

# Deploy and Secure an Internet Facing Application with the Barracuda Web Application Firewall in Amazon Web Services

#### https://campus.barracuda.com/doc/70586316/

In this lab, you will deploy an unsecure web application into Amazon Web Services (AWS), and then secure the application using the Barracuda Web Application Firewall. To create the environment, you will deploy a Virtual Private Cloud, Internet Gateway and NAT Gateway to provide for the virtual networking. Then a Barracuda Web Application Firewall and an Ubuntu server with Apache, PHP, MySQL and the Damn Vulnerable Web Application (DVWA), installed.

DVWA is a PHP/MySQL web application that is vulnerable attack. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment. More information can be found on the DVWA <u>site</u>.

Once this infrastructure is built you create an Elastic Load Balancer in AWS that will direct traffic from the Internet to the Barracuda Web Application Firewall (both management and web). Next you will configure a Barracuda Web Application Firewall (WAF) to provide the service of the Damn Vulnerable Web Application (DVWA). After this is created you will connect to the DVWA web application and run the attacks to see how they are logged in the Barracuda Web Application Firewall.

These detailed step-by-step instructions will guide you through the lab.

## Scenarios

- Deploy and configure an AWS Virtual Private Cloud.
- Provision and configure the Barracuda Web Application Firewall.
- Deploy and configure the DVWA application.
- Simulate attacks on the site using the DVWA application and capture the attacks being launched, configure policies and run reports from the WAF.

## Requirements

- Amazon Web Services subscription
- Valid contact details to complete the Barracuda Web Application Firewall trial registration

The following is a diagram of the deployment that will be completed at the end of this hands-on lab.





## **Exercise 1: Environment Setup**

In this exercise, you will use an AWS Console to implement the infrastructure that will be leveraged for the rest of the exercises. This includes creating the Virtual Private Cloud (VPC), provisioning the Barracuda Web Application Firewall, the Elastic Load Balancer (ELB), and the Ubuntu server which will host the DVWA application.

#### Task 1: Create the Networking Infrastructure using an AWS Console

- 1. Go to the AWS portal <u>https://console.aws.amazon.com/</u>. After entering your credentials, the AWS Dashboard will display.
- 2. Click through **Console > Networking & Content Delivery > VPC**.



3. Next, click **Start VPC Wizard**.





- 5. Complete the **Step 2: VPC with a Single Public Subnet** screen using the following details and then click **Create VPC**.
  - **IPv4 CIDR block** 10.0.0.0/16
  - **VPC name** BarracudaWAFLab
  - Availability Zone us-east-1a
  - Subnet name www



	🧵 Services 🗸 Res	ource Group	s v '	*				
	Step 2: VPC with a Sir	ngle Public	Subn	et				
	IPv4 CIDR block:*	10.0.0/16		(65531 IP ad	dresses a	available)		
	IPv6 CIDR block:	No IPv6 CI	DR Block					
		Amazon pr	ovided IP	v6 CIDR block				
	VPC name:	BarracudaW	AFLab					
	Public subnet's IPv4 CIDR:*	10.0.0/24		(251 IP addre	esses ava	ailable)		
	Availability Zone:*	us-east-1a	٣					
	Subnet name:	www						
		You can add r	nore subr	ets after AWS creat	es the VF	PC.		
	Service endpoints							
		Add Endpo	pint					
	Enable DNS hostnames:*	● Yes ○ No						
	Hardware tenancy:*	Default	¥					
6.	Next, click <b>Subnets</b> and re	view the sul	bnet tha	at was created b	by the v	wizard.		
	VPC Dashboard Filter by VPC: None	•						
	Virtual Private Clo	ud						
	Your VPCs							
	Subnets							
	Route Tables							
	Name * Subnet	ID - Sta	ate - \	/PC	Ŧ	IPv4 CIDR	Ŧ	Available IPv4 /-
	www subnet-f	21d3ea9 av	ailable v	pc-15b6f673   Barracuda	aWAFLab	10.0.0/24		251

7. Right click on the subnet, and then click **Modify auto-assign IP settings**. The **Modify auto-assign IP settings** screen opens.



Cancel

Save

	Name	<ul> <li>Subnet ID</li> </ul>	✓ State ✓ VPC	~	
	www Right- Click	subnet-281436	72 Delete Subnet Edit IPv6 CIDRs Create Flow Log Modify auto-assign IP setti	BarracudaWAFLab	
8.	Check the box for <b>En</b> a	able auto-assigr	<b>1 public IPv4 address</b> an	d then click <b>Save</b> .	
	Modify auto-ass	ign IP setting	S	1	×
	Enable auto-assign pub launched into this subn	olic IPv4 or IPv6 addr net.	resses to automatically reques	an IP address for instances	
	Auto-assig	gn IPs 💽 Enable at	uto-assign public IPv4 address	0	

Note: You can override the auto-assign IP settings for each individual instance at launch time for IPv4 or IPv6. Regardless of how you've configured the auto-assign public IP feature, you can assign a public IP address to an instance that has a single, new network interface with a device index of eth0.

9. From the Subnet screen, click Create Subnet to create a new subnet.

Create Subnet

- 10. Complete the **Create Subnet** screen using the following details, then click **Yes Create**:
  - Name tag apps
  - Availability Zone us-east-1a
  - **IPv4 CIDR block** 10.0.1.0/24

Create Subnet					×
Use the CIDR format to spec and /28 netmask. Also, note	cify your subnet's IP addr that a subnet can be the	ress block (e.g., 10.0.0.0/24). same size as your VPC. An I	Note that block sizes must Pv6 CIDR block must be a	be between a /16 n /64 CIDR block.	etmask
Name tag	apps		9		
VPC	vpc-15b6f673   Barrad	cudaWAFLab 🔹 🚯			
VPC CIDRs	CIDR	Status	Status Reason		
	10.0.0/16	associated			
Availability Zone IPv4 CIDR block	us-east-1a	(	9		
				Cancel Yes, C	Create



- 11. On the **Subnets** page, review both the **www** and **apps** subnets.
- 12. From the **VPC Dashboard**, click **Internet Gateways** and review how this was created by the wizard. Make sure that the **State** shows **attached**.

T Services v I			
VPC Dashboard Filter by VPC: None			
Virtual Private Cloud			
Your VPCs			
Subnets			
Route Tables			
Internet Gateways			
Egress Only Internet Gateways			
Name	↑ ID	- State -	VPC -
	igw-47f8fc20	attached	vpc-15b6f673   BarracudaWAFLab

13. Next, click **Route Tables** to review how the routing has been configured.



14. Notice that the **www** subnet has been configured to associate the Internet bound route 0.0.0.0/0 to the **Internet Gateway**.



Summary	Routes	Subnet Associations	Rou	ite Propag	ation	Tage
Edit	View:	All rules v				
Destination		Target		Status	Propag	gated
10.0.0/16		local		Active	No	
0.0.0/0	<u> </u>	igw-47f8fc20		Active	No	

15. From the AWS console, click **VPC** under the **Networking and Content Delivery**, then click **NAT Gateways**.

VPC Dashboard
Filter by VPC: None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways

16. Click Create a NAT Gateway.



You do not have any NAT gateways in this region.							
Choose the Create	NAT gateway button to create your first NAT gateway.						
	Create a NAT Gateway						

The Create a NAT Gateway window opens.

	Create a NAT Gatew	ау		×
	Create a NAT gateway and assig	n it an Elastic IP address. Learn more		
	Subnet*	Search subnets by ID or name or VPC e	g. "subnet-1a2b3c	
	Elastic IP Allocation ID*	Subnet	VPC	
		subnet-28143673   www	vpc-7b01431d   Ba	rracudaWAFLab
		subnet-ea1537b1   apps	vpc-7b01431d   Ba	arracudaWAFLab
.8.	Once this is complet	ed click Create a NAT G	ateway.	
	Create a NAT Gatewa	У		×
	Create a NAT gateway and assign	it an Elastic IP address. Learn more		
	Subnet*	subnet-28143673	0	
	Elastic IP Allocation ID*	eipalloc-5e80366f	Create New EIP	0
		New EIP (34.206.113.110) creation succes	sful.	
			Cancel Create a NA	T Gateway
	Create a NAT Gatew	ау		
	<ul> <li>Your NAT gatew Note: In order to use 09302ee9c47d9a5b Find out more.</li> </ul>	ay has been created. your NAT gateway, ensure that you edit you	our route tables to include a route with a tar	rget of <b>'nat-</b>

19. Next, click **Route Tables** to review how the routing has been configured.



🧊 Services 🗸
VPC Dashboard
Filter by VPC: None
Virtual Private Cloud
Your VPCs Subnets
Route Tables
Internet Gateways

- 20. Locate the second route table that was created, but currently has 0 subnets associated.
- 21. Click this **Route Table** and select **Routes**. Notice how currently this is only a route for local traffic in the CIDR range of 10.0.0.0/16. This means there is no route to the Internet.

Name	▲ Route 1	Table ID 🗸	Explicitly A	Associat -	Main	VPC		
	rtb-43d2	2463a	1 Subnet		No	vpc-15b	6f673   Barr	acudaWAFL
	rtb-41d2	24638	0 Subnets		Yes	vpc-15b	6f673   Barr	acudaWAFL
b-41d24638								
5-41d24638 Summary	Routes	Subnet As	ssociations	Route P	ropagatio	n	Tags	
5-41d24638 Summary Edit	Routes View:	Subnet As All rules	ssociations	Route P	ropagatic	n	Tags	
b-41d24638 Summary Edit Destination	Routes View:	Subnet As All rules Target	ssociations	Route P	ropagatio	n opagated	Tags	

- 22. Click **Edit**, to make changes to the route table:
  - 1. Click Add Another Route.
  - 2. As the **Destination**, select **0.0.0.0**/0.
  - 3. As the **Target**, select the NAT gateway.
  - 4. Click Save.



	rtb-41d24638							
	Summary	Routes	Subnet Association	ns Rou	ite Propag	gation	Та	igs
	Cancel Save	View:	All rules					
	Destination		Target		Status	Propag	ated	Remove
	10.0.0/16		local		Active	No		
	0.0.0.0/0		nat-09302ee9c47d9	a5b4		No		0
	Summary Edit	Routes	Subnet Associatio	ns				
	Edit							
	Subnet	IPv4 CIDR	IPv6 CIDR					
	You do not have ar The following subne associated with any rou associated	iy subnet asso its have not be te tables and a l with the main	ciations. en explicitly ire therefore route table:					
	Subnet	IPv4 CIDR	IPv6 CIDR					
	subnet-ea1537b1   apps	10.0.1.0/24	-					
24.	Now, check the box	for the <b>ap</b>	<b>ps</b> subnet to ass	sociate tl	nis rout	e table	with t	he <b>ap</b>
	Summary	Routes	Subnet Ass	sociations	Ro	ute Prop	pagatio	n

	Summary		Routes	Subnet Associations		Route Propagation
	Cancel	Save				
	Associate	Subnet		IPv4 CIDR	IPv6 CIDR	Current Route Table
(		subnet-2	8143673   www	10.0.0/24	-	rtb-204fd859
	•	subnet-e	a1537b1   apps	10.0.1.0/24	-	Main

Now the private servers on the **apps** subnet will use the NAT gateway for their Internet bound traffic.

#### Task 2: Provision the Barracuda WAF using the AWS Marketplace

- 1. Sign-in to the AWS Console.
- 2. On the right-hand side of the console under AWS Marketplace, click the Learn more link.



3. In the AWS Marketplace search box, type Barracuda Web Application Firewall and



then click on	the magnifying glass.
<b>aws</b> marketpl	ace AMI & Saa5 - barracuda web application firewall
. Several Barra Web Applica	icuda Networks products will be returned by this search. Choose the <b>Barracu ation Firewall (WAF) - PAYG</b> .
barracuda web	application firewall (4 results) showing 1 - 4
Free Trial Product Support Connection	Barracuda Web Application Firewall (WAF) - PAYG ★★★★★ (0) Version 8.1.1.014-20170109   Sold by Barracuda Networks, Inc. Starting from \$1.038/hr or from \$7,999.00/yr (12% savings) for software + AWS usage fees Many AWS-hosted applications choose Barracuda, an AWS Preferred Security Competency Partner, due to its continuous monitoring and policy tuning by world-class security experts Linux/Unix, Other 3.4.11 - 64-bit Amazon Machine Image (AMI)
Barracuda Product Support Connection	Barracuda Web Application Firewall (WAF) - BYOL
. Once the WA	F page loads, click <b>Continue</b> .
Barracuda	Barracuda Web Application Firewall (WAF) - PAYG Sold by: Barracuda Networks, Inc. I See product video C Product Support Connection 30 Day Free Trial Available - Many AWS-hosted applications choose Barracuda, an AWS Preferred Security Competency Partner, due to its continuous monitoring and policy tuning by world-class security experts. Barracuda's dynamic profiling and application- aware technologies minimize false positives and protect against emerging threats. Working seamlessly with your AWS environment, the Barracuda Web Application Firewall's unmatched security capabilities, customization options and reporting analytics are used by the world's most security-conscious businesses, including financial institutions, government agencies, and trading platforms. The built-in Barracuda Wuherability Remediation Service automates vulnerability scanning and remediation, simplifies ongoing maintenance and accelerates development cycles making the Barracuda WAF the ideal app security solution for Devops environments. The Barracuda WAF monitors all inbound web traffic to detect and block threats arising from all types of attacks against your web applications, and guards against data loss by inspecting the HTTP responses from your back-end servers. The integrated access control engine enables administrators to create granular access control policies for Authentication, Authorization & Accounting (AAA), giving organizations strong authentication and user control. The Barracuda Web Application Firewall on AWS also features the ability to use CloudFormation templates for autoscaling, allowing you to automatically bootstrap and cluster additional instances as needed, for higher throughput and easy deployment. Free Scan: Follow the link https://bwm.barracudanetworks.com/appscan_signup C Read more
Customer Rati	ing ★★★★★ € (0 Customer Reviews) ion 8.1.1.014-20170109 (Other available versions)

- Type 1-Click Launch
- $\circ\,$  Software Pricing Hourly / m3. medium



v

1-Click Launch	Manual Launch	
Review, modify and launch	With EC2 Console, API or CLI	
Click "Accept Soft launch this softwa Once you accept the term in any supported region. directly from the EC2 con	ware Terms & Launch ware with the settings be are with the settings be s, you will have access to launch For future launches, you can retu sole, APIs or CLI.	with 1-Click" to elow any version of this software irm to this page or launch
➡ Software Pricin	ıg	
Subscription Term	Applicable Instance Type	Hourly fee \$1.04 / hour Find instance details in EC2 instance section below.
Region - US East ( EC2 Instance Type	(N. Virginia) e – m3.medium	
VPC Settings - Sel	ect the VPC and www	subnet (10.0.0.0/24).
▼ VPC Setting	s	
Select a VPC:		
vpc-15b6f673	(10.0.0/16)	
Or Create a VPC 🕻		
Select a subnet:		
subnet-f21d3ea	a9 (10.0.0.0/24)	
Security Group - <sup>c</sup>	Select Create new ba	ased on seller settings





• Key Pair - Select or Create a New Key

7. After verifying the selections, click Launch with 1-click.



8. Next on the AWS Marketplace Product Support Connection screen, click Share your contact details.



You can register for support.	with this coffware's worder by disking the h	utten beleur urbich will
rou can register for support	with this software's vendor by clicking the b	outton below, which will
open a new browser tab. Sha	ring your contact details is not required, bu	t offering this
information to the vendor wi	ll make it easier for you to obtain support f	or this product.
We recommend you enter thi	s information now, but you can do so from	the right column of this
page or the Your Software pa	age at any time.	
	Share your contact de	tails Skip this step
anan lata tha Dawa and	Notworks Support Form and die	k Register & Close
omplete the <b>Barracuda</b>	<b>I Nelworks Subborl Form</b> and Chi	
add contact 1 of 5 for Barr	acuda Web Application Firewall (WAF)	- PAYG
Add contact 1 of 5 for Barr	acuda Web Application Firewall (WAF)	- PAYG
Add contact 1 of 5 for Barr	acuda Web Application Firewall (WAF)	PAYG you are not required to register a
Add contact 1 of 5 for Barr Add contact 1 of 5 for Barr Mease list the contact details for a person you ontact for support, if you choose to do so ver	a wetworks Support Form and che acuda Web Application Firewall (WAF) would like to have as a support contact for this subscription. While dors will need the information in the fields marked with an asterisk	PAYG     you are not required to register a
Add contact 1 of 5 for Barr Please list the contact details for a person you contact for support, if you choose to do so ver	would like to have as a support contact for this subscription. While dors will need the information in the fields marked with an asterisk.	PAYG     you are not required to register a
Add contact 1 of 5 for Barr Please list the contact details for a person you contact for support, if you choose to do so ver First Name *	a Network's Support Form and Check acuda Web Application Firewall (WAF) would like to have as a support contact for this subscription. While dors will need the information in the fields marked with an asterisk Last Name *	PAYG you are not required to register a
Add contact 1 of 5 for Barr Please list the contact details for a person you contact for support, if you choose to do so ver First Name *	a Network's Support Form and Check acuda Web Application Firewall (WAF) would like to have as a support contact for this subscription. While dors will need the information in the fields marked with an asterisk Last Name *	- PAYG you are not required to register a
Add contact 1 of 5 for Barr Add contact 1 of 5 for Barr Nease list the contact details for a person you ontact for support, if you choose to do so ver irist Name *	A Network's Support Form and Check acuda Web Application Firewall (WAF)      would like to have as a support contact for this subscription. While     dors will need the information in the fields marked with an asterisk     Last Name *     Organization *     Phone *	- PAYG you are not required to register a
Add contact 1 of 5 for Barr Add contact 1 of 5 for Barr fease list the contact details for a person you ontact for support, if you choose to do so ver irst Name * ob Title mail *	A Network's Support Form and Check acuda Web Application Firewall (WAF)      would like to have as a support contact for this subscription. While     dors will need the information in the fields marked with an asterisk     Last Name *     Organization *     Phone *	- PAYG you are not required to register a
Add contact 1 of 5 for Barr Add contact 1 of 5 for Barr lease list the contact details for a person you ontact for support, if you choose to do so ver lirst Name * ob Title mail *	A Network's Support Form and Check acuda Web Application Firewall (WAF) would like to have as a support contact for this subscription. While dors will need the information in the fields marked with an asterisk      Last Name *      Organization *      Phone *      Country	PAYG  you are not required to register a
Add contact 1 of 5 for Barr Add contact 1 of 5 for Barr lease list the contact details for a person you ontact for support, if you choose to do so ver irst Name * ob Title imail * ip Code	A Network's Support Form and Check acuda Web Application Firewall (WAF)      would like to have as a support contact for this subscription. While     dors will need the information in the fields marked with an asterisk     Last Name *     Organization *     Phone *     Country     inting permission to share the contact information listed above with	PAYG  you are not required to register a  Barracuda Networks, Inc.
Add contact 1 of 5 for Barr Add contact 1 of 5 for Barr Please list the contact details for a person you ontact for support, if you choose to do so ver irrst Name * lob Title imail * ip Code I agree that by submitting this form I am gra- lick Here to learn more about how Amazon p	A Network's Support Form and Cite acuda Web Application Firewall (WAF)      would like to have as a support contact for this subscription. While adors will need the information in the fields marked with an asterisk      Last Name *      Organization *      Phone *      Country      inting permission to share the contact information listed above with rocesses the provided information and how it can be shared with v	PAYG     you are not required to register a
Add contact 1 of 5 for Barr Add contact 1 of 5 for Barr "lease list the contact details for a person you ontact for support, if you choose to do so ver "irst Name * lob Title imail * ip Code I agree that by submitting this form I am gra lick Here to learn more about how Amazon p	A Network's Support Form and Cite acuda Web Application Firewall (WAF) would like to have as a support contact for this subscription. While adors will need the information in the fields marked with an asterisk Last Name * Organization * Phone * Country anting permission to share the contact information listed above with rocesses the provided information and how it can be shared with v	PAYG  you are not required to register a  Barracuda Networks, Inc. endors for product support purposes.

<ul> <li>Thank you for su An instance of this software You can check the status of t Software and AWS hourly us</li> </ul>	bscribing to Barracuda Web Application Firew will be deployed on EC2 soon after your subscription completes. his instance on EC2 Console. You can also view all instances on Your Software pa age fees apply when the instance is running and will appear on your monthly bill	all (WAF) - PAYG 9º.
Next Steps: You will receive an email once you Once you are subscribed, an ins The software will be ready in a	your subscription completes. stance of this software will be deployed on EC2. few minutes.	AWS Marketplace Product Support Connection You can register for support with software vendors by providing contact information.
Software Installation D Product Version	etails Barracuda Web Application Firewall (WAF) - PAYG 8.1.1.014-20170109	Sharing your contact details is not required, but offering this information to the vendor will make it easier for you to obtain support for this product. We recommend you enter this information now, but you can do so from the Your
Region EC2 Instance Type	us-east-1 m3.medium	Software page at any time. Share your contact details Related Links
VPC Subnet	vpc-26357040 subnet-4134131a Create new security group based on seller settions	AWS Management Console Your Software Continue shopping on AWS Marketplace
Key Pair	AWSKEY	Service Catalog Click here for instructions to deploy Marketplace products in AWS Service Catalog.

11. Click on the EC2 Console link in the green message about the deployment of the Barracuda



Web Application Firewall. Once it is deployed the instance will show it is **Running**.



Don't continue on to the next step until the Barracuda WAF instance is in the running state as in the screen shot above.

#### Task 3: Provision the Elastic Load Balancer

1. In the AWS Console, click on Load Balancers.



2. Select Create Load Balancer.



3. Select the **Classic Load Balancer** as the type of Elastic Load Balancer, and click **Continue**.



- 4. In **Step 1: Define Load Balancer**, complete the screen using these inputs.
  - Load Balancer Name BarracudaWAF-ELB
  - **Create LB Inside** Select the VPC that you created for this lab.
  - **Subnet** Select the **www** subnet.



Lis	stener Configura	tion:				
Load Balancer	Protocol	Load Balancer Po	rt Instance Pr	rotocol	Instance Port	
HTTP	•	80	HTTP	٣	80	
HTTP		8000	HTTP	٣	8000	
You will need to a please select at li	eelect a Subnet for east two Subnets 40 (10.0.0.0/16)	r each Availability Zone when in different Availability Zones BarracudaWAFLab	re you wish traffic to be routed by s to provide higher availability for	your load balancer. If y your load balancer.	ou have instances in only one Ava	ailabi
You will need to splease select at l VPC vpc-263570 Please select	elect a Subnet for east two Subnets 40 (10.0.0/16)   t at least two Sub	r each Availability Zone when in different Availability Zones BarracudaWAFLab nets in different Availability Z	re you wish traffic to be routed by s to provide higher availability for cones to provide higher availability	your load balancer. If y your load balancer.	ou have instances in only one Ava	ailabil
You will need to s please select at l VPC vpc-263570 Please selec Available subne	tat least two Subret tat least two Subrets	r each Availability Zone when in different Availability Zones BarracudaWAFLab nets in different Availability Z	re you wish traffic to be routed by s to provide higher availability for cones to provide higher availability	your load balancer. If y your load balancer.	ou have instances in only one Ava	ailabil
You will need to s please select at l VPC vpc-263570 Please select Available subne Actions	tat least two Subret tat least two Subrets	r each Availability Zone when in different Availability Zones BarracudaWAFLab nets in different Availability Z Availability Zone	re you wish traffic to be routed by s to provide higher availability for cones to provide higher availability Subnet ID	your load balancer. If y your load balancer. If for your load balancer for your load balancer Subnet CIDR	ou have instances in only one Ava	3
You will need to s please select at i VPC vpc-263570 Please select Available subnet Actions Selected subnet	select a Subnet for east two Subnets 40 (10.0.0.0/16) [ t at least two Subn ts	r each Availability Zone when in different Availability Zones BarracudaWAFLab nets in different Availability Z Availability Zone	re you wish traffic to be routed by s to provide higher availability for cones to provide higher availability Subnet ID	your load balancer. If y your load balancer. for your load balancer Subnet CIDR	ou have instances in only one Ava	ailab
You will need to s please select at l VPC vpc-263570 Please select Available subne Actions Selected subnet Actions	t at least two Subrets t at least two Subrets t at least two Subrets	r each Availability Zone when in different Availability Zones BarracudaWAFLab nets in different Availability Z Availability Zone Availability Zone	re you wish traffic to be routed by s to provide higher availability for cones to provide higher availability Subnet ID Subnet ID	your load balancer. If y your load balancer. for your load balancer Subnet CIDR	ou have instances in only one Ava	ailabi

5. Click Next: Assign Security Groups.

```
Next: Assign Security Groups
```

6. Deselect the default security group, and select the new **Barracuda Web Application (WAF)** security group that was created by the AWS Marketplace deployment of the device.



Next: Configure Health Check

9. Complete the **Step 4: Configure Health Check** screen, using the following settings:



0	Ping	Protocol -	TCP
---	------	------------	-----

- Ping Port 8000
- Advanced Details Accept defaults.

Step 4: Configure He	alth Check	
Your load balancer will automatically health check, it is automatically remo	perform health checks on your oved from the load balancer. Cu	
Ping Protocol	TCP	
Ping Port	8000	
Advanced Details		
Response Timeout	5 seconds	
Interval (j	30 seconds	
Unhealthy threshold (i)	2 🔻	
Healthy threshold (j)	10 🔻	
LO. Click Next: Add EC2 Instan	ces.	
Next: Add EC2 Instances		
11. On the Step 5: Add EC2 Ins	<b>tances</b> screen, click on t	he instance.
Step 5: Add EC2 Instan	C2 Instances. Check the boxes in th	e Select column to add those instar
VPC vpc-26357040 (10.0.0.0/16)   Barr	acudaWAFLab	
Instance - Name	- State -	Security groups
i-001be783	🥥 running	Barracuda Web Application Firew
12. Click Next: Add Tags.		
Next: Add Tags		

13. Click Review and Create.



14. Review **Step 7: Review** and compare to the ensure that everything is configured properly.



Load Balancer name: BarracudaWAF-E Scheme: internet-facing 80 (HTTP) forwar	ELB
BOOD (HTTP) for	rding to 80 (HTTP) warding to 8000 (HTTP)
<ul> <li>Configure Health Check</li> </ul>	Edit health check
Ping Target: TCP:8000 Timeout: 5 seconds Interval: 30 seconds Unhealthy threshold: 2 Healthy threshold: 10	
<ul> <li>Add EC2 Instances</li> </ul>	Edit instances
Cross-Zone Load Balancing: Enabled Connection Draining: Enabled, 300 sec Instances: I-068104bc019b7	conds 7c6a5
<ul> <li>VPC Information</li> </ul>	Edit subnets
VPC: vpc-26357040 (B Subnets: subnet-4134131a	arracudaWAFLab) a (www)
<ul> <li>Security groups</li> </ul>	Edit security groups
	Cancel Previous Create
, ou should then get a message that t	he BarracudaWAF-ELB was successfully of
oad Balancer Creation Status	

16. In the AWS Console, click the Load Balancers link.



17. On the **BarracudaWAF-ELB** load balancer that you crated, on the **Description** tab, locate the DNS name of the load balancer and copy it to a text file. You will use this to connect to later in the lab.

Close



l oad balancer:	BarracudaW	AF-FI B			000
	Darracudar				
Description	Instances	Health Check	Listeners	Monitoring	Tags
Basic Config	guration				
	Name:	BarracudaWAF-	ELB		
* D	NS name:	BarracudaWAF- 1.elb.amazonaw	ELB-14740277 s.com	'57.us-east-	
Scheme: internet-facing					
Availabil	ity Zones:	subnet-2814367	3 - us-east-1a		
barracudalab	- Notepad				
File Edit Format	View Help				
BarracudaWA	F-ELB-147	4027757.us-0	east-1.elt	.amazonaws	.com

18. Next, click the **Instances** tab. You may notice that the WAF has yet to be put into service by the ELB. Wait until you see that the **Status** change to **InService**. You need to hit the refresh button to see the updates.

Load balancer: BarracudaWAF-ELB			
Description Instances Health Check Listeners	Monitoring Tags		
Connection Draining: Enabled, 300 seconds (Edit)			
Edit Instances			
Instance ID	Name Availability Z	one Status	Instance registration is still in progress.
i-068104bc019b7c6a5	us-east-1a	OutOfService	Remove from Load Bal
Load balancer: BarracudaWAF-ELB Description Instances Health Check	Listeners Monitoring	Tags	
Connection Draining: Enabled, 300 seconds (	Edit)		
Edit Instances			
Instance ID	Name	Availability Zone	Status
i-068104bc019b7c6a5		us-east-1a	V InService (j)

19. Click the **Instance ID** number which will break up details about the BarracudaWAF instance.





- 20. On the **Description** tab, locate the IPv4 Public IP for the WAF and take note of the address.
- 21. Open a new tab on your web browser and point it to **PUBLIC IP address on the management port of 8000**. This will bring you to the home page of the WAF where there will be a licensing agreement displayed.



If the VM has just booted there may be a note that the VM is provisioning. This is normal and takes a few minutes to complete.

22. Scroll down to the bottom of the webpage and click **Accept**.

Accept		
	Barracuda	
	Thank you! You will be redirected shortly as the system is starting up.	
	Please wait while the system starts up	

23. Once the system starts the login page will appear. Once this page has loaded move on to the next step leaving the tab here.

К	arracuda   Web Application Firewall
	Please enter your administrator login and password.
	Password
	Sign in



#### Task 4: Provision Ubuntu Server with the DVWA Application

1. From the AWS console click **Instances**, then click **Launch Instance**.



 Scroll down and select the Ubuntu Server 14.04 LTS (HVM) AMI to deploy as your Web Server for the DVWA.



3. At Step 2: Chose an Instance Type, select t2.small size for the VM. Then click Next: Configure Instance Details.

ter by:	All instance types	* Current	generation 👻	Show/Hide Col	umns			
Current	fly selected: t2.small (Va	riable ECUs, 1 v	PUs, 2.5 GHz, In	tel Xeon Family, 2	GiB memory, EBS only)			
	Family -	Туре –	vCPUs (j) +	Memory (GiB)	Instance Storage (GB) (j) *	EBS-Optimized Available ①	Network Performance (j) *	IPv6 Support
	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
•	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
	General purpose	t2.medium	2	4	EBS only		Low to Moderate	Yes
	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes
	General purpose	m4.4xlarge	16	64	EBS only	Yes	High	Yes

- On Step 3: Configure Instance Details, complete the screen using these details wherever details are not provided leave the defaults, move on to the next step without clicking Next.
  - $\circ~$  Subnet apps
  - $\circ$  Primary IP 10.0.1.50



Step 3: Configure Instan	ce De	etails					
Network	1	vpc-15b6f6	73   BarracudaWAF	FLab	۳	С	Create new VPC
Subnet	1	subnet-94 250 IP Add	Ic3fcf   apps   us-ea resses available	st-12A	۳		Create new subnet
Auto-assign Public IP		Use subne	t setting (Disable)		۳		
IAM role	()	None			۳	C	Create new IAM role
Shutdown behavior	(i)	Stop			٠		
Enable termination protection	(i)	Protect a	against accidental te	ermination			
Monitoring	1	Enable CloudWatch detailed monitoring Additional charges apply.					
Tenancy	()	Shared - R	un a shared hardwa	are instance	۳		
		Additional	charges will apply fo	r dedicated tenancy.			
✓ Network interfaces ①							
Device Network Interface S	Subnet		Primary IP	Second	ary IP	ado	iresses
eth0 New network interface *	subnet-94	1c3fcf ( 🔻	10.0.1.50	Add IP			

- 5. Again, on **Step 3: Configure Instance Details**, scroll down and click the **Advanced Details** tab. Copy this script text into the **User Data** box:
  - o #!/bin/bash
  - wget https://opsgilityweb.blob.core.windows.net/20170304-barracudaw af/dvwa.sh
  - o bash dvwa.sh

Make sure that when pasting from the work document you could get spacing issues. The script is only 3 lines, so check the spacing or the VM won't provision properly.

6. Click Next: Add Storage.



7. On the Step 4: Add Storage screen, accept the defaults and click Next: Add Tags.



8. On the Step 5: Add Tags screen, accept the defaults and click Next: Configure Security Groups.



9. On **Step 6: Configure Security Group**, name it DVWA, click **Add Rule**, and add a rule for **HTTP Port 80**.



existing one bek	ow. Learn more abo	out Amazon EC2 security groups.		a nin o porte, ros canoceare a new second group o seco	
	Assign a secur	rity group: @Create a new security	group		
		Select an existing sec	curity group		
	Security gro De	up name: DVWA scription: This rule is used by t	he Damn Vulnerable Web Application (DVWA	A) http://http://w	
Type (i)		Protocol ()	Port Range 🕕	Source ()	
SSH	٣	TCP	22	Custom • 0.0.0/0	6

#### 10. Click Review and Launch.



#### 11. On Step 7: Review Instance Launch, click Launch.

tep 7: Review I lease review your instance	Instance	Launch You can go b	ack to edit changes for	each section. Click Launch to assi	gn a key pair to your instance and con	nplete the launch process.			
Improve your instances' security. Your security group, DVWA, is open to the world.     Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.     You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups									
Your instance To launch an inst tier eligibility and	e configurati tance that's elig d usage restrict	ion is not e gible for the fre ions.	ligible for the free ( ee usage tier, check you	usage tier r AMI selection, instance type, cont	figuration options, or storage devices.	× Learn more about free usage			
						Don't show me this again			
AMI Details						Edit AMI			
Instance Type	ECUs	VCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Edit instance type			
t2.small	Variable	1	2	EBS only		Low to Moderate			
Security Groups						Edit security groups			
Security group name         DVWA           Description         This rule is used by the Damn Vulnerable Web Application (DVWA) http://http://www.dvwa.co.uk/									
Security group name Description	DVW/ This r	A ule is used by	the Damn Vulnerable V	Veb Application (DVWA) http://http:	//www.dvwa.co.uk/				
Security group name Description Type (j)	DVW/ This n	4 ule is used by Pro	the Damn Vulnerable V	Veb Application (DVWA) http://http: Port Range ①	//www.dvwa.co.uk/	0			

#### 12. Select your AWS key pair, and click Launch Instances.



allow you to con obtain the passy securely SSH in	sts of a <b>public key</b> nect to your instan vord used to log inf to your instance.	y that AWS stores, an ice securely. For Wind to your instance. For	Id a private key file that yo dows AMIs, the private key Linux AMIs, the private key	ou store. Together, the file is required to file allows you to
Note: The select about removing	ed key pair will be existing key pairs	added to the set of k from a public AMI.	eys authorized for this inst	ance. Learn more
Choose an	existing key pair			٣
AWSKEY	/ pair			٣
		and the second second	entuate key file (AMRKEY	

13. After a few minutes (maybe 10), check back on the EC2 Console and now both the WAF and the DVWA server should show as **running**. You can add names to the instances to make it easier to identify the VMs. The T2.small is the DVWA and the M3.Medium is the WAF.

DVWA	i-0069c029edfaf3e82	t2.small	us-east-1a	running	🥝 2/2 checks
BarracudaWAF	i-054e125e897bf1f04	m3.medium	us-east-1a	🥚 running	2/2 checks

#### Summary:

In this exercise, the AWS Console was to implement the infrastructure that will be leveraged for the rest of the exercises. This included creating the Virtual Private Cloud (VPC), provisioning the Barracuda WAF, the Elastic Load Balancer (ELB), and the Ubuntu server.

# Exercise 2: Configure the Barracuda WAF Virtual Appliance and the DVWA Application

In this exercise, the Barracuda WAF Appliance and the DVWA Services will be configured. First the WAF will be configured to connect to the DVWA. Once this is completed then a connection to DVWA server will be made and the configuration will be completed. After this is finished the end to end setup will be complete allowing for simulated attacks in the next exercise.

#### Task 1: Configure the WAF Appliance

- 1. Move back to the tab that contained the login page or if this has been closed open it backup and connect to the WAF.
- 2. Use the following login information:
  - **Username** admin
  - **Password Instance ID** of your Barracuda WAF Instance in Amazon Web Services.



EC2 Dashboard Events	Î.	Launch Instance	Conn WAF	¥
Tags		Q. Filter by tags and	attributes or search by k	lyword
Reports Limits	11	Name -	Instance ID	Insta
INSTANCES		DVWA	i-0059c029edfaf3	t2.sm
Instances		BarracudaWAF	i-054e125e897bf1f04	m3.m
Ar Sensoria Good Innut.      ■           G ← − C <sup>*</sup> Δ   Q Rotecum   b            G → C <sup>*</sup> Δ   Q Rotecum   b	anaadasaf elb-Mi	607797 ha ear tallanaonae com	inn Contrag - matrixeda cap 🔹 🕷 🔮	
G Homesta Gant Hand	ansoutered with white Barracud	a   Web Applic	cation Firewall	
€ C B O Hotener D	Barracud	10079777a est tellansposes.com	cation Firewall	

3. Once logged in, you will be directed to the **Dashboard** page of the Barracuda Web Application Firewall.



- 4. Go to **BASIC > IP Configuration**.
- 5. Review the networking configuration and **take note of the IP address** assigned to the WAF by AWS.

WAN IP Configuration	
IPv4 Address:	10.0.67
	The system IP address, which is assigned to the WAN port on the Barracuda Web Application Firewall. This is a required configuration. Note: During the change of the system IP address the browser may not redirect back to the IP Configuraton page. Please open the Web Interface in a separate browser tab to continue with the configuration.
IPv4 Subnet Mask:	255.255.255.0
IPv4 Default Gateway:	10.0.0.1

6. Update the **Default Host Name** barracudawaf which is the name you gave the VM when you



provisioned in the AWS	Portal.
Domain Configuration	1
Default Host Name:	barracudawaf Used in reports and notifications
Default Domain:	
	The default domain for the system. Example: mydomain.com

The Host Name is used in reporting, and is displayed in alerts, notifications and messages sent by the Barracuda Web Application Firewall.

#### 7. Click Save.



An error will be displayed about a Default Domain not configured. For this lab, this can be ignored. In production, the domain should be matched to that of the certificates being used for the SSL configuration.

#### Task 2: Create a Web Service to Publish the DVWA Application

- 1. Log into the Barracuda Networks device.
  - **User** admin
  - **Password** [InstanceID]
- 2. Go to **BASIC > Services**.



- 3. Go to ADD NEW SERVICE, update the fields, and then click Add.
  - Service Name DVWA
  - Type HTTP
  - Virtual IP Address IP address assigned to the WAF by AWS.
  - **Port** 80
  - **Real Servers** 10.0.1.50 (This is the address you assigned to the DVWA Server)
  - Create Group No
  - Service Groups default

Add New Service				
Service Name	туре НТТРВ	Virtual IP Address	Port	Real Servers
Create Group	Service Groups	DDA		



4. After about 15 seconds the firewall will update and the **Services** pane will now look like below:

Services													
Filter	Service Name 🔻	Searc	h	Sear	ch								
	Name	Status	Hostname	IP Address	Port	Interface	Domain	URL	Туре	Mode	Policy	Ad	bb
🗆 👸 defa	ault												
Ξ	default												
Ξ.	🖶 DVWA	*		10.0.0.67	80	WAN			HTTP	Passive	default	Server R	tule
	Server 10.0.1.50	×		10.0.1.50	80								

5. Open a new tab on the web browser and point it at the DNS name of the Elastic Load Balancer. This should be in the text file that you saved, or can be found on the ELB in the AWS Console. The DVWA server should load with the traffic flowing through the ELB and if the DVWA folder is on the server then it is installed.

If for some reason this webpage doesn't load make sure that you have entered the correct IP address for the barracudawaf and the DVWA web server. Another troubleshooting step if the DVWA is not coming up is to review the NAT Gateway configuration. The NAT Gateway must be deployed into the www subnet and the routing table for the apps subnet must point 0.0.0.0/0 to the NAT Gateway instance.



Task 3: Configure the Damn Vulnerable Web App

1. From the connection to the DVWA server through the ELB, click the **DVWA** link to attach to DVWA and complete its configuration.



	□ Index of / ×	
	$\leftrightarrow$ $\rightarrow$ C $\triangle$ (i) barracudawaf-elb-147	4027757.us-east-1.elb.amazonaws.com
	Index of /	
	<u>Name</u> <u>Last modified</u> <u>Size</u> <u>De</u>	escription
	DVWA.zip 2017-03-07 01:45 1.2M	
	2017-03-04 07:18 -	
	Apache/2.4.7 (Ubuntu) Server at barracuda	rwaf-elb-1474027757.us-east-1.elb.amazonaws.com Port 80
2.	2. This will load the DVWA web applicat	ion and bring up the <b>Database Setup</b> page.
	Setup :: Damn Vulnerable 🗙	
	> C 🟠 🛈 barracudawaf-elb-1474027757.us-ea	st-1.elb.amazonaws.com/DVWA/setup.php
		DYWA
	Setup DVWA Databas	e Setup 🍾
	Instructions Click on the 'Cre If you get an erro	ate / Reset Database' button below to create or reset your database. r make sure you have the correct user credentials in:
	About If the database a You can also use	ready exists, it will be cleared and the data will be reset. this to reset the administrator credentials ("admin // password") at any stage.
	Setup Che	eck
	Operating system Backend databa: PHP version: 5.5	n: *nix e: MySQL .9-1ubuntu4.21
	Web Server SER	VER_NAME: barracudawaf-elb-1474027757.us-east-1.elb.amazonaws.com
_		

3. Scroll down and click **Create / Reset Database**. You will briefly see an update that the database was created and then be redirected to a login page.



- 4. Once at the login page use the following login information to test the application.
  - **Username** admin
  - **Password** password



DVW	A
Username admin	
Password	
******	\$
Login	

This will bring you to the home page of the DVWA page. This means that the application has been setup properly.

Home	Welcome to Damn Vulnerable Web Application!
Instructions	Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its m
Setup / Reset DB	goal is to be an aid for security professionals to test their souts and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teache learn about web application security in a controlled class room environment.
Brute Force	The aim of DVWA is to practice some of the most common web vulnerability, with various difficultly
Command Injection	levels, with a simple straightforward interface.
CSRF	
File Inclusion	General Instructions
File Upload	
Insecure CAPTCHA	It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. T
SQL Injection	is not a fixed object to complete a module; however users should feel that they have successfully exploited system as best as they possible could by using that particular vulnerability.
SQL Injection (Blind)	-,,
XSS (Reflected)	Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.
XSS (Stored)	Digital de la balancia de la companya de la compa
DIGNA Complex	increase the difficulty. This will demonstrate how adding another layer of security may block certain malicion
DVWA Security	actions. Note, there are also various public methods at bypassing these protections (so this can be see an extension for more advance users)!
PHP Into	There is a hale bottom at the bottom of each many which allows you to view blate it time for that whereablish
About	There is a neip button at the bottom of each page, which above you to view nints & tips for that vulnerability There are also additional links for further background reading, which relates to that security issue.
Logout	
	WARNING!
	Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's publi html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as <u>VirtualBox</u> or <u>Vilware</u> ), which is set to NAT networking mode. Inside a guest machine, can drawlasting and testal XAMPS for the web server and database

## Logout

#### Summary:

In this exercise, the Barracuda WAF appliance and the DVWA services were configured. The WAF was configured to connect to the DVWA, and then the DVWA application configuration was completed. This completed the necessary steps to allow for an end to end setup allowing for simulated attacks in



the next exercise.

## Exercise 3: Simulate Attacks and Secure the Environment using the WAF

In this exercise, attacks will be simulated against a website using the DVWA application. Using the tools of the WAF, fixes will be applied to avoid these attacks in the future.

#### **Task 1: Command Injection Attack**

- Open a new tab on your local web browser and navigate to the public IP address of the ELB. The example here is at http://BarracudaWAF-ELB-1474027757.us-east-1.elb.amazonaws.com/DVWA (DVWA is case sensitive). This will load the DVWA application as published via the Barracuda Web Application Firewall.
  - If the address to the ELB is entered into the browser, then simply click the DVWA folder to load the application.
- 2. The login page of the DVWA website will appear. Use these credentials:
  - **Username** admin
  - $\circ$  <code>Password</code> <code>password</code>

	DVWA
Username admin	
Password	
	Login

3. The home page for DVWA will appear in the browser window.



Home	Welcome to Damn Vulnerable Web Application!
Instructions	Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main
Setup / Reset DB	goal is to be an aid for security protessionals to test their skills and tools in a legal environment, help web developers better understand the processes of security web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.
Brute Force	The aim of DVWA is to practice some of the most common web vulnerability, with various difficultly levels
Command Injection	with a simple straightforward interface.
CSRF	Our well be structions
File Inclusion	General Instructions
File Upload	It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There
Insecure CAPTCHA	is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible cruid by using that particular valuerability.
SQL Injection	Diance extentions are beth desumented and underumented underum Rear Black with this software. This is
SQL Injection (Blind)	Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.
XSS (Reflected)	DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further
XSS (Stored)	increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be see an as extension for more advance users)
DVWA Security	There is a bein button at the bottom of each name which allows you to view hints & tips for that uninerability
PHP Info	There are also additional links for further background reading, which relates to that security issue.
About	
	WARNING!
Logout	Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as <u>VirtualExx</u> or <u>VMwarn</u> ), which is set to NAT networking mode. Inside a guest machine, you can downloading and instal XAMPP for the web server and database.

4. Once on the home page click on the **Command Injection** link. Next, type 8.8.8.8 (this is the Google DNS server IP address), in the **Enter an IP address** box, and click **Submit**.

DYWA	
Vulnerability: Command Injection	
Ping a device	
Enter an IP address 8.8.8.8 × Submit	
The page will take 10 seconds or so to run and the provide the following	) output.
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.	
8.8.8.8 ping statistics 4 packets transmitted, 0 received, 100% packet loss, time 30	09ms
Now move back to the browser tab for the WAF and go to <b>BASIC &gt; We</b>	b Firewall Logs.
Barracuda Web Application Firewall	

		all				
BASIC SECURITY POLICIES	WEBSITES	ACCESS	ONTROL	ADVANCED		
Dashboard Services Reports Online Help Search	Default Security	Certificates	IP Configu	ration Admini	stration	Web Firewall Logs

5.



- 6. On the **Web Firewall Logs** page, update the filter with the following details, and then click **Apply Filter**.
  - Service IP
  - is equal to
  - $\circ$  IP address of the WAF

Web Firewall Logs Gener							
Service IP   is equal to	◄ 10.0.0.67	+ Apply Filter					

Notice how the WAF has alerted at the attack.
 Highlighting the red arrow will show the severity alert.

Tim	0		Event Details		Client Detail	5	Attack Details		Actio	ns
$\mathbf{T}$	LOG	GED	URL	/DVWA/vulnerabilities/exe	,		-			
\$	Severity ID	ALERT 8 15aa6cd28fd-f9ecddc6	Service IP:Port Service Name Protocol	10.0.0.67:80 dvwa HTTP	Client IP Country Method	10.0.217 ? Z1 POST	Attack Name Attack Detail Rule	Python PHP Attack in URL type="python-php-attacks-mediur security-policy	Fix	Details
$\mathbf{T}$	LOG	GED	URL	/DVWA/vulnerabilities/exe			-			
	Time Date ID	19:25:47.645 2017-03-06 15aa6cd28fd-f9ecddc6	Service IP:Port Service Name Protocol	10.0.0.67:80 dvwa HTTP	Client IP Country Method	10.0.217 ? Z1 POST	Attack Name Attack Detail Rule	Cookie Tampered Cookie="currentPage" Reason="0 global	Fix	Details
1	LOG Time Date ID	GED 19:25:47.645 2017-03-06 15aa6cd28fd-f9ecddc6	URL Service IP:Port Service Name Protocol	/DVWA/vulnerabilities/exe 10.0.0.67:80 dvwa HTTP	Client IP Country Method	10.0.0.217 ? Z1 POST	Attack Name Attack Detail Rule	Cookie Tampered Cookie="PHPSESSID" Reason=" global	Fix	Details
↑	LOG Time Date ID	GED 19:06:18.407 2017-03-06 15aa6bb51a7-f9ecddc6	URL Service IP:Port Service Name Protocol	/DVWA/vulnerabilities/exe 10.0.0.67:80 dvwa HTTP	Client IP Country Method	10.0.0.217 ? Z1 POST	Attack Name Attack Detail Rule	OS Command Injection in URL type="os-command-injection" pat security-policy	Fix	Details

8. Click **Save Filter**, this will open a new window. Type myfilter into the **Filter Name** box, and then click **Save**.

🖌 Web	Application Firev	vall: Save F	lter - Google Ch	rome	_		×
i barra	acudawaf-elb-147	4027757.u	s-east-1.elb.ama	zonaws.	.com:8000/c	:gi-mod/ind	lex.cg
					S	ave	cel
Save I	Filter						He
Filter	Name: myfi	Iter the name that	you wish to give for	your filter.			
Find th	ne last logged	with the	attack name	OS Co	ommand	Injectio	<b>n in URL</b> , and click <b>Fix</b> .
Time		Event Details		Client Deta	ils	Attack Details	Actions
1 LOG	GED	URL	/DVWA/vulnerabilities/ex	e:	-		
Time	19:06:18.407	Service IP:Port	10.0.0.67:80	Client IP	10.0.0.217	Attack Name	OS Command Injection in URL Fix Details
Date	2017-03-05	Service Name	dvwa	Country	? Z1	Attack Detail	type="os-command-injection" pat
ID	15aa6bb51a7-f9ecddc6	Protocol	HTTP	Method	POST	Rule	security-policy

10. This will open a **Policy Fix** window. Read the details and then click **Apply Fix**.



barracudawaf	elb-1474027757 u	s-east-1 elb amaz	onaws.com:800	)/cai-mod/ir	dev cai	nasswo
y barracudawar	eib-14/402//5/.d.	s-cast- r.eib.amaz	.011aws.co111.0000	o, egi-mou, ii	idex.cgi	passwo
Policy Fix						
OS Command I	jection in URL					
The URL conta	ned /exec/ which is a	OS Command Injec	tion pattern. This is	a Blocked Att	ack type	that is
enabled in the I	efault URL Protection	n of the correspondi	ng Security Policy,	or in the Block	ed Attack	type List
the matching U	RL Profile.					
Recommended	Fix					
Modify the "def	ault" security policy on	the SECURITY PO	LICIES > URL Pro	tection page by	y adding (	c-languag
function-substri	ngs to the "Exception	Patterns" list.				
Click Close V	<b>/indow</b> . ion Firewall: Policy	Fix - Google Chr	ome		_	
) barracudawaf	elb-1474027757.u	s-east-1.elb.ama	zonaws.com:800	)0/cgi-mod/i	index.cg	ji
Policy Fix						
OS Command I	njection in URL					
The URL conta	ned /exec/ which is a	OS Command Inje	ction pattern. This	is a Blocked A	ttack type	e that is
enabled in the	Default URL Protection	n of the correspond	ing Security Policy	, or in the Bloc	ked Attac	ck type Lis
the matching U	RL Profile.					
Policy Fixed.	/					

- 12. Move back to the DVWA application and again launch the command injection attack by entering 8.8.8.8 in the **Ping a Device** tool.
- 13. Once this is completed move back to the WAF tab and click **Apply Filter**. Notice that you no longer see the Attack Name **OS Command Injection in URL**, in the logs.
- 14. Go to **Basic > Dashboard**.



	Barracuda   Web Application Firewall							
	BASIC	SECURITY POLICIES	T	WEBSITES	ACCESS CONTROL			
D	ashboard eports	Services Online Help Search	Defa	ult Security	Certificates	IP Configur		

15. Once at the **Dashboard**, scroll down to the **Attacks** graphs. Change the time to **Last Hour**. It should then resemble the following showing attacks that you have made against the site. You may have to change the time from **Last Day** to **Last Hour** to see the results.



**16**. Move back to the DVWA application in your browser. Click through some of the other attacks. Once this is completed move on to the next task.

#### Task 2: Using Reporting

1. On the BarracudaWAF management screen, click **Reports**.

<b>L</b> Barr	Barracuda   Web Application Firewall										
BASIC	SECURITY	POLICIES	WEBSITES	AC	CESS CONTROL	ADVANCED					
Dashboard Notifications	Reports	Default Secur Online Help S	rity Certific Search	ates	IP Configuration	Administration					

2. In **Report Options** section, change the **Time Frame** to **Today**.





3. Scroll down to the **Security** section, select the checkbox next to **Attacks by Category**, and then click **Show Report**.

Security	
Attacks by Category	Show Report

4. The report window will load showing the different attacks. Take the time to review the report.

Acertije); Sele Flanger Generaled ce:	10.0.0.52 001 2017.04.21.00.00 - 2017.04.22.00.00 diox: 2017.04.21.15.54.05			This report displays the number of stacks for the categories such as Forceful Browning, Xild Injections, etc., for the specified Derivolut) and time trans.						
Vilecks by Cel	egory									
Secolor Temp	₩A									
Facada Ba	turking _									
injection /	dacks _		L .							
Protocal Vic										
			10	n	30 Co	25 unt	20	20	40	
Attacks by	Calegory			Co.	int			-0	eiklove*	
Session Te	mper Attacks				40			Services	Clients	Time
Forceful Bri	awing				10			Services	Clerts	Time
Interface Adv	tacks							Services	Clarits	Time

5. In the drill down section, click on the different areas to better understand the information behind the report. Select **Clients** or **Time**.



- 6. Close the report by hitting the **X** at the top of the window.
- 7. Locate the **Top Attacked URLs** in the **Security** section, select the checkbox, and then click **Show Report**.



Security					
	Attacks by Category	Show Report			
	Attacks By Services	Show Report			
	Attack by Hour	Show Report			
	Attack by Day	Show Report			
	Top Attacking Clients	Show Report			
	Top Attacked Domains	Show Report			
	Top Attacked URLs	Show Report			

8. Review the report and mouse over the charts to see the URLs.





#### Figures

1. worddav8ff9fb17da705b0ef2a20c131f8e9f19.png worddavfc437f774a01573bedf0f2893e11e4d5.png worddavef956a67c35bf222190858f39cdc7c99.png 4. worddavf3e0620c66c3b3404f1db222a1b0ae8a.png 5. worddavc3882903a899cd3ad4695a5a8a9418d7.png 6. worddav0ee9b48178251895c53a8b3ba32bccc7.png 7. worddavc6973ffb21d925fc33817897ed135680.png 8. worddav38490ab292a8ecf4c9488642034df800.png 9. worddav74a33011f21a721717c3b1a5549b79ab.png 10. worddav466ee782638a0e11d4245e95e07f0267.png 11. worddave0dc9f82b83eb199d8c637f8a8907da4.png 12. worddav56be5cfe1ca9af6ca41cd10ca73ec16b.png 13. worddav7b733c09535ad20966652462f3dea4c4.png 14. worddav53be39c2c01954dc36b34adc64d991dd.png 15. worddavd5e033d00901e2466facf74cb0da7845.png 16. worddav17eae58f122d14e789d9177da436b119.png 17. worddavd3e4ae226e330d5510be22682e54353c.png 18. worddava72156f7881ad224db891558193b4958.png 19. worddav9c62d25dcfe1006122e4e6d4127d0ee0.png 20. worddavfa5b3001366ba64a43e47959f15b440a.png 21. worddavfabb225af2887635303226347311b06f.png 22. worddavfda046b87d9435dd1d85a2178973487b.png 23. worddav86cfaa03094bd67249a73727daa2a66a.png 24. worddav4a4166fe965f49c8582ba1b3d0a2b053.png 25. worddav345ae2557ce23d9d82b548b42acc7e67.png 26. worddave1115815535e08269ca9562e00d17287.png 27. worddav4c94ba01377cc2bb0db8fa84470e821b.png 28. worddavf33bd941cb6dd8c2b3610fcc17ab9fef.png 29. worddav115bf6fbce5b3ffc6b45210ab945b993.png 30. worddavc8a73c0a6dc2ecc61871dd8e05d8094c.png 31. worddav0e79554be9acac8d0ab0137c92109d2b.png 32. worddavb574a53d521fcd02c5015370cbe52ba0.png 33. worddav1f562f6082f27918d96a1d1f45eb7314.png 34. worddav35ea34227343c70c5b22625024a4731b.png 35. worddav1048f46a178d51364417112dba4e669d.png 36. worddav4a0e31f4a5866d565a8eb87a5745b9cc.png 37. worddav89f42efb2cae6be3a263c6b51aea462c.png 38. worddav4392991937196367767da9f49a443bff.png 39. worddav8df663f652f3bfeea7b570c2f986f700.png 40. worddavbc637f5f6a985a19cc63781930934b0b.png 41. worddav9b90af958b67e203396d3444c5aa4fff.png 42. worddav7730b0256018f225a6019dc8605ba55f.png 43. worddav01fa4165b21322ddd42b96a5c2fc753a.png 44. worddav4281c00b7838301a78bfbd3678157e36.png



45. worddav82676a9ba0f69f767432784d47dc1045.png 46. worddav094d8acd10cb9b8b15e7984f0ee4c041.png 47. worddav98d03457add444c37a8ac95c98d13bbf.png 48. worddavf6d26255034c21c973d34e9baf6b1354.png 49. worddav32673b37633831396fddd414dc952297.png 50. worddavaf0bb9d34375cec271fc430c365fc1ff.png 51. worddavb83a866e248926edb54b1437a48b2ecb.png 52. worddavcadb6f8f2fd8c41a0c23670638c25304.png 53. worddave0545191485f739a556fea4796b2177f.png 54. worddav0898892df695aa5fcf36cddc7aedd90c.png 55. worddav6fe33f1c26e691b59c4508d1a8da1f2e.png 56. worddavb46c0a86d50b64cba4c6be5b876535b4.png 57. worddavd0af9570dfcd46596a813cce5c0fc7cf.png 58. worddav642ca406a92acdb346cac9a16a7f74b5.png 59. worddav98f426dc282320b7fabeef4a1ea8da8e.png 60. worddav89be6be278341951bd0791494b7ff5fe.png 61. worddav05e68e3b0dd60999efe8dd8251687017.png 62. worddavaa0caddef66d8abe0ae54b85df7b48ad.png 63. worddav419bdf9043d5439fa5a21744120aa244.png 64. worddav885b786336765591e4465fbbd7fd91bc.png 65. worddav08a6886573bd374304417b01fbc102e3.png 66. worddav4913b582a649bacae834e5e086f9e803.png 67. worddav249294e44f173b816f8861878a4e3fcd.png 68. worddav6c5ac430913a6943276fb59a93225409.png 69. worddav22e9e2eb906f90274d538cac9fb5c038.png 70. worddav4824df566c365f0a584399595df772e3.png 71. worddavc5dcab64c5e6be0916622eefc27886fc.png 72. worddav320a041b0c3f6e7977a598e46e90901b.png 73. worddavfd35f03d3d1af7ff873d57a95db9a0e6.png 74. worddava5acfe5b2d2476e45470525cd25bcb79.png 75. worddav06665c890f0295af9f3d707fe2c6e26d.png 76. worddav38260db66bc34a5a461ac93dd377e7b1.png 77. worddav02648564b5f306943cdf8170da8892b4.png 78. worddavfd4f36a2306f13e48bcb1d455910dd31.png 79. worddav0d32601525cfd1556f10cf2ddcd1d296.png 80. worddav2f329f45a10cb4d2eb37431565d077d1.png 81. worddav3d026e7bd5b2a2eff2542c6e24546069.png 82. worddav596254fe45cd52f0c7af1ea3f87ac7ab.png 83. worddav55bfab4ad0fad9ee83bf1ca1f4a31236.png 84. worddavb7fc9dd81930eac922a2c2c6e2f07961.png 85. worddav32ffefc46f79badba2c563f19f523b69.png 86. worddavb11cdc19d121485728690174ad4c995e.png 87. worddavcbb197e3763a53d0f93fc66dcf28e5b1.png 88. worddavbb6d6f8611b9bf79b92099486ce8f23c.png 89. worddav1650ad5358e6ced0ab2893cf6c81d454.png 90. worddav794fdceff6675b7800424d37c1ab8cdf.png



91. worddav49dfcd05d8d2830c87de165113c2abcb.png 92. worddav0f9e84fd32993e5c93b04b6c806d5319.png 93. worddavea5dff0af68581ab9634877d9ea475e8.png 94. worddav91253f722774901ecfa23ec001c58b3c.png 95. worddav0392b84bb5f701533713ad1aab7799a4.png 96. worddav42908e8e7d181f14eed7cd5c9f69f5b7.png 97. worddav3be06025b5514404be4af4e1ecb3e66d.png 98. worddav3822110428382fd73ed91c7bf807ec1f.png 99. worddavc9202fd38692192ed4c899ec80da6e05.png 100. worddave754f06d15b095549f11bf81495a1a58.png 101. worddavd0501c5d3bc56d4fd41c47956f1c2de3.png 102. worddav12437c9e962b3caec91aa8a0be9189b9.png 103. worddav4e5e7652bda57232826d4dce40ffbc68.png 104. worddavefea08350a1456428358916e1cfac607.png 105. worddav305c54e6b6181349ff7062c3ccede8ec.png 106. worddavd338e13fc1aa154ad8c6c10f7a924500.png 107. worddav91359f09ff26f5da9976f83b0c81f147.png 108. worddavff7204555747ef5343b535d579ad2fe5.png 109. worddav4544c714e6ed6b34446e733ae26d40b4.png 110. worddava57cdb947303c8fad7e8d0a36c3e640a.png 111. worddav602857c687ba53880235e957fa84a42f.png

<sup>©</sup> Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.