Operating Systems

What is the standard location of Windows event logs?

 The default location of event logs on Vista/2008 and better is

"C:\Windows\System32\winevt\Logs\"

Networking

If you're on a machine and it can't resolve a URL, but if you browse to the IP address for the URL it displays the web page, what may be causing the issue? What's one step you could take to attempt to resolve it?

The technical reason for resolving host issue is that the DNS servers configured by your Internet Service Provider (ISP) takes long time to find a mapping IP address for the URL you have entered. This is probably due to change in ISP or change in DNS settings by your ISP

solutions:

- restarting router or modem

-fix configuration dealing with dns

Security Principles

What is CVSS? Describe the three metric groups that compose it.

-CVSS is the common vulnerability scoring system.

Metric groups:

-base-Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: the Exploitability metrics and the Impact metrics.

-temporal-The Temporal metric group reflects the characteristics of a vulnerability that may change over time but not across user environments

-environmental- The Environmental metric group represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

**Cyber Threat Intelligence**

Using information from this recent CTI report, provide examples for each of the four points of the Diamond Model. (Recommendation is to begin with the actual report, and then potentially use the article to help provide context.)

<https://blog.nviso.eu/2020/09/01/epic-manchego-atypical-maldoc-delivery-brings-flurry-of-infostealers/>

<https://www.zdnet.com/article/malware-gang-uses-net-library-to-generate-excel-docs-that-bypass-security-checks/>

Adversary

* **Epic Manchego**

Infrastructure

SHA256 HASH:

* 341c88ec95fe4544b021ca347504064ae6d75c5e6e34d15f0823added11270e2
* 33105255568dc2908288601f702518c107d1262f127328218fdde70047b1a78b

Victims:

* medical equipment sector, aluminum sector, facility management and a vendor for custom made press machines.
* companies

Capabilities:

* **phishing emails**
* Microsoft Office documents are created using the EPPlus software rather than Microsoft Office Excel, these documents may fly under the radar as it differs from a typical Excel document;