COURSE: Recon for Ethical Hacking / Penetration Testing & Bug Bounty

Navigating the Art of Reconnaissance in Ethical Hacking, Penetration Testing & Bug Bounty Hunting

Introduction:

In the ever-evolving landscape of cybersecurity, one truth remains constant: knowledge is power. Ethical hackers, penetration testers, and bug bounty hunters are driven by an insatiable curiosity to uncover vulnerabilities, safeguard systems, and contribute to a safer digital realm. Welcome to the enlightening Udemy course "Recon for Ethical Hacking / Penetration Testing & Bug Bounty." In this article, we invite you to embark on a journey of discovery through the intricacies of reconnaissance—the foundation upon which effective cybersecurity strategies are built.

New Tools And Techniques for Passive Recon

1) The Harvester:

   The Harvester is a reconnaissance tool that allows hackers to gather information about email accounts, subdomains, and hostnames. This tool uses a combination of search engines and data sources to collect information that can be used for social engineering, phishing, and other attacks.

- You can read up more about The Harvester here: https://www.kali.org/tools/theharvester/

2) **Recon-ng:**

Recon-ng is a reconnaissance framework that provides a modular approach to passive recon. This tool can be used to gather information from multiple sources, such as search engines, social media platforms, and other data sources. Recon-ng is highly customizable, making it an excellent choice for hackers looking for a tool that can be tailored to their specific needs.

```
File  Actions  Edit  View  Help
[recon-ng][javatpoint] > marketplace
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [ ... ]

[recon-ng][javatpoint] > marketplace search
```

Path	Version	Status	Updated	D	K
discovery/info_disclosure/cache_snoop	1.1	not installed	2020-10-13		
discovery/info_disclosure/interesting_files	1.2	not installed	2021-10-04		
exploitation/injection/command_injector	1.0	not installed	2019-06-24		
exploitation/injection/xpath_bruter	1.2	not installed	2019-10-08		
import/csv_file	1.1	not installed	2019-08-09		
import/list	1.1	not installed	2019-06-24		
import/masscan	1.0	not installed	2020-04-07		
import/nmap	1.1	not installed	2020-10-06		
recon/companies-contacts/bing_linkedin_cache	1.0	not installed	2019-06-24		*
recon/companies-contacts/censys_email_address	2.0	not installed	2021-05-11	*	*
recon/companies-contacts/pen	1.1	not installed	2019-10-15		
recon/companies-domains/censys_subdomains	2.0	not installed	2021-05-10	*	*
recon/companies-domains/pen	1.1	not installed	2019-10-15		
recon/companies-domains/viewdns_reverse_whois	1.1	installed	2021-08-24		
recon/companies-domains/whoxy_dns	1.1	not installed	2020-06-17		*
recon/companies-hosts/censys_org	2.0	not installed	2021-05-11	*	*
recon/companies-hosts/censys_tls_subjects	2.0	not installed	2021-05-11	*	*
recon/companies-multi/github_miner	1.1	not installed	2020-05-15		*
recon/companies-multi/shodan_org	1.1	not installed	2020-07-01	*	*
recon/companies-multi/whois_miner	1.1	not installed	2019-10-15		
recon/contacts-contacts/abc	1.0	not installed	2019-10-11	*	
recon/contacts-contacts/mailtester	1.0	not installed	2019-06-24		
recon/contacts-contacts/mangle	1.0	not installed	2019-06-24		
recon/contacts-contacts/unmangle	1.1	not installed	2019-10-27		
recon/contacts-credentials/hibp_breach	1.2	not installed	2019-09-10		*
recon/contacts-credentials/hibp_paste	1.1	not installed	2019-09-10		*
recon/contacts-domains/migrate_contacts	1.1	not installed	2020-05-17		
recon/contacts-profiles/fullcontact	1.1	not installed	2019-07-24		*
recon/credentials-credentials/adobe	1.0	not installed	2019-06-24		
recon/credentials-credentials/bozocrack	1.0	not installed	2019-06-24		
recon/credentials-credentials/hashes_org	1.0	not installed	2019-06-24		*
recon/domains-companies/censys_companies	2.0	not installed	2021-05-10	*	*
recon/domains-companies/pen	1.1	not installed	2019-10-15		
recon/domains-companies/whoxy_whois	1.1	not installed	2020-06-24		*
recon/domains-contacts/hunter_io	1.3	not installed	2020-04-14		*
recon/domains-contacts/metacrawler	1.1	not installed	2019-06-24	*	
recon/domains-contacts/pen	1.1	not installed	2019-10-15		
recon/domains-contacts/pgp_search	1.4	not installed	2019-10-16		
recon/domains-contacts/whois_pocs	1.0	not installed	2019-06-24		
recon/domains-contacts/wikileaker	1.0	not installed	2020-04-08		
recon/domains-credentials/pwnedlist/account_creds	1.0	not installed	2019-06-24	*	*

- You can read up more about The Harvester here:
  https://github.com/lanmaster53/recon-ng
  https://www.kali.org/tools/recon-ng/