注意事项

在本题目中勒索软件样本为真实样本，请选手一定在虚拟环境中分析，不要在物理机中有任何分析操作，如若造成物理机及数据被加密或损坏，造成损失由选手个人承担，主办方不承担任何责任。
在本题目中勒索软件样本为真实样本，请选手一定在虚拟环境中分析，不要在物理机中有任何分析操作，如若造成物理机及数据被加密或损坏，造成损失由选手个人承担，主办方不承担任何责任。
在本题目中勒索软件样本为真实样本，请选手一定在虚拟环境中分析，不要在物理机中有任何分析操作，如若造成物理机及数据被加密或损坏，造成损失由选手个人承担，主办方不承担任何责任。

节点接入信息

节点【加固修复】接入信息
ssh服务于22端口，账号user，密码123456

节点【应急响应】接入信息
ssh服务于22端口，账号root，密码FD7!#fd8s
web服务于80端口，账号admin，密码JD67s@!#l

节点【威胁分析】接入信息
ssh服务于22端口，账号root，密码toor

节点【溯源反制】接入信息
无接入信息，需要通过其他手段实现权限控制

加固修复-01

加强SSH服务的安全性
为了防止SSH服务被暴力破解攻击，应禁用密码登录并改用密钥认证。
请在Linux服务器上为root用户配置以下公钥以进行验证ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIEhw/9RBAh4qW36/LZXn80sLIZhq2hAJ7qY9KhzfJ3rW

加固修复-02

配置Nginx重定向和HSTS
配置Linux服务器的Nginx服务，将所有站点的HTTP请求重定向到HTTPS，并配置严格传输安全策略（HSTS），以确保客户端与服务器之间的通信安全。

加固修复-03

启用Web应用防火墙
为Nginx服务的默认站点启用ModSecurity Web应用防火墙，并集成OWASP核心规则集（CRS），以防御常见的Web攻击和漏洞利用。

加固修复-04

加强防火墙策略
配置Linux服务器的防火墙，使其仅允许通过以下端口的访问：22/tcp（SSH）、53/tcp和53/udp（DNS）、80/tcp（HTTP）、443/tcp（HTTPS）。
关闭其他不必要的端口，减少攻击面。

加固修复-05

优化Kubernetes RBAC权限
配置App1应用的Kubernetes RBAC权限，只允许读取App1应用命名空间下所有Pods的信息，防止越权访问其他命名空间的资源。

加固修复-06

修复Kubernetes服务
使Pods状态为running，确保应用的可用性。

加固修复-07

修复App2应用漏洞
修复App2应用的已知漏洞，并重新部署App2应用，确保其安全性和稳定性。

应急响应-01

查明并处理植入的后门
公司Web业务系统遭受黑客攻击，并被植入后门。请您立即进行排查和处理，确保系统的安全性和完整性。

应急响应-02

定位持久化服务和木马文件
找到Linux服务器中驻留的持久化服务，并将持久化技术所依赖的二进制木马文件复制到/home/user/checker目录中。

应急响应-03

卸载恶意模块
找到Linux服务器被加载的恶意模块并卸载，恢复系统的正常功能。

应急响应-04

发现并提取隐藏的进程
找到Linux服务器中隐藏的进程，并将该进程的二进制文件复制到/home/user/checker目录中，为后续分析提供依据。

应急响应-05

查找被删除的勒案软件名称
找到攻击者被记录的删除加密勒索软件的痕迹，尝试恢复分析该勒索软件并提交勒索软件十六进制格式的加密密钥到/home/user/checker/key.txt文件中，以便于解密攻击者勒索的文件。

应急响应-06

恢复被加密的数据
恢复服务器上被勒索软件加密的分区数据到/home/user/checker目录，确保业务数据的完整性和可用性。

应急响应-07

查明并处理篡改的首页
公司web业务系统首页遭受黑客攻击，并被植入恶意链接。请您立即进行排查和处理受影响的首页，确保系统的可用性、安全性和完整性。

应急响应-08

查明并处理植入的后门
公司web业务系统遭受黑客攻击，并被植入后门。请您立即进行排查和处理，确保系统的安全性和完整性。

应急响应-09

查明被利用的漏洞
公司web业务系统遭受黑客攻击，黑客利用漏洞进行攻击并被植入后门。请您立即进行排查黑客利用的漏洞点，确保系统的安全性和完整性。

应急响应-10

查明泄露的文件
公司web业务系统遭受黑客攻击，有敏感信息丢失。请您立即进行排查，确保系统的机密性。

威胁分析-01

在调查网络性能或安全问题时，了解特定应用程序在一段时间内的数据传输情况对于检测异常流量和潜在威胁至关重要。通过分析网络活动日志，我们可以确定是否存在数据泄露或异常通信。
请问，firefox进程自有记录以来一共发送了多少字节的数据？（请将答案编辑并存入/opt/wxfx/answer/1.txt文件中，参考/opt/wxfx/example目录）

威胁分析-02

识别安全防护软件的查杀记录，对于评估系统受感染的程度和了解攻击者所使用的工具至关重要。通过检查安全日志，可以获取被检测到的威胁信息。
请问，Windows Defender 检测到的第一个恶意软件的威胁ID是什么？（请将答案编辑并存入/opt/wxfx/answer/2.txt文件中，参考/opt/wxfx/example目录）

威胁分析-03

了解恶意软件的内部名称（如开发者给它的命名）有助于识别其家族、版本和特定功能，进而制定有效的防御策略。
请问，系统中正在运行的恶意软件的内部名称是什么？（请将答案编辑并存入/opt/wxfx/answer/3.txt文件中，参考/opt/wxfx/example目录）

威胁分析-04

逆向分析恶意软件时，确定其在进程内存中存储关键数据的位置，对于理解其工作机制和防范进一步的攻击非常重要。
请问，恶意软件在进程内存中存储密钥的内存地址是什么？（请将答案编辑并存入/opt/wxfx/answer/4.txt文件中，参考/opt/wxfx/example目录）

威胁分析-05

分析恶意软件的行为包括了解其在系统中启用了哪些权限，这有助于评估其潜在的危害和攻击范围。通过检查进程的权限列表，可以发现其可能执行的敏感操作。
请问，恶意软件在其进程中启用了多少个权限？（请将答案编辑并存入/opt/wxfx/answer/5.txt文件中，参考/opt/wxfx/example目录）

威胁分析-06

在分析勒索软件的行为时，确定其在内存中加载的位置对于深入理解其运行机制和发现潜在的漏洞非常重要。通过内存取证，可以找到打开勒索软件文件的设备的虚拟地址。
请问，打开勒索软件文件的设备的虚拟地址是什么（16进制）？（请将答案编辑并存入/opt/wxfx/answer/6.txt文件中，参考/opt/wxfx/example目录）

溯源反制-01

在用户家目录留下23798632.txt

溯源反制-02

尝试在攻击机上提升权限并在提升权限后在高级用户的家目录中留下862382.txt文件