Global Information Assurance Certification Paper

GIAC Security Essentials Practical (version 1.4)

Option 2: Case Study

A Secure Implementation of HP OpenView Web Transaction Observer

Author: Matthew Patterson
Date: 26 September 2002

Table of Contents

1 Scope

This paper discusses an actual implementation of the product HP OpenView Web Transaction Observer 3.0 (WTO) as a repeatable service offering within an Outsourcing environment. This paper describes the product architecture of WTO, and its main components. Then a high-level threat analysis is performed on this architecture, uncovering several security vulnerabilities in the standard 'out-of-the-box' product. Then the actual architecture implemented is discussed in terms of the mitigation or acceptance of risks. As this is an implementation that has been released into production, some details will be omitted from this paper, or will be changed where appropriate. Where sources are referenced they will be indicated with the reference number in parentheses, for example [1], matching the reference listed in Section 8.

2 Introduction

In an outsourcing environment it is an important part of Service Level Management to define acceptable measures of performance, and then to monitor the performance of the outsourced resources and report on the metrics gathered. This is often an important part of outsourcing contracts.

One important set of performance data to be gathered for web sites hosted in an outsourcing environment is the response-time and availability of web sites and applications from an end-user's perspective.

In a recent project aiming to build an End To End Web Performance Monitoring of customer websites as a service to be offered to existing and new outsourcing customers a product HP OpenView Web Transaction Observer was used. A trial implementation for a web application used by reseller customers within the Asia-Pacific region was performed. This web application had been the subject of many complaints from reseller customers for slow performance. Since then the WTO service has been implemented in production as a service that can be sold to new and existing outsourcing customers.

3 HP OpenView Web Transaction Observer

HP OpenView Web Transaction Observer (WTO) is one product of the HP OpenView suite. This product aims to provide true end-to-end response time monitoring of web transactions from an end-user's perspective. This gives a good real-time snapshot of the health of a web site.

WTO has Client Monitors that are downloaded and run within end-user's web browsers that post performance data back to a central Management Server. These provide real-time performance data gathered from the user's browser as it downloads web pages, and distinguish where time is spent in processing each web transaction such as in the network, on the target web server, in DNS processing time. This architecture is described below.

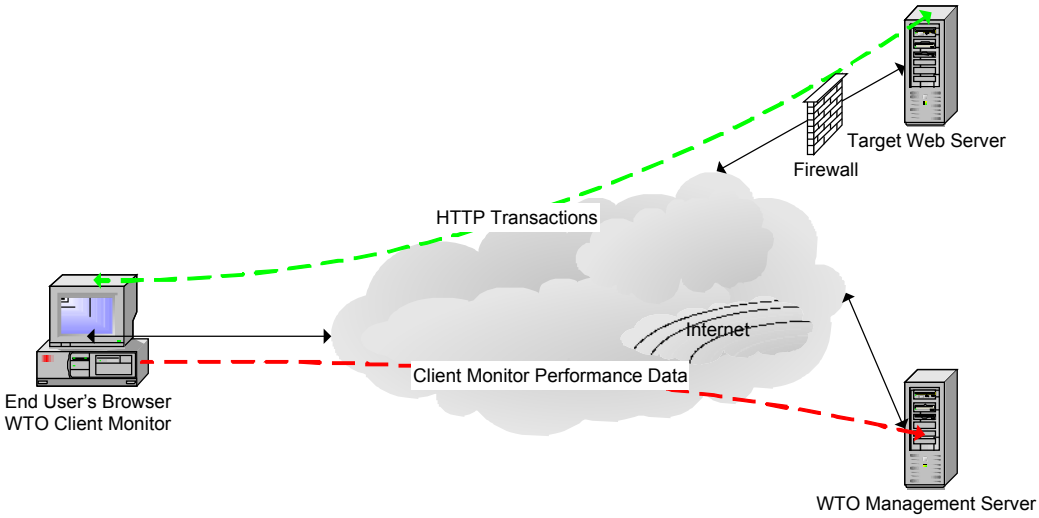

Figure 1 WTO Architecture

The Client Monitor is downloaded onto the user's browser as an ActiveX component, or as client-side JavaScript by embedding HTML tags into the existing target web pages. An XML configuration file is also downloaded, and contains the URL's that are to be monitored by the WTO Client Monitor. Whenever the browser begins downloading one of specified URL's, then the Client Monitor sends performance data for that download back to a central WTO Measurement server using a HTTP/S Post.

The web site to be monitored can be instrumented with a WTO Web Server Monitor, provided the web site runs on a Microsoft Internet Information server (IIS) platform. WTO provides the web server monitor as a DLL that can be installed on web servers as an ISAPI filter. The WTO Web Server Monitor sends performance data to the WTO Management Server via HTTP Post. This data can be used in combination with the performance data from the Client Monitor to help identify poor performance experienced by the user due to poor system performance from poor network performance.

The WTO Measurement server receives all the performance data, and stores this information into a central database. The WTO product provides a web interface for reporting allowing views of the real-time performance of the target web site. This allows managers a good health check of the performance of their web sites as seen by their users. Integrations can be configured with other HP OpenView products to facilitate service assurance functions such as alarming when service levels are violated.

More specific information about WTO can be found in [1].

4 Before: Risk Analysis

Before a threat analysis can be taken, we must first define what a threat is: "anything that would negatively affect the confidentiality, integrity or availability of your systems or services"[2]. Vulnerabilities are defined as "weaknesses that allow threats to happen" [2].

Clearly understanding the threats and vulnerabilities exposed by implementing WTO will allow us to analyse the risk in undertaking this implementation. Risk is often calculated as the product of Threats and Vulnerabilities [1]. For this Risk analysis, we will be performing a qualitative risk assessment based upon the possible business impact of threats, due to the vulnerabilities if the implementation. Each risk identified will be classed as High, Medium or Low risks. High risks will clearly be unacceptable and must be mitigated. Low risks might be accepted or transferred.

The following threat analysis will focus on WTO implementation-specific vulnerabilities rather than those facing the average web application in today's hostile Internet environment, which have been well-documented and discussed by others, including [2]. These threats and associated risks are out of scope for this paper, but should be accepted, mitigated or transferred. These threats include, but are not limited to:

- Large Scale Interruption of Service (Fire, Flood, Earthquake)
- Physical infrastructure failure (CPU failure)
- Malicious Insider Attack

To perform a threat/vulnerability assessment we must first identify the threats and vulnerabilities exposed by an implementation of WTO monitoring as shown in Figure 1. This is best done by first identifying the relevant threat vectors of attack for this architecture:

- Outsider Attack from Network
- Malicious code

For the purpose of this paper, it is assumed that the threat vectors of; Outsider Attack from telephone, Insider Attack from Network and Insider Attack from Local System are not exposed specifically by implementing the product WTO. These threat vectors still exist, but are outside the scope of this paper.

The following summarises the vulnerabilities or threats exposed by the implementation of WTO. Each threat is briefly described, and given a risk level of high, medium or low based upon the probability of the threat occurring and the business impact if it did occur. It should be noted that prior to this implementation, the architecture in Figure 1 failed an internal security review where a well-defined security policy and standards were used to measure the security of the implementation.

4.1 WTO Measurement Server Hacked

If WTO is deployed to monitor the performance of a public facing web site, then the WTO Client Monitor will be downloaded by outside users, and therefore the WTO Measurement Server must be accessible from the public internet for Client Monitors to send performance data to via HTTP Post.

If the WTO Measurement Server is hacked, then the three cornerstones of security: integrity, confidentiality and availability are significantly at risk. WTO stores performance and configuration data concerning customer web sites being monitored in a database locally. This may be information if it were revealed to customer's rivals or to the public media would be damaging to the reputations and businesses both the customer and the outsourcing company. If this data were altered, then any SLA's between the outsourcer and the customer might be significantly affected, as financial penalties or costs to both the outsourcing company and the client could result from false performance data. Also, the availability of the WTO monitoring service could not be guaranteed, which once again could have negative financial impact on the outsourcing company. On a side note, it is a common hacker tactic to target monitoring systems both to gain configuration information on the system or web-site monitored, and to silence any possible alarms resulting from a subsequent attack on the monitored systems, as shown by the Mitnick attack [3]. So a loss of availability of the WTO Measurement Server could be a precursor to further attacks on the customer's web sites.

As the impact of this threat is large in business terms for both the outsourcer and the customer, the risk of this threat has been rated as High.

4.2 Denial Of Service Attack

The WTO Measurement server is vulnerable to a Denial of Service attack, as it is reliant on receiving performance data from both Client Monitors and Web Server Monitors as HTTP/S Posts. An attacker could flood the WTO Measurement Server with false HTTP Posts, preventing the processing of correct performance data. This could impact the outsourcing company, as SLA's may be violated due to downtime of the WTO monitoring service causing financial penalties to be imposed. As above, this could also be a precursor to an attack on the customer's web-site. The availability of the WTO monitoring is threatened.

The business impact of this threat is lower than that of the WTO Measurement Server being hacked by an outside attacker, but still real in today's environment where scripting engines and malicious code can easily engineer a Denial of Service attack. This risk is therefore classed as a Medium level risk.

4.3 False Performance Data

If an attacker were to analyse the traffic between the Client Monitors and the WTO Measurement server, then false performance data could be inserted into the WTO database using a similar mechanism to the DoS attack above, but rather than flooding the WTO Measurement Server, the aim is to format HTTP Post requests to mimic real performance data. This would impact the integrity of the WTO monitoring data gathered for a customer's web sites, resulting in flawed monitoring and performance reporting.

The probability of this threat is low, as the WTO Measurement infrastructure

would not have a high visibility, but this is not a guarantee of safety, as it is quite possible that scanning robots could locate the WTO Measurement Server's URL. However the attacker would be more likely to attempt to hack into the server rather than spoof performance data sent to the Measurement Server. The business impact of this threat is classed as medium, as the integrity of the WTO monitoring and reporting would be compromised, and if this were later revealed, would impact the outsourcing company's or the customer's reputation. Overall, this risk is classed as Low/Medium.

4.4 Malicious Code

The WTO Measurement Server runs on a Microsoft Windows 2000 platform, using IIS and SQL Server. Therefore the availability of the WTO monitoring system is at risk from malicious code attacks of which Code Red and Nimda are two high profile examples.

The probability of this threat is quite high, given the incidence of viruses and worms in the Internet today, and the impact of such an attack would be a reduced availability of the WTO monitoring. However, many such malicious code targets these system platforms such as Microsoft Windows 2000 and IIS. However this threat can be mitigated by the regular application of Microsoft's security updates.

It should be noted that in the early stages of the pilot, WTO was installed on a development system. During the install, WTO modifies some of the security settings in IIS, specifically the permissions on some virtual directories created in IIS[1]. Microsoft security patches had been installed on the development server previously, and were not reapplied. Within one day the Nimda virus infected the system. This clearly shows the need for reapplying of all security patches and updates after WTO is installed, and highlights an important vulnerability exposed by the product WTO that can be mitigated very simply.

The overall risk of this threat is Medium.

5 Implementation: Addressing the Risk

The following diagram shows the architecture that was implemented [7] to address the risks identified above in Section 4. There are three ways to address risk; to accept the risk, to mitigate the risk, or to transfer the risk in a way such as the insurance model [4]. The architecture implemented will be described at a high level, and then the ways in which the risks identified in Section 4 are addressed will be discussed.

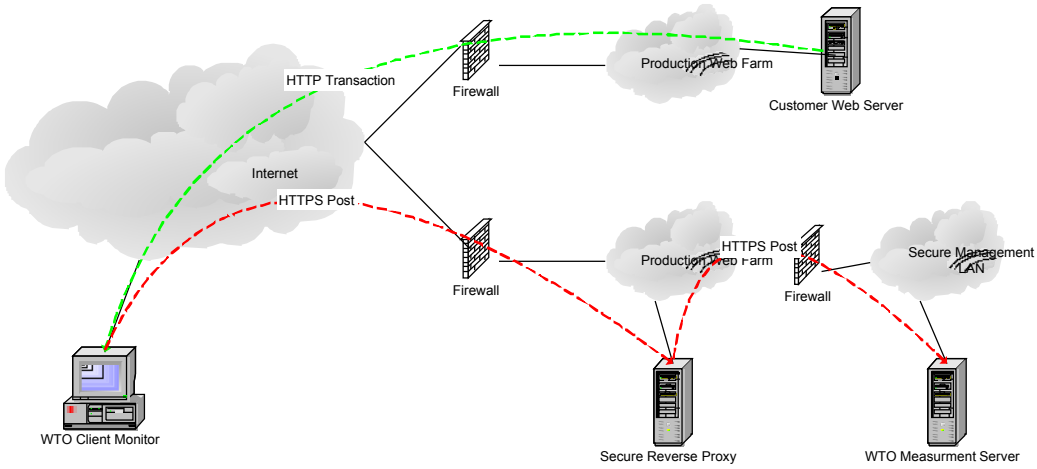

Figure 2 Implemented WTO Architecture

5.1 Client Monitor to Measurement Server Traffic

All traffic from the WTO Client Monitors to the Measurement Server are configured to use HTTPS Posts, and never HTTP Post. WTO provides this capability automatically when monitoring web sites that are using HTTPS, but as a default uses HTTP Post to send performance data back to the measurement server for all other types of web site. This was a simple configuration change within WTO, but needed to be explicitly performed.

5.2 Reverse Proxy

The most significant addition to the architecture is the use of a Reverse Proxy system to sit between the WTO Measurement Server and the public Internet. A proxy is "a service handling the request made by another for a resource on a foreign client/host and serves as an intermediary between all systems involved"[5]. This system receives incoming web requests, inspects some packet header fields to ensure that it is a valid HTTP request, and if it is valid then forwards the request to the content server. The proxy then alters packets received from the content web server to set the proxy system as the originating system. This helps protect the web server from attacks such as the Ping of Death[5]. In addition, the proxy system is less vulnerable than a web server, as it is running fewer services and many attacks attempt to exploit specific vulnerabilities in a web server product, which are not available on a proxy system. This also protects the integrity of the content stored on the web server as if a hacker compromises the proxy system then the content is still stored on a separate system.

In the architecture implemented for WTO the reverse proxy sits in a production web farm, behind a firewall. This firewall has been configured to only allow inbound packets to the reverse proxy system on port 443 from the Internet, as the reverse proxy is only expected to accept inbound HTTPS Posts from WTO Client Monitors. This secure reverse proxy was built on a HP-UX platform, which was hardened to meet HP's security standards for HP-UX web servers hosted in a public Internet facing web farm. There are

multiple web server products commercially available that provide secure reverse proxy functionality, including Apache and Netscape Proxy Server [6].

The reverse proxy is implemented so that all HTTPS Post traffic intended for the WTO Measurement Server from the public Internet is posted to the proxy system, which is configured to map external URL's to internal URL's. The proxy maintains session information so that any return traffic from the WTO Measurement Server to the public Internet has it's source information altered so that to external destinations, the traffic originated from the reverse proxy system. This hides knowledge of the WTO Measurement Server from the public Internet and potential attackers. This is similar to a common mechanism used by many firewall products for hiding the internal IP network from external visibility. The proxy system is configured so that only valid URL HTTP Posts will be forwarded to the Measurement Server. All other URL hits to the proxy system will be denied.

The secure reverse proxy is only accessible to users from within the Management LAN using SSH sessions. Processes restricting users to those with a legitimate business need to use the system, meeting HP's security standards, control access to the system. This helps mitigate the threat of Insider Attack from Network threat vector.

5.3 WTO Measurement Server

The secure reverse proxy than forwards all inbound HTTPS traffic through to the WTO Measurement Server still using HTTPS Post. Traffic between the Proxy and the Measurement Server passes through a second firewall that separates the web farm from the management LAN. This firewall is configured to only allow HTTPS traffic between the proxy system and the Measurement Server on port 443.

The WTO Measurement Server is hosted within a secure Management LAN, and is hardened according to HP's security standards, including the installation of all recommended system patches and security updates as recommended by Microsoft. These were applied after WTO was installed. All service ports other than inbound HTTPS, and SSH access were disabled. This ensures that the WTO database, which might contain sensitive information concerning a customer's web-site performance, is not stored in a public Internet facing web farm, protecting the confidentiality and integrity of this data.

6 After: Implementation Review

The risks identified and assessed in section 4 will be reanalysed in terms of the architecture implemented in Figure 2. This will be in order to see if the risks have been addressed either by mitigation to reduce the risk, acceptance or transferral.

6.1 Measurement Server Hacked

This risk was classified as High in Section 4 above, due to the high business and financial impact that could arise from the integrity, confidentiality and availability of the Measurement Server being compromised. In Figure 1, the WTO Measurement Server was attached to the public Internet as a web server. In Figure 2, the Measurement Server is hosted in a secure management LAN, with two firewalls between the system and the public Internet. This has reduced the probability of an outside attacker gaining control of the system. No traffic is allowed to pass directly between the Internet and the Measurement Server, instead being routed via a reverse proxy system. This means that the Measurement Server is much less vulnerable to outside attack from the network.

For an attacker to compromise the Measurement Server, they would first need to compromise the reverse proxy system. No knowledge of the WTO Management Server is available to the public Internet. All WTO Client Monitors download an XML configuration file from the monitored web server as part of their standard operation, and these configuration files direct the Client Monitors to post performance data to the reverse proxy system. All responses originating from the WTO Measurement Server that pass into the public internet are modified by the reverse proxy so that the proxy system is the originator of those packets. So the outside attacker would not be aware of specific information regarding the existence of the WTO Measurement Server until the reverse proxy system was compromised.

The reverse proxy system is less vulnerable to attack than a Windows 2000 platform system running IIS. It is running less services that could be compromised by and attacker, and is protected by a firewall that should only allow inbound traffic to the proxy system on port 443. The HPUX platform is less vulnerable to malicious code attacks as statistically most such attacks target Microsoft platform systems, and in addition the system has been hardened in line with define security standards and policies.

If an attacker compromises the reverse proxy system, the WTO Measurement Server is protected by a second firewall that will only allow traffic from the reverse proxy to the Measurement Server on port 443. This limits the opportunities to further attack the WTO Measurement Server and protects the integrity and confidentiality of the WTO monitoring service. However if the reverse proxy is compromised, then the availability of the WTO monitoring service is compromised. However, if this is detected using host-based intrusion detection systems, there is the opportunity to replace the reverse proxy with a honey pot system, meanwhile the reverse proxy system can be moved to a different IP address, and the WTO monitoring service resumed. This approach might help identify how the reverse proxy was compromised in the first place so that this can be addressed later.

Based upon the mitigation of risk provided by the system architecture shown in Figure 2, this risk is reduced to Low.

6.2 Denial of Service Attack

This risk was classed as Medium in Section 4, and is somewhat addressed in the architecture of Figure 2. The reverse proxy system sits between the WTO Measurement Server and the public Internet, and would be the initial target of all Denial of Service (DoS) attacks.

Both the reverse proxy and the Measurement Server have been sized anticipating a high volume of performance data to be received, but is still vulnerable to DoS attacks. However, the reverse proxy system will protect the Measurement Server from these attacks. The proxy system investigates each packet, and only forwards valid HTTPS packets to the Measurement Server. This means that a DoS using repeated resource requests that are not valid HTTPS would only impact the reverse proxy. This would mean that in the case that the reverse proxy was the target of a DoS attack it is feasible to replace the reverse proxy system with a second reverse proxy, and deploy updated WTO XML configuration files to the monitored web-sites. As the WTO Client Monitor re-downloads this file each time the user starts a new a monitored server the WTO monitoring service could be restored faster, as the Measurement Server was still available.

However, it should still be noted that DoS attacks using valid HTTPS packets would still impact the availability of the WTO monitoring service. This residual risk is accepted, as the WTO monitoring service is not a mission critical service for the customer or HP, and the ability to deploy a second reverse proxy system is an acceptable resolution path. To transfer this risk the time to deploy such a system should be built into any SLA's agreed upon with the customer. This risk is classed as Low/Medium.

6.3 False Performance Data

This risk is addressed in the implemented system architecture by requiring all WTO Client Monitors to send performance data back to the Measurement Server using HTTPS Posts. This helps mitigate the risk of an attacker scanning this traffic to identify the format and expected contents of the performance data packets. This level of encryption is not completely secure, and better levels exist, but given that this is not a mission critical service this is acceptable in addressing the level of risk identified and to counter against any reasonable expected loss. If the customer's web site is also monitored with other HP OpenView products such as HP OpenView Operations or HP OpenView Network Node Manager then the impact of an attacker planting false performance data is reduced. The remaining risk is accepted, and is classed as Low.

6.4 Malicious Code

The risk of the WTO monitoring service systems being attacked by malicious code is addressed in several ways. By placing the WTO Measurement Server in a secure management LAN with no direct access from the public Internet the threat vectors of malicious code is reduced. The reverse proxy is based on a HPUX platform, which is less vulnerable to malicious code than Microsoft platforms, which are statistically targeted by most malicious code.

The remaining risk is mitigated by hardening the reverse proxy system and the Measurement Server according to internal security standards and policies. Together, these actions reduce the probability of this threat occurring. It should be noted that these vulnerabilities are not completely reduced, as new viruses and other malicious code are discovered every day. However these actions help remove any vulnerability exposed by the implementation of the WTO product, and place the burden of managing this risk onto the operational processes used to manage systems in production web farms and the management LAN. This risk is classed as Low/Medium.

7 Conclusion

Securely implementing End To End Monitoring based upon the product HP OpenView Web Transaction Observer required implementing this product within an overall architecture designed to reduce the threat from outside attackers and malicious code.

The architecture implemented was based upon the central concept of a reverse proxy system and firewalls to provide "defence in depth" [2]. The reverse proxy system allowed the implementation of a policy that the WTO Measurement Server should be inaccessible directly from the Internet. The two firewalls between the Measurement Server and the Internet helped enforce this policy. By forcing all WTO traffic to use HTTPS, the exposure to false performance data being inserted into the WTO database is reduced. The threat of a Denial of Service attack being directed against the WTO monitoring service is somewhat addressed by the implementation of the reverse proxy, and means that the Measurement Server itself is less vulnerable to this attack, and can be used together with a second reverse proxy system in the event of such an attack. The risk of malicious code was reduced by hardening the WTO monitoring systems using internal security standards, and basing the reverse proxy system on a less vulnerable platform such as HP-UX.

The architecture implemented here was successful, in that the risks identified were reduced through mitigation and the residual risk was accepted. Also, the proposed architecture passed an internal security review before it was implemented. The architecture used was generic enough to be useful for most monitoring implementations using the product HP OpenView Web Transaction Observer, where this monitoring is performed over the public Internet.

8 References

1. Hewlett-Packard. “HP Web Transaction Observer 3.0 Users Guide.” Edition 3. April 2001.
   URL: http://ovweb.external.hp.com/ovsnmdps/pdf/b7238-90004.pdf
2. SANS GSEC Course Notes. “Security Essentials: Defence in Depth.” SANS 2001
3. SANS GSEC Course Notes. “Security Essentials: Risk Management: The Big Picture.” SANS 2001
4. SANS GSEC Course Note. “Security Essentials: Risk Management and Auditing.” SANS 2001
5. Mourer, Darrin. “Why Place Your Web Servers on the Web? A Look at Web Proxy Technology and Architecture.” RemainSecure.com. November 8, 2000.
   URL: http://www.remainsecure.com/whitepapers/general/webpxy.htm
6. Netscape. “Netscape Proxy Server Administrator’s Guide for Unix.” Version 3.5. March 1998. URL: http://developer.netscape.com/docs/manuals/proxy/adminux/revpxy.htm
7. Douillet, L and Mathieu, C, “Service Architecture for End to End Web Monitoring (WTO)”, Hewlett-Packard, November 2001

9 Glossary

The following glossary is based upon the SANS “Security Essentials Glossary of Terms” 2001.

1. **Browser**: A client computer program that can retrieve and display information from servers on the World Wide Web.
2. **Denial of Service**: The prevention of authorized access to a system resource or the delaying of system operations and functions.
3. **Firewall**: A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.
4. **Honey Pot**: Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.
5. **HTTPS**: When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL.
6. **HTTP**: The protocol in the Internet Protocol (IP) family used to transport hypertext documents across the Internet.
7. **Internet Protocol (IP)**: The method or protocol by which data is sent from one computer to another on the Internet.
8. **Malicious code**: Software (e.g., Trojan horse) that appears to perform

a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

9. **Ping of death**: An attack that sends an improperly large ICMP echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash.
10. **Secure Sockets Layer (SSL)**: A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.
11. **Security policy**: A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.