

Adversarial Offensive Training (AOT)

Learn to exploit and explore remote networks using Immunity's CANVAS!

Adversarial Offensive Training

AOT teaches the essentials of remote network exploitation by demonstrating the offensive methodology in a coherent framework. You'll learn how to analyze remote networks, what the domain controller does, how to find credentials, as well as how to expand access across a network, and much more!

This course is for people who love network and computer security, programmers, and people who are responsible for protecting their organizations' networks from threats. This course gives you an in-depth look at the essentials of remote network exploitation, from scanning and enumeration of a network space to performing client-side attacks, which are quickly becoming the most reliable vector into target networks.

NOTE

In this class you will use real exploits against simulated targets. For example, you will perform spear-phishing attacks against email addresses found in your scenario, and your remote target computers will check their email and open your exploit attachments and links sent.

All exploits are performed in a realistic network with routing, public IP addresses and domain names. But don't worry! Our network is safely sandboxed to prevent any accidents. Parrot Labs provides a secure environment where you can learn and practice new skills without worrying about inadvertently



INFORMATION GATHERING

Introduction to the Offensive Methodology, Information Gathering using open source tools



SCANNING & ENUMERATION

Network scanning using [nmap](#) and Immunity CANVAS scans. You will also use [BeEF](#), to scan and enumerate remote web browsers.

GAINING ACCESS

Learn how to send exploits using [Immunity CANVAS](#), advanced tunneling using SSH, CANVAS bouncing, and netcat tunnels. You will also perform manual Cross Site Scripting and SQL Injection.

You will then compile and deploy actual malware to set up a small botnet using client side exploits.



EXPANDING ACCESS

In this phase, you will learn in depth about the Windows Registry, Offensive Digital Forensics, How to find files of interest, Windows Active Directory queries, How to crack passwords, and Linux backdoors using a covert Dropbear SSH Server.

SUSTAINING ACCESS

In this phase, you will learn about stealing credentials to gain access to routers, how to crack Cisco passwords, Routing and Network Infrastructure, and Antivirus Evasion techniques

CAPSTONE

The capstone is a full day that uses all of the skills learned in the previous two weeks. Students are given a target domain name, and they will be able to scan the DMZ for servers, mine for email addresses, use server-side and client-side exploits, all to gain access to a remote network. Once inside, you will find a large network and practice tunneling and pivoting to get to the data.

Course Details

LOCATION

FACILITIES

PROVIDED EQUIPMENT

COST

7740 Milestone Parkway, Suite 500

Hanover, MD 21076

[Get Directions to visit](#)



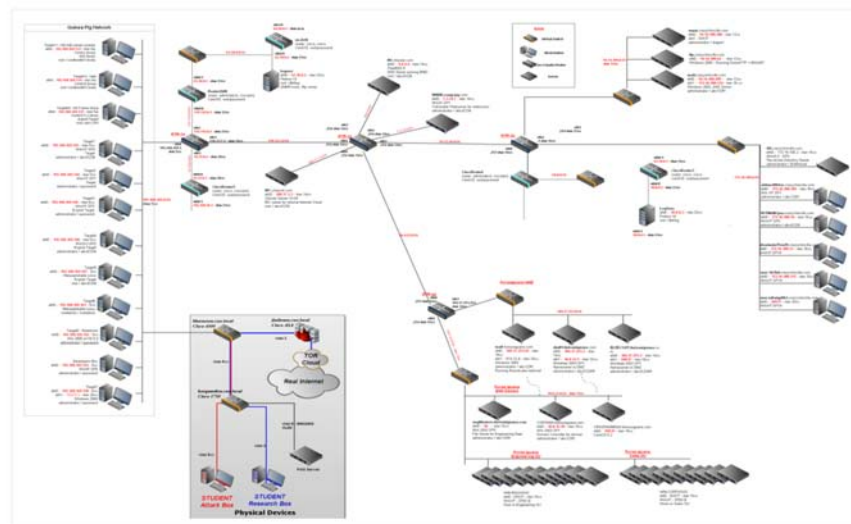
Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified borders.

— Ronald Reagan

What is this course all about?

This class is designed to teach you the full process than an external threat may use to attack your network

What makes this course unique?



We have a large, realistic network for each student.

Each student performs all of their exercises in a sandboxed

network. This means that everyone has the same IP addresses, but different computers, so if your fellow student crashes their web server (it happens often), your copy of that web server is fine.

Each individual network has 5 routers, domain controllers, functioning root DNS server, DMZs to find and scan, and internal networks that are live and active.

This is the best way to learn exploitation with a detailed lab!

Email us for details!

OUR STORY

Parrot Labs is the cybertraining wing of KEYW Corporation. We are here to make sure you get the most realistic and relevant cybertraining available.

CONTACT US

Parrot Labs, KEYW Corporation
7740 Milestone Parkway, Suite 500
Hanover, MD 21076
Phone: (443) 733-1600
Email: cybertraining@keywcorp.com

COURSE INFO

[Course Schedule](#)
[Class Offerings](#)
[FAQ](#)

DETAILS

[Location](#)
[About Us](#)
[We are Hiring!](#)

Offensive Methodology & Analysis (OMA)

Learn to exploit and expand access into remote networks using open source tools!

**Use real client
side-exploits against web
browsers**

**Deploy and control a
botnet**

**Learn how to tunnel and
pivot deep into a network**

Offensive Methodology & Analysis

OMA is a course that teaches the essentials of remote network exploitation by demonstrating the offensive methodologies in a coherent framework. You'll learn how to analyze remote networks, what the domain controller does, how to find credentials, as well as how to expand access across a network, and much more!.



This course is for people who love network and computer security, programmers, and people who are responsible for protecting their organizations' networks from threats. This course gives you an in-depth look at the essentials of remote network exploitation, from scanning and enumeration of a network space,

down to performing client-side attacks, which are quickly becoming the most reliable vector into target networks.

NOTE

In this class you will use real exploits against simulated targets. For example, you will perform spear-phishing attacks against email addresses found in your scenario. Our remote



INFORMATION GATHERING

Introduction to the Offensive Methodology and Information Gathering using open source tools.



SCANNING & ENUMERATION

Learn to scan networks and servers using [nmap](#), Analyze network packets (at a low level), and use simple python scripts to scan and enumerate remote web browsers.

GAINING ACCESS

Learn to send exploits using [the Metasploit Framework \(MSF\)](#), advanced tunneling using custom tunneling executables, Metasploit pivoting, and SOCKS proxy tunnels. Also perform manual Cross Site Scripting (XSS) and SQL Injection.

Compile and deploy actual

target computers will check their email and open your exploit attachments and links sent.

All exploits are performed in a realistic network with routing, public IP addresses and domain names. But don't worry! Our network is safely sandboxed to prevent any accidents. Parrot Labs provides a secure environment where you can learn and practice new skills without worrying about inadvertently crashing the Internet.

malware to set up a small botnet using client-side exploits.

EXPANDING ACCESS

In this phase, you will learn in-depth about the Windows Registry, Offensive Digital Forensics, and Windows Active Directory queries. Learn to find files of interest, how to crack passwords, and use the pass-the-hash technique to maneuver around a remote Windows network.

Course Details

LOCATION

FACILITIES

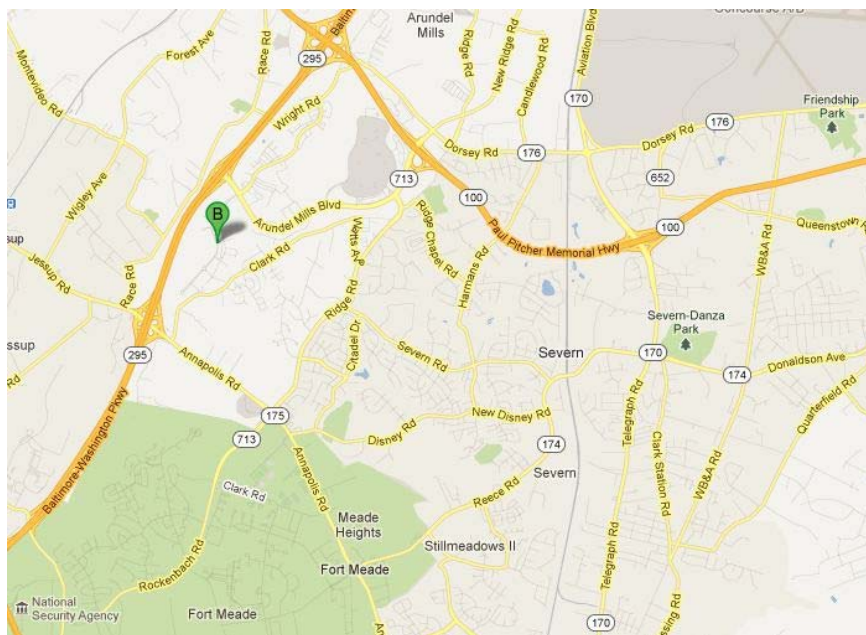
PROVIDED EQUIPMENT

COST

7740 Milestone Parkway, Suite 500

Hanover, MD 21076

[Get directions to visit](#)



SUSTAINING ACCESS

Learn how to steal credentials to gain access to routers, and to crack Cisco passwords. Also review routing and network infrastructures, and antivirus evasion techniques.

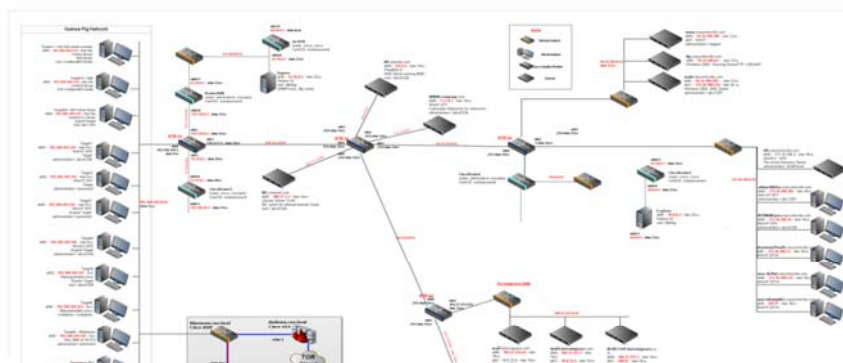
CAPSTONE

The capstone is a full day that uses all of the skills learned in the previous two weeks. Students are given a target domain name, and they will be able to scan the DMZ for servers, mine for email addresses, use server-side and client-side exploits, all to gain access to a remote network. Once inside, you will find a large network and practice tunneling and pivoting to get to the data.

Q: How many of the Fortune 500 are compromised? A: 500.

— Mikko Hypponen

What makes this course unique?





hands-on training on a variety of tools for gaining access to a remote network.

Parrot Labs creates a large scale, realistic network for each student. Each individual network has five routers, functioning domain controllers, a functioning root DNS server, multiple domains with DMZs to find and scan, and internal networks that are live and active.

You'll perform all of your exercises and scenarios in a sandboxed network. Each student has the same set of IP addresses, but different computers. So if a fellow student crashes their copy of a web server (it happens!), you can continue to work on your copy of the web-server without interruption.

We love this material and you will too!

Email us for details!

OUR STORY

Parrot Labs is the cybertraining wing of KEYW Corporation. We are here to make sure you get the most realistic and relevant cybertraining available.

CONTACT US

Parrot Labs, KEYW Corporation
 7740 Milestone Parkway, Suite 500
 Hanover, MD 21076
 Phone: (443) 733-1600
 Email: cybertraining@keywcorp.com

COURSE INFO

Course Schedule
 Class Offerings
 FAQ

DETAILS

Location
 About Us
We are Hiring!