary.
20. Appoint well-trained staff with operating system and Internet knowledge with awareness of threat conditions and cyber forensic skills.

Cloud and Virtual Environment:

Since cloud and virtualization technology became popular in an age when there is a universal awareness of cyber security, the developers of this technology have been under heavy scrutiny to make the technology harder to compromise. In the private cloud environment the resource owners usually have elevated privileges such as root password

and the ability to open or close port to public network. The host providers usually don't have much control on the activities of the virtual host and virtual network, but they do have control on the hosted machines and hosted network. The cloud administrators have sufficient privileges even to examine the virtual instances running on a host machine. In a cloud environment through virtual networking and virtual instances different users are in their own isolated network and compromise on one virtual instance is isolated to only the resources owned by that group. In a way security is little bit better in cloud environment than a HPC cluster where all the nodes have identical set up. It is also easy to discard a compromised image in a cloud environment and build and deploy a new one. Also, it is not necessary to provide public Internet connection to all virtual instances in a private cloud-computing environment.

The security in public cloud environment is less well defined compared to a private cloud environment depending on the service level agreement (SLA). The data is already moved to a public resource where employees of the service provider may have access to the data and if the data is unencrypted, there is a possibility of data getting intercepted during the transfer process. Also, access to data is not guaranteed all the time.

Firewalls at the campus border

A commonly used practice in university environment is network filtering (firewalls) at the campus border as the first line of defense starts there. The campus network administers are continuously monitoring high volume and high frequency traffic for abuse and periodically block the network traffic from those IP addresses until the authenticity of the network behavior is investigated (blacklisting/whitelisting). Network administrators can also block traffic specific to a certain communication protocol and ports if there are known vulnerabilities until mitigation steps have been taken.

Another commonly adopted approach is to block all inbound traffic to a group of compute resources or devices as a matter of policy and punch holes in the filter only to the resources, which needs both inbound and outbound traffic. Where possible private subnets are connected to Internet using network address translation (NAT) methodology, which involves rewriting the source and destination IP addresses when the packet traverses a firewall. This process is called IP masquerade used to hide an entire private subnet from Internet. In this way private subnet can access public network and not vice versa.

Implementing intrusion detection systems (IDS) also results in many false positive alerts because application developers do not follow any strict guidelines and anomalous behavior in one organization may be within the acceptable limits of another organization. Because of this reason many HPC centers do not rely on IDS.