Bug Bounty Recon Like A Pro

October 9, 2018 xer0dayz Bug Bounties, Hacking Tutorials, Uncategorized

Total Share 4

Facebook 0 Twitter 4 Google plus 0 Reddit 0 +

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Overview

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

In this blog post, I will cover the basic steps to performing bug bounty recon against large, open scoped programs and penetration tests.

If you're like most starting out, this process can seem daunting and overwhelming depending on how many hosts you're dealing with. Twitter for instance has 20,000+ subdomains and a HUGE attack surface to go through. How do you know where to focus your time? How do you keep track of which hosts you scanned and reviewed? These questions can quickly lead you spinning in circles, wasting valuable time while more experienced hunters get the gold. Luckily, there are tools and methodologies that can assist and make your life easier as a bug bounty hunter or penetration tester. This is where Sn1per comes in...

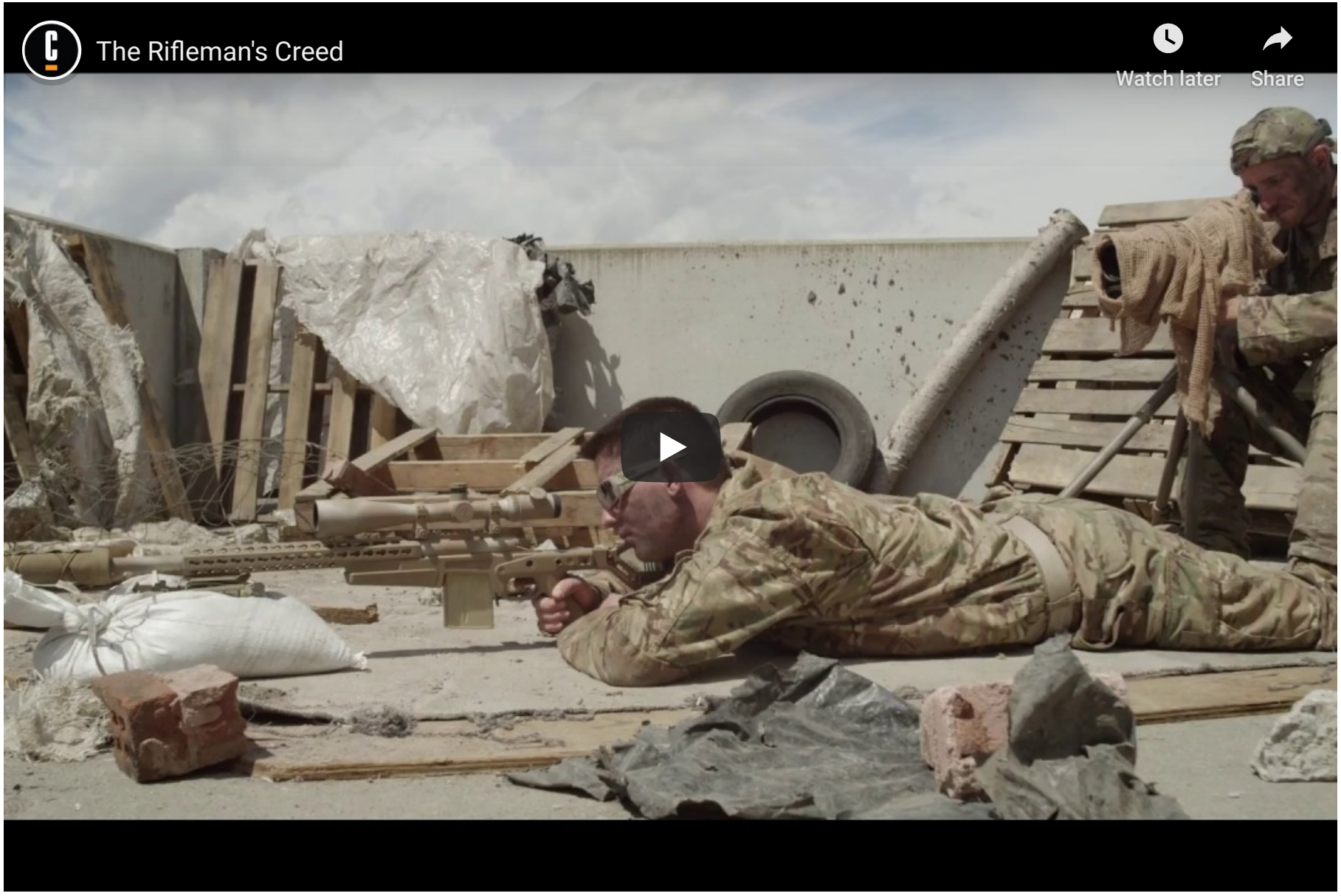
What is Sn1per?

Sn1per is an automated pentest reconnaissance scanner that can be used during penetration tests and bug bounties and to enumerate targets and scan for vulnerabilities. There are two versions of Sn1per available depending on your needs. Sn1per Community Edition (CE) is the open source scan engine that is maintained on Github (https://github.com/1N3/Sn1per). Sn1per Professional is XeroSecurity's premium reporting add on for Sn1per and is available exclusively from the XeroSecurity website (https://xerosecurity.com).

Installation

Installation is extremely easy. Just clone the Github repo (git clone https://github.com/1N3/Sn1per) and run ./install.sh from a Kali Linux OS. This will install all tools and dependencies which are used to collect recon info and scan for vulnerabilities.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Scoping your target

Create PDF in your applications with the Pdfcrowd HTML to PDF API
PDFCROWD

So we have Sn1per installed and we've recited "The Rifleman's Creed" a few times, the next phase is scoping our target. This is fairly obvious but we need to carefully review the bug bounty or pentest scope which gives us legal permission to test without getting thrown in prison. If you find yourself getting outside the intended scope, you've been warned – **This "could" land you in jail!**.

Create PDF in your applications with the Pdfcrowd HTML to PDF API
PDFCROWD

Now that the legal disclaimer is out of the way, what's the first step?

Tactical Reconnaissance & OSINT

The first step in your reconnaissance process should be enumerating all subdomains and hosts within the target scope. For this, we're interested in any wildcard domains (ie. *.target.com). In this case, it is up to the researcher to hunt for subdomains and hosts which fall within this target scope but haven't been explicitly stated. For this, we will use sniper to actively and passively scan a target domain for subdomains via the -re switch and we'll create a new workspace to store all our hosts via the -w switch. Additionally, we'll also add the –osint switch to our scan to perform basic OSINT (Open Source Intelligence Gathering) searches on the target domain. This can reveal tons of useful information such as email addresses, public domains, documents, usernames, software used, whois info, reverse IP lookups, virtual hosts, etc. In addition, Sn1per will perform basic checks for subdomain hijacking and takeovers.

```
sniper -t target.com --recon --osint -w workspace_alias
```

This will store a complete list of all subdomains discovered and sorted at the following location:

```
/usr/share/sniper/loot/workspace/<WORKSPACE_ALIAS>/domains/domains-all-sorted.txt
```

Calling In The Airstrike...

Now that we've enumerated all subdomains for the in-scope wildcard domain, we need to quickly enumerate all hosts with a high level flyover. This can be done by passing our host list from the previous step via the -f switch and running sniper in airstrike mode via the -m airstrike options. This will store all gathered data to our workspace and combine the data from all hosts scanned under /usr/share/sniper/loot/workspace/<WORKSPACE_ALIAS>/.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Some basic info gathered from this mode include: DNS, open ports, HTTP headers, SSL ciphers, web fingerprints, TCP banners, WAF detection and basic file/directory and passive URL discovery.

```
sniper -f /usr/share/sniper/loot/workspace/<WORKSPACE_ALIAS>/domains/domains-all-sorted.txt -m airstrike -w workspace
```

Summary

After the Sn1per finishes scanning all hosts in our workspace, Sn1per Professional gives us some high level info via the console for each host as shown below. This will help us get a high level visual of the attack surface based on which ports are open, interesting HTTP headers, page titles and DNS records. It will become very clear that if the host has no DNS or open ports, there probably isn't much of an attack surface to dig into further. It's best to focus on interesting ports (ie. port 21 (FTP), port 22 (SSH), 3306 (MySQL), etc.) and web targets with interesting headers (ie. Server: Apache Tomcat v7.0.0) may be vulnerable and have known exploit code available.

Professional Reporting Interface

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

After our report gets generated, we can see Sn1per enumerated and scanned 1268 unique hosts automatically. As a penetration tester, you can now sift through all the information contained in your workspace to begin looking for interesting hosts and potential vulnerabilities. To help us manage all this

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

data, we will leverage Sn1per Professional for the next steps in the process. Sn1per Professional offers the following features to help make our lives a bit easier.

Features:

– Professional reporting interface.
– Slideshow for all gathered screenshots.
– Searchable and sortable DNS, IP and open port database.
– Quick links to online recon tools and Google hacking queries.
– Personalized notes field for each host.

Demo Video:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Slideshow For All Gathered Screenshots

Create PDF in your applications with the Pdfcrowd HTML to PDF API
PDFCROWD

From here, we can perform visual recon via the "Slideshow" feature in Sn1per Pro. This can reveal all sorts of potentially interesting hosts which can help identify which hosts need to be scanned further for more information.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Searchable/Sortable DNS, IP and Open Port Database

To supplement our surface level reconnaissance, we can also utilize the "Port List" feature which provides a widget of all subdomains, open ports, DNS and page titles. All data stored within this widget can then be sorted and searched for based on your needs (ie. If you're looking for port 22/tcp (SSH), search for "22". If you want to find all virtual hosts in the environment based on the same page title, enter the full page title (ie. "Overstock Cars"), etc. The possibilities here are endless but we can quickly find interesting hosts and ports or DNS records using this feature in Sn1per Professional.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Conclusion

This concludes part one of this series. This is by no means a comprehensive recon tutorial, but it should be enough to get you started in the process. Stay tuned for more recon tips and tricks for getting the most out of your bug bounty and pentest recon with Sn1per.

@xer0dayz

https://xerosecurity.com

https://twitter.com/xerosecurity

Total Share **4**

Facebook 0 | Twitter 4 | Google plus 0 | Reddit 0 | +

Related

Sn1per Professional v7.0 Released!
May 31, 2019
In "News"

Sn1per Community Edition v7.0 Released!
May 8, 2019
In "News"

Aruba Networks AP-205 (Multiple Vulnerabilities)
February 17, 2017
In "Bug Bounties"

Tags: Bugbounty Pentest Professional Recon Scanner Sn1per Xer0dayz

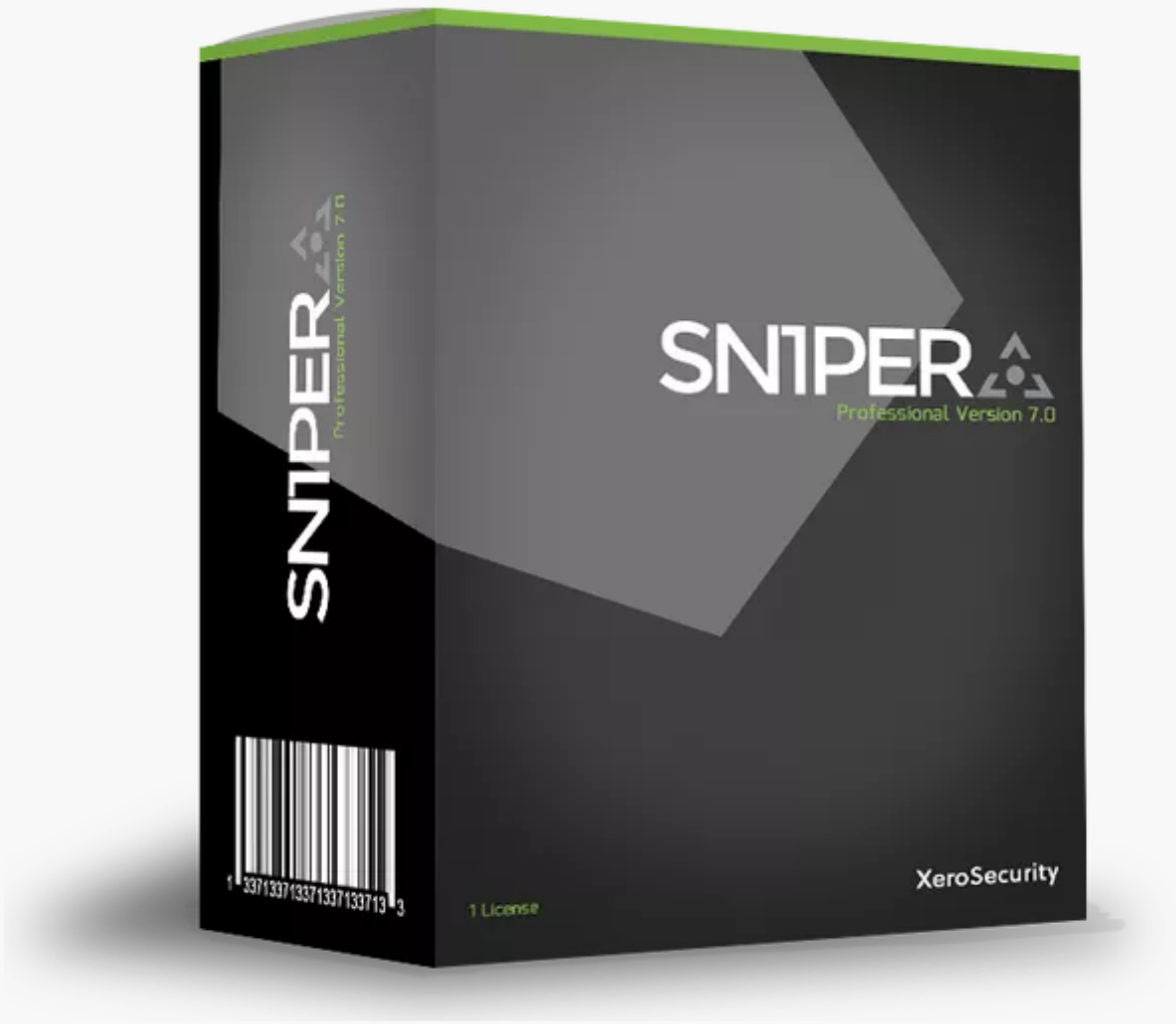
Leave a Reply

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Enter your comment here...

Products

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Sn1per Professional v7.0

$99.00

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Search

Recent Posts

Sn1per Professional v7.0 Released!

May 31, 2019

Sn1per Community Edition v7.0 Released!

May 8, 2019

Sn1per Professional v6.0 now available!

December 17, 2018

Bug Bounty Recon Like A Pro

October 9, 2018

IPSwitch MoveIt Stored Cross Site Scripting (XSS)

January 15, 2018

Exploiting Python Deserialization Vulnerabilities

September 4, 2017

Exploiting Path Traversal in PSPDFKit for Android (2.3.3 – 2.8.0)

August 11, 2017

Advanced Client Side Exploitation Using BeEF

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

April 15, 2017

Aruba Networks AP-205 (Multiple Vulnerabilities)

February 17, 2017

WordPress 4.7.0 – 4.7.1 REST API Content Injection Exploit

February 1, 2017

Dirty COW EoP PoC (CVE-2016-5195)

October 24, 2016

CVE-2016-4401 – Unauthenticated Database Credential Leak In Aruba ClearPass

October 17, 2016

Zabbix 2.2.x, 3.0.x SQL Injection/RCE 0day Vulnerability

August 17, 2016

Droopy Boot2Root CTF Solution

May 15, 2016

Exploiting PHP Serialization/Object Injection Vulnerabilities

April 15, 2016

Recent Comments

Archives

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

May 2019

December 2018

October 2018

January 2018

September 2017

August 2017

April 2017

February 2017

October 2016

August 2016

May 2016

April 2016

February 2016

January 2016

December 2015

November 2015

October 2015

July 2015

June 2015

Categories

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Bug Bounties

CTF's

CVE's

Exploits & PoC's

Hacking Tutorials

News

Uncategorized

Meta

Log in

Entries RSS

Comments RSS

WordPress.org

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

ABOUT

Offensive security solutions for professional hackers, pentesters, bug bounty hunters and enterprise security teams.

CONTACT INFO

E-Mail: support@xerosecurity.com

Web: https://xerosecurity.com

ADDITIONAL LINKS

Blog

Github

Legal

Twitter

YouTube

RECENT NEWS

Sn1per Professional v7.0 Released!

Sn1per Community Edition v7.0 Released!

Sn1per Professional v6.0 Released!

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Copyright 2019 @XeroSecurity. All rights reserved.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD