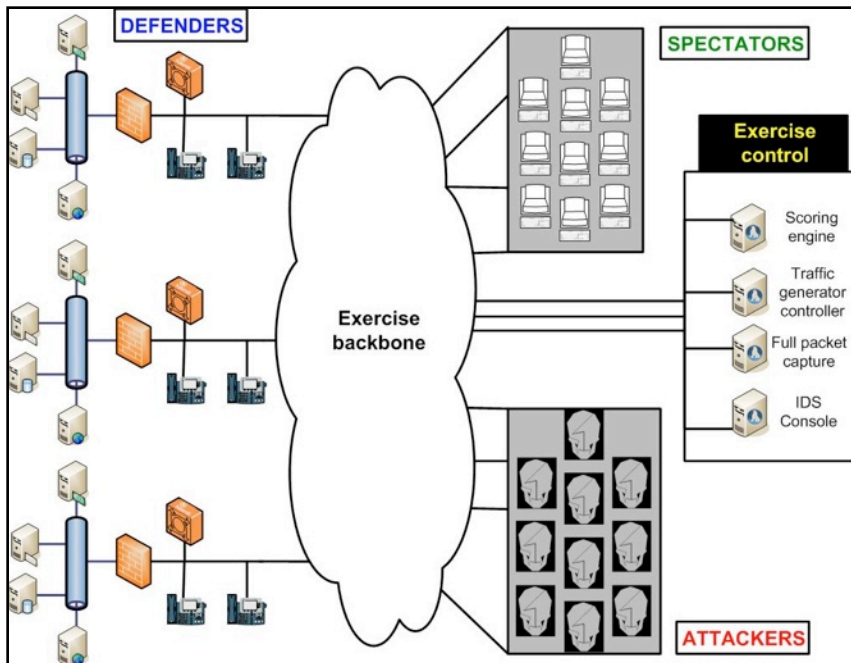




Cyber Exercises

What is a Cyber Exercise?

...and why do I need one?



A cyber exercise is a live computer network attack and defense event. A typical exercise runs at least one day for a small team and up to five days for large organizations or multiple teams. Teams generally fall into two categories; attackers and

defenders. Defenders are scored on their ability to keep their IT systems up and functional in support of their business processes. Attackers are scored on their ability to disrupt business operations.

Why White Wolf Security?

White Wolf Security has driven the market in information security training. In 1999 we taught one of the first hands on hacking courses.

Cyber Exercises are the next logical evolution of training and once again, White Wolf Security is leading the pack by providing the most realistic exercises in the market today.

Our exercises include the latest in technology and support VoIP, SCADA, full packet capture and custom traffic generators.

– CEO Tim Rosenberg



EVALUATE PEOPLE, PROCESSES AND TECHNOLOGY IN A LIVE ENVIRONMENT

Our complex environment allows you to run any number of scenarios that you can use to test people, processes and technologies in a live, consequence free environment.

The flexibility of the environment allows us to implement any response call list using an internal VoIP network. Our



proprietary traffic generators allow you to test your technology's ability to filter out white noise and identify real network attacks.

The central inject server can send emails to teams which can test their ability to respond to management and customer requests in a timely and effective manner.



THE PARTS OF A CYBER EXERCISE: RED CELL

The Red Cell is responsible for conducting attacks against the various defending teams. They are limited only by their tools, imagination and skills. Over the years, we have seen a variety of creative attacks, some successful and some not so. One year, a Red Cell member compromised a team's PBX server and re-routed calls from the CEO into the Red Cell room. Hidden wireless access points and trojaned USB sticks have likewise been used to create stress and mayhem for the defending teams. The attacks have ranged from the silly (such as remotely forcing a Windows XP system to install Vista), to the damaging (the re-directing of critical logs to /dev/null and thus crashing the entire system).

No device is safe from the activities from the Red Cell. IP cameras, routers, firewalls, servers and desktops have all been compromised in one way or another during our exercises.

While the chief job of the Red Cell is to antagonize and stress the defending teams; they are to do so within an educational framework. In order for a Red Cell member to get credit for a

compromise, they must execute the Phone Home script; thus logging time of entry into a system. With the piece of information, the Red Cell is better



able to conduct a comprehensive after action review and recount what they did and when. This model thus maximizes the educational benefit for all.

THE PARTS OF A CYBER EXERCISE: BLUE CELL



In the midst of all the attacks, scoring traffic, injects, and pressures are the brave defending teams. The Blue Cell teams are responsible for maintaining a predetermined set of systems and services within a real business

environment. The Blue Cell is charged with operating as a real IT shop. They must keep critical systems up and running and prevent the Red Cell from getting in. All of this must be performed while receiving management and customer requests (injects) to provide support, fix issues, etc.

Most teams do exceptionally well, considering that the environment is designed to let in the attackers. After all, it is not much of an exercise if there is no conflict between the teams. But there is a bright side.

In every exercise we conduct; the Blue Cell must complete a network incident response form and open a case with onsite law enforcement (usually volunteer federal law enforcement officers). Upon completing the incident report a case is opened with the onsite officer. The team can now earn back lost points and may succeed in getting the offending hacker 'arrested' (banned from the network for a period of time). Just like real life; it is bad if the hackers get in, but if they do, it is better if they get caught.



WHITE WOLF SECURITY EXERCISE DEVELOPMENT

In 2008, look for the integration and deployment of SCADA and remote telepresence robotics into our exercises. Another first from the leader in Cyber Exercises



THE PARTS OF A CYBER EXERCISE: SCORING

Scoring is a very important part of any competition or exercise. Players and teams both need to know how they performed within a predetermined set of rules and evaluation criteria. It is here that again, White Wolf Security is leading the pack.

Defenders are scored within four domains. Teams are given an overall score on their ability to keep systems up and available while maintaining information integrity. Individuals on the team can also be scored on their ability to respond correctly and timely to inject requests. A separate score is kept that keeps track of compromises. This score represents the number of Phone Home scripts that have been executed by the Red Cell on a given team. Finally, teams are also scored on their ability to maintain business processes.

Attackers are scored on their ability to gain and maintain entry into the defenders' systems. Attackers are also scored on obtaining certain flags such as entries in a database and clear text passwords.

Scoring visualization is used to enhance and expand the exercise for the players and spectators. 3D animations show system status and compromises while the world map show who is attacking whom. News tickers are also available and accept posts from Red Cell and Exercise Control.



THE PARTS OF A CYBER EXERCISE: TRAFFIC



In most cyber exercises, generating non malicious traffic is a real concern. Without legitimate traffic, the defenders have an easy time since every packet is an attack. There have been several attempts to implement client side

traffic generators, but they have all fallen short of being reliable and scalable.

Every exercise is a bit different. Different services running on different IP addresses with unique settings and credentials. Setting up traffic generators used to be a time consuming and hit or miss endeavor. White Wolf Security has solved this by integrating a new proprietary distributed traffic generator into the Scoring Engine.

Teams are easily configured in the Scoring Engine. Teams are

assigned IP assets and IP assets are assigned services. The Scoring Engine takes this network information and uses it to command and control a distributed grid of agents. These agents generate legitimate network traffic to/from the defending teams and elsewhere within the network infrastructure.

We currently support HTTP, FTP, SSH, SMTP, POP3, DNS and MySQL. The clients are modular and can also support execution of any PERL and Python scripts.

CYBER EXERCISE TECH FACT - PACKETS EVERYWHERE



As part of our exercise infrastructure, we have the ability to mirror all packets into and out of the defenders' networks. This custom designed infrastructure allows for full packet capture, centralized IDS and even the ability to hang multiple IDS systems and compare alerts on identical traffic.

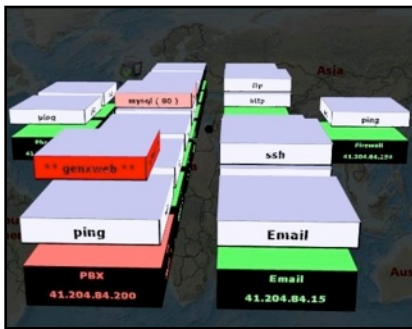


IN DEPTH: THE WHITE WOLF SECURITY SCORING ENGINE



The past year has seen vast improvements in our scoring engine. We've listened to your comments and implemented your suggestions (and even added a few of our own). Here's just a few of the additions.

4 suffered a data breach". The top news ticker complements the bottom ticker which displays messages from the Red Cell.



Top: Zoom in of attacker engaging Team 4

Bottom : Zoom in of 3D team status

1. Red Cell Tracking - using a phone home script, we can now track when Red Cell team members acquire execute privileges on systems. The scoring engine logs the hacker handle and allows for the attacker to post messages to the score display.

3. Mapping of Asset Status - the new scoring engine can associate a service or system availability with a geographic region. For example, a VoIP PBX server can be assigned as the telephone service provider for a given geographic region. If the server goes down, the corresponding map region on the Scoring Engine darkens to show service failure. This allows for a new range of scenarios and visualization for the exercises.

2. News Ticker - we now have the ability to dynamically update a scrolling news ticker on the main scoring engine site. This ticker can be used for general news stories; for example "Team

Many thanks to the team at Seisan Consulting for their hard work and dedication on this project. The team led by Chuck Durham has delivered again.

SCORING ENGINE: MAP VIEW

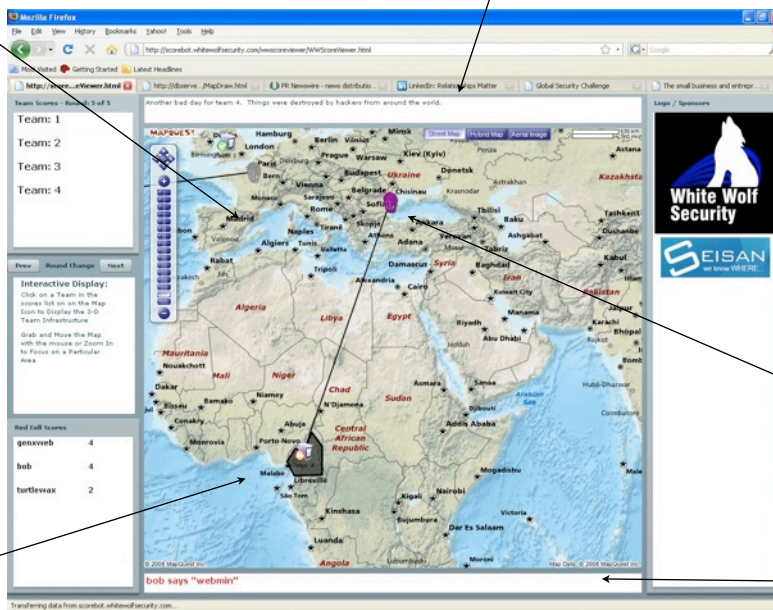
Top news ticker populated as necessary. Can be used to provide 'story' type data about a specific team in real time.

GIS driven scoring engine allows for attackers and defenders to be placed in real world locations.

Defender Teams' scores, ranked by standing.

Attacker ranking. Number indicates total systems compromised.

Dark area shows regional outage of phone service as a result of hackers shutting down the PBX server



Space for sponsor/event logos

Skull (attacker) and line drawn to defending team in Africa shows that the team was compromised during the last scoring round. See above for zoom in.

Bottom news ticker populated by Red Cell as a result of the phone home script



THE VALUE

Team Infrastructure	Business Injects	Inject Status	Scores
Refresh Scores			
Team 1	Team 2	Team 3	Team 4
1300	2270	2360	4910

For Players

Everything we deploy in our exercises is real. Real IP addresses, real infrastructure and real systems. Where ever possible, databases and user tables are populated. We've deployed e-Commerce systems with over 10,000 customers and Active Directory servers with 12,000 employees. This data rich environment not only gives the teams real data to protect and attack, it also provides a powerful context for scenarios. With all this data to protect, our exercises can test technical offensive, defensive and even forensic and investigative skills.

For Teams and Organizations

The complex and distributed exercise environment allows customers to test their team dynamic under stress. With the high realism factor, participants can test incident response plans, communication trees, crisis mitigation and even team leadership. White Wolf Security cyber exercises make great team and leadership building experiences.

For Technology Vendors

Vendors of information security products and services can use our exercises to demonstrate their tools in a live and safe environment. With the diversity of the infrastructure, we can place almost any security product into place and show how it performs under fire. Furthermore, we can

hide which networks are unprotected from those that are secured to provide a blind attack field for the Red Cell. Both networks will be scored through the scoring engine. This results in a hard numerical score for each network. This allows vendors and potential customers to viscerally demonstrate the efficacy of their products in a way unlike any other marketing event.

For Colleges and Universities

White Wolf Security has the tools and experience to design and host your own college competition. We have a complete turnkey solution to a complete cyber exercise. Packages are highly customizable and available in one, two and three day engagements. Educational institutions can also use their own equipment and license our Scoring Engine.

For Special Interest Groups

White Wolf Security collects a staggering amount of data from each cyber exercise. This data includes:

1. Network diagrams
2. Start/finish OS version and service pack
3. Start/finish network service version
4. Date/time stamp of successful intrusions
5. Central IDS log of all defending teams
6. Central full packet captures of all traffic to/from defending teams.

This data is available to groups who wish to provide members with access to real world network attack/defend traffic and statistics.

Calendar

August, 2008

Private exercise for US DoD

September, 2008

Start robotics testing

September, 2008

Tim Rosenberg to present and moderate technology panel at Proteus Management Group

October 1 - 3, 2008

SANS/ICE II, Caesar's Palace, Las Vegas, NV. Open to all SANS attendees

December, 2008

Tim Rosenberg to chair Safety and Security track at ITRevolutions

Partners

THE FOLLOWING HAVE PROVIDED SERVICES AND/OR FUNDING TO HELP BETTER OUR EXERCISES.



If you are interested in partnering, please contact Joe Decree at 717-295-6201 or joe@whitewolfsecurity.com



Flexible framework, dynamic delivery



The White Wolf Security Cyber Exercise framework is entirely customizable to your organization's needs. Exercises can be simple and quick or complex and multi dimensional. We have the skills and experience to deliver an engagement that

focuses on the needs and requirements of your organization.

Come join us for ICE II; the second annual Integrated Cyber Exercise hosted this year at SANS Las Vegas. We are running a complex cyber exercise for three nights; October 1 - 3 at Caesar's Palace, Las Vegas, Nevada. The event is open to all registered SANS attendees. White Wolf Security has a limited amount of invites that we may extend to those who wish to observe without attending the SANS conference. Call today if you are interested.



Contact Information

Web:

www.whitewolfsecurity.com

Phone:

717-295-6201 (o)

717-295-6202 (o)

717-295-6205 (f)

Email:

Tim Rosenberg

tim@whitewolfsecurity.com

Joe DeCree

joe@whitewolfsecurity.com

Blog:

whitewolfsecurity.typepad.com