Naples Eye

Dutizer

Incident Handling System (IHS)

Protect your Reputation

Let HacWar handle the Incidents

Incident Handling System (IHS)

❑ About HacWar

HacWar Systems, is a leading provider of secure computing solutions that help companies protect their assets. Founded in 2009, HacWac combines SaaS, networking, and cloud computing technologies into a full portfolio of products that enable protection for companies and datacenters against web defacements. HacWac helps them build simpler and more cost-effective IT environments.

HacWar®
With the constant growth of the Internet, more and more web sites are being deployed. Websites became essential for all businesses for all the benefits they come with. But nothing is risk free with publicity. By their nature, web applications are often widely accessible to the Internet as a whole meaning a very large number of potential attackers. All these factors have caused web applications to become a very attractive target for attackers and the emergence of new attacks. And so websites are the most commonly available figure for everyone around the world simply it runs on the Internet. And the first thing comes in mind when we talk Internet is availability as a nature of the internet. Still, having all standards security measures in place does not make any business 100% protected

Naples Eye

www.hacwar.com

❑ INTRODUCTION

The adoption of the web browser as the medium to provide application access and Internet communication has completely permeated the enterprise computing environment. More than ever, organizations are implementing browser-based applications as solutions for nearly every aspect of their business operations. From public sites to corporate web e-mail systems to application portals, web applications have become increasingly business-critical.

This explosive growth of web applications has created numerous challenges for enterprises.


DON’T PANIC HacWar GOT YOUR BACK

❑ DON’T PANIC HacWar GOT YOUR BACK

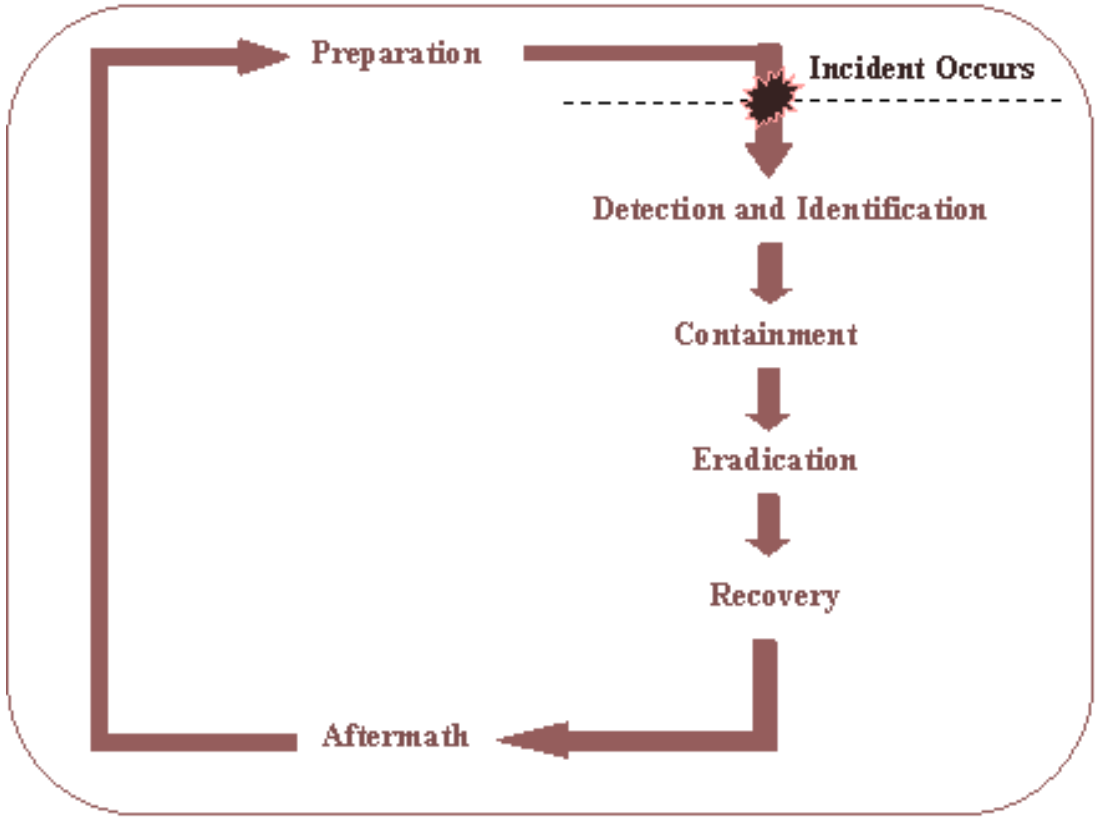
A simple incident handling process such as the one here might not help in the event of an incident that involve defacement of a corporate website since that might happen any minute during the day or the night, and involve a complicated coordination between different groups of IT administrators.

A simple incident handling process.

❑ HacWar AUTOMATES THE INCIDENT HANDLING PROCESS

Although the symptoms may be complex, the prescription is simple:
Organizations need an incident handling solution that ensures secure website and protect the business reputation.

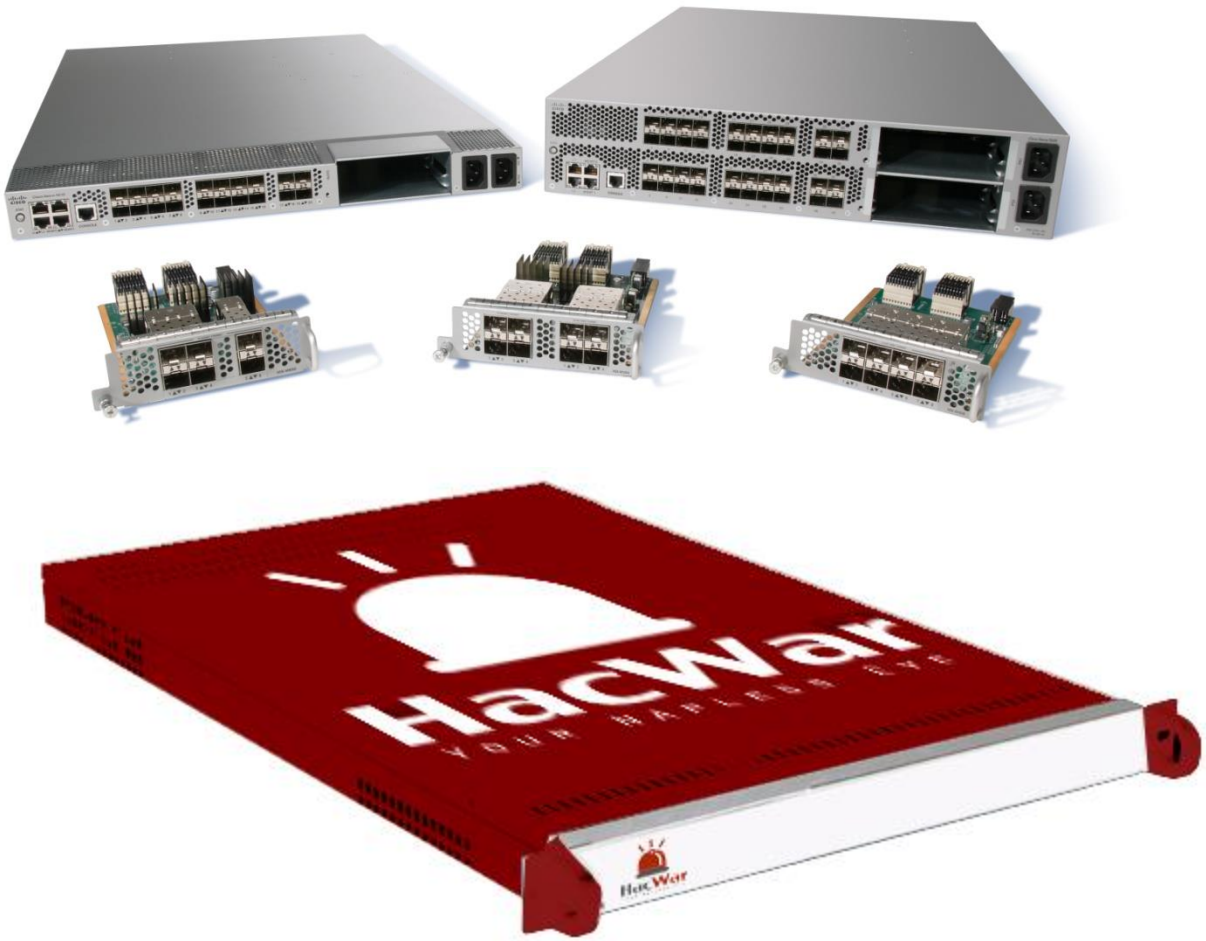
An incident handling system (IHS) is a network server or appliance, which typically resides in the DMZ next to the web applications and the Internet. It is effectively a “trusted processor” for web servers, acting as a guard to keep eyes on the web applications. An incident handling system monitors web servers constantly through different ways to ensure the security and safety of the website all the time. In an event of a website compromise or defacement, the HIS will react upon with pre-configured settings to perform the required actions.



❑ HacWar AUTOMATES THE INCIDENT HANDLING PROCESS

Things are required of a high-quality incident handling solution:

1) A systematic automated process following the best practices of incident handling process.
2) A proactive preparation for incidents which involve a package of system setups to react upon, those might be the web server itself or other network devices interact with it ; backups tested and tried in hand; a Computer Security Incident Response Team (CSIRT) to be alerted through different channels.
3) A continuous periodical checking on the web server with a pre defined time interval. Including a varieties of key ways to determine the status of the web site these methods include: visual checking of the website with a different levels of thresholds to see whether a pre defined crop of the web page has been change or not. Other technique is to check certain included or excluded keywords list. Another technique is to perform URL analysis to check to see if any has been added by malicious attacker that is not supposed to refer the site visitors to.
4) Web server protection and containment. IHS isolate web servers from direct Internet access; control access to the applications it protects; ensure that files uploaded to the application(s) are free of malware such as viruses, worms, and Trojans; store and forward related logs which are valuable for further investigation.
5) A quick and swift action in the event of the incident coordinated with all the parties involved in the incident. This coordination has been built already in setting up the system, which include coordination with other network elements such as firewalls, routers, DNS, backup web server, the syslog server and the victim web server
6) A recovery is what we all aim to after an incident. Rolling back to the previous stage before the incident after doing the required analysis and investigation to prevent such thing from occurring again. Depending on when has been done during the series of action rolling back should take place accordingly.
7) Finally what conclude an efficient handling of an incident is a professional logging and reporting which contains all the useful information related that could be beneficial in a forensic report or lessons learned.


HacWar
YOUR HACKER EYE

❑ Incident Handling System Appliance

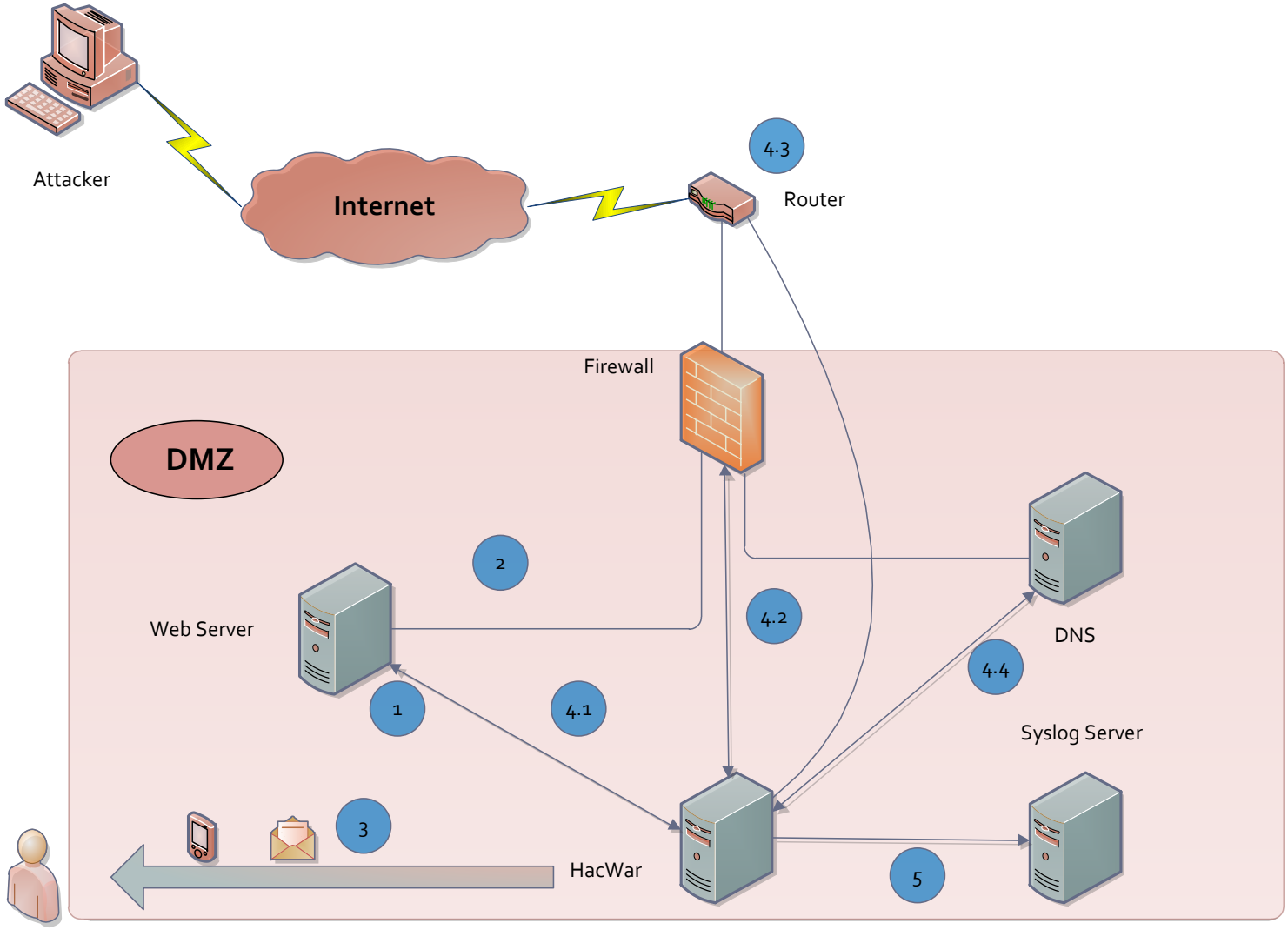
HacWar box is a secured box given the nature of the responsibility in charge of, what makes HacWar secure is that:

1) The appliance is encrypted with the highest level of encryption to ensure the confidentiality nature of the data stored in. even if the box given away cracking the files stored would be impossible.
2) Controls User Access: As an extra layer of protection, HacWar will challenge who attempt to access it, either challenging admins for their credentials or transparently checking existing authentication credentials. HacWar authenticates users using an organization's existing security framework, which may include LDAP, RADIUS, certificates, NTLM, local lists, etc. Several different ways to identify a user are supported, including password, certificate, token, group membership, IP address, subnet, and network identifier.
3) Supports SSL Encryption.

HacWar keeps eyes on the web server

❑ HOW HACWAR WORKS?

1) HacWar keeps eyes on the web server by performing the following metrics to determine whether the website got defaced:
    1) Visual checking: through crop of the web page threshold comparison.
    2) Included or excluded lists of strings
    3) URL referals within the web page.
2) The web server gets compromised by an attacker.
3) HacWar immediately alerts the right party through SMS/ email, with a full detailed report of the incident.
4) Through preset of rules, HacWar may do one or more of the following actions:
    1) Shut down the web server/ service, or redirect it to another site.
    2) Block the access at the firewall
    3) Block the access at the router
    4) Redirect the visitor to another site through DNS redirection.
5) Finally log the incident back up the logs to a pre-configured syslog server.



HacWar Network Diagram and Operational Steps

❑ Features and Benefits

TIME GLOBAL SYNCHRONIZATION	As a security device a lot of care will be taken for the time when the incident happened, as a result synchronizing the appliance is crucial to assure the accuracy of the logging and reporting.
SIMPLE AND EASY SETUP	Through a step-by-step wizard HacWar can be up and running, with a user friendly interface and intuitive menus HacWar would be a straightforward for all administrators to work with.
SINGLE POINT OF CONTROL AND MONITORING	HacWar provides centralized control of configurations across the entire physical and virtual IT infrastructure, including servers and network devices, applications, and multiple platforms and operating systems.
BUILT-IN INTEGRATION WITH SYSLOG CENTERAL SERVER	As part of the HacWar suite, HacWar integrates with syslog Center out of the box. The integration enables admins to correlate change and event information to transform raw data into actionable knowledge. It also provides a centralized view of date center security.
WORKFLOW TOOLS FOR MANAGING FAILED CONFIGURATIONS	The Remediation Manager module provides role-based workflow tools that let users approve, deny, defer or execute remediation of failed configurations.
SUPPORT FOR FASTER, EASIER AUDIT PREPARATION	Tripwire Enterprise dramatically reduces the time and effort for audit preparation by providing continuous, comprehensive IT infrastructure baselines along with real-time change detection and built-in intelligence to determine the impact of change.
ENCRYPTION TO ENSURE CONFIDENTIALITY	HacWar does encrypt the appliance to ensure the security of all the data stored in, as well as the connection to the appliance is established through secure connection whether it is SSH or SSL.

Protect your Reputation

Let HacWar handle the Incidents

HacWar is an innovative way of protecting your most valuable asset, your “Reputation”. By automating the incident handling process and monitoring your public website in a constant manner. HacWar comes as a real need on a very unrested Internet where the fear of abusing and defacement going around is every organization issue

❑Cover Back

Support Enquiries
Email: support@hacwar.com

General Enquiries
Email: info@hacwar.com

Partnership Enquiries
Email: partner@hacwar.com

Press Enquiries
Email: press@fhacwar.com

Tel :- 966-1-4857232

Fax :- 966-1-4857262

Saudi Arabia
Jordan
United Kingdom
Hong Kong
China