root@hacklab:~/parte-01/lezione-06

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 06

Wireless e Network Attacks

Sicurezza delle reti wireless e attacchi di rete.

docente **Vincenzo Calabro** fase Dominio di rete: wireless e attacchi di rete

root@hacklab:~/lezione-06/agenda $

LEZIONE 06 / AGENDA

In questa lezione

// PERCORSO

> 802.11 e sicurezza WPA2/WPA3
> Rogue AP, evil twin, WPS
> Packet crafting e MITM
> Sicurezza della rete cablata
> Analisi del traffico

metodo obiettivi -> teoria -> strumenti -> laboratorio -> caso di studio -> etica -> verifica

LEZIONE 06 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

> Comprendere — protocolli wireless e debolezze
> Applicare — MITM e sniffing in laboratorio
> Analizzare — il traffico catturato
> Valutare — contromisure (WPA3, HSTS, 802.1X)
> Creare — una relazione di analisi del traffico

LEZIONE 06 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Reti wireless e cablate offrono vettori spesso sottovalutati, dal rogue AP al man-in-the-middle. La lezione analizza protocolli, debolezze e contromisure, con l'analisi del traffico come filo conduttore.

// PERCHE CONTA

Sicurezza delle reti wireless e attacchi di rete.

LEZIONE 06 / MAPPA // INSIEME

Mappa d'insieme del modulo

Attacco/tecnica · Difesa · Norme & metodo · IA

FONDAMENTI

- 01 Wi-Fi: WEP, WPA2 e WPA3
- 02 Rogue AP, evil twin e deauth
- 03 Man-in-the-middle e SSL stripping
- 04 Attacchi alla rete cablata
- 05 Analisi del traffico e dati in chiaro

APPROFONDIMENTI

- 06 Handshake, PMKID e cracking offline
- 07 Limiti dell'SSL stripping
- 08 VLAN hopping e difesa 802.1X
- 09 DNS spoofing e captive portal
- 10 Dati in chiaro e anomalie di rete

LEZIONE 06 / MAPPA // FONDAMENTI

Mappa dei concetti — Fondamenti

Attacco/tecnica · Difesa · Norme & metodo · IA

LEZIONE 06 / CONCETTO 1/10

[Attacco/tecnica]

Wi-Fi: WEP, WPA2 e WPA3

// SPIEGAZIONE

Le reti 802.11 si sono evolute da WEP, rotto da anni, a WPA2 e WPA3. L'autenticazione WPA2-PSK si basa su un handshake a quattro vie o sul PMKID, catturabili via radio e attaccabili offline per recuperare la passphrase; WPA3 introduce SAE per resistere a questo.

// ESEMPIO

```
$ hcxdumptool cattura il PMKID, poi hashcat -m 22000 tenta la passphrase offline
```

LEZIONE 06 / CONCETTO 2/10

[Attacco/tecnica]

Rogue AP, evil twin e deauth

// SPIEGAZIONE

Un access point civetta (evil twin) imita una rete legittima per indurre i client a connettersi e cedere credenziali; i frame di deautenticazione forzano la disconnessione per catturare l'handshake; il WPS debole accelera il recupero del PIN. Scapy consente di forgiare questi pacchetti.

// ESEMPIO

> Deauth mirato per staccare un client e catturarne l'handshake alla riconnessione.

LEZIONE 06 / CONCETTO 3/10 [Difesa]

Man-in-the-middle e SSL stripping

// SPIEGAZIONE

Avvelenando ARP o DNS l'attaccante si inserisce tra vittima e gateway; l'SSL stripping tenta di declassare HTTPS a HTTP per leggere il traffico. HSTS vanifica lo stripping obbligando il browser a usare sempre HTTPS verso i siti noti.

// ESEMPIO

```
$ arpspoof -i eth0 -t 10.0.0.5 10.0.0.1
```

LEZIONE 06 / CONCETTO 4/10

[Difesa]

Attacchi alla rete cablata

// SPIEGAZIONE

Anche il cablato ha debolezze: il VLAN hopping sfrutta trunk mal configurati per saltare tra segmenti, mentre 802.1X controlla l'accesso alla porta. Senza un NAC robusto, una semplice presa di rete puo bastare per entrare.

// ESEMPIO

> Un laptop collegato a una presa non protetta da 802.1X raggiunge la VLAN interna.

LEZIONE 06 / CONCETTO 5/10

[Attacco/tecnica]

Analisi del traffico e dati in chiaro

// SPIEGAZIONE

Catturare e leggere il traffico rivela protocolli non cifrati, credenziali in chiaro e metadati utili. Wireshark e strumenti simili trasformano i pacchetti in evidenza, ma generano dati sensibili da trattare con cautela e solo entro lo scope.

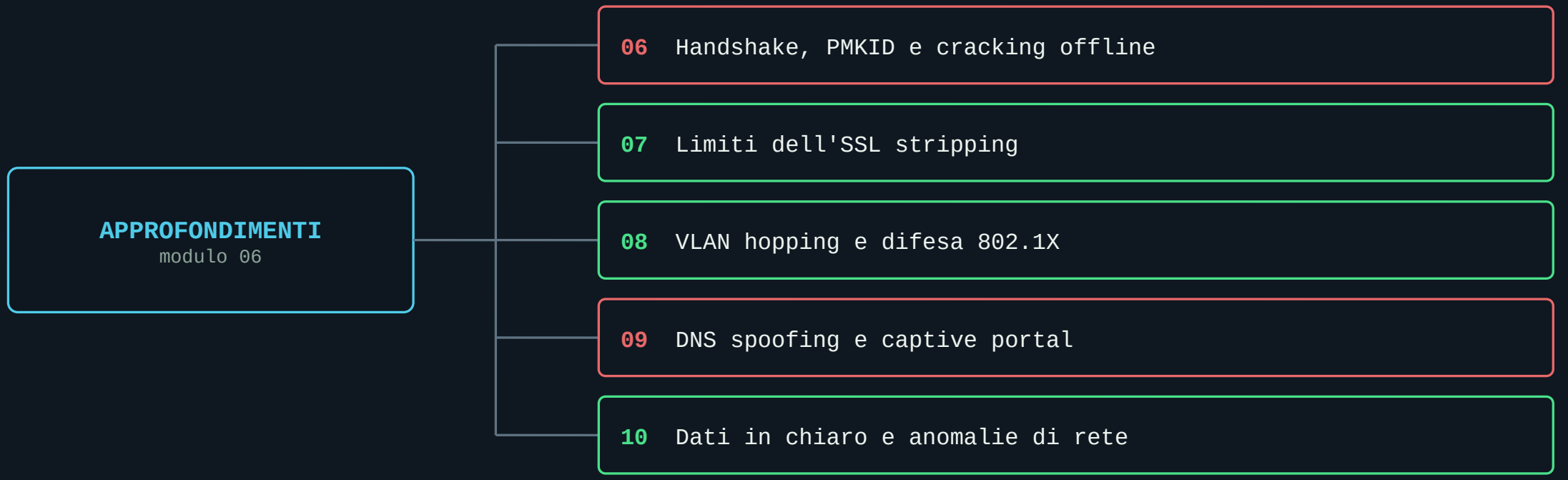
// ESEMPIO

> Un protocollo legacy invia la password in chiaro, visibile in un singolo pacchetto catturato.

LEZIONE 06 / MAPPA // APPROFONDIMENTI

Mappa dei concetti — Approfondimenti

Attacco/tecnica · Difesa · Norme & metodo · IA



LEZIONE 06 / CONCETTO 6/10

[Attacco/tecnica]

Handshake, PMKID e cracking offline

// SPIEGAZIONE

Catturato l'handshake o il PMKID, l'attacco prosegue offline senza altra interazione con la rete: la robustezza dipende solo dalla passphrase. Una chiave lunga e casuale rende il cracking impraticabile, una debole cade in minuti.

// ESEMPIO

> Una passphrase da dizionario cade; venti caratteri casuali resistono al cracking offline.

LEZIONE 06 / CONCETTO 7/10

[Difesa]

Limiti dell'SSL stripping

// SPIEGAZIONE

L'SSL stripping funziona solo se il browser accetta di parlare in HTTP. HSTS, soprattutto con preload, chiude questa finestra imponendo HTTPS dal primo contatto: per questo e una contromisura chiave contro gli attacchi MITM sul web.

// ESEMPIO

> Con HSTS preload il browser rifiuta a priori la connessione HTTP, bloccando lo stripping.

LEZIONE 06 / CONCETTO 8/10

[Difesa]

VLAN hopping e difesa 802.1X

// SPIEGAZIONE

Il VLAN hopping sfrutta auto-trunking e native VLAN mal configurate; si previene disabilitando DTP, fissando le porte in modalita access e usando 802.1X per autenticare chi si collega. La segmentazione vale solo se la rete la applica davvero.

// ESEMPIO

> Disabilitare DTP e impostare le porte utente come access blocca il double-tagging.

LEZIONE 06 / CONCETTO 9/10

[Attacco/tecnica]

DNS spoofing e captive portal

// SPIEGAZIONE

Controllando la risoluzione DNS si dirottano le vittime verso server controllati; un captive portal falso imita la pagina di login di una rete pubblica per raccogliere credenziali. Sono tecniche comuni sui Wi-Fi aperti.

// ESEMPIO

> Un evil twin mostra un captive portal che chiede le credenziali aziendali.

LEZIONE 06 / CONCETTO 10/10

[Difesa]

Dati in chiaro e anomalie di rete

// SPIEGAZIONE

L'analisi del traffico serve anche alla difesa: individuare protocolli non cifrati, beacon periodici e picchi anomali aiuta a scoprire sia misconfigurazioni sia attivita malevola. Un C2 nascosto spesso emerge come pattern regolare insospettabile.

// ESEMPIO

> Beacon verso un dominio sconosciuto ogni cinque minuti: possibile canale C2.

LEZIONE 06 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Aircrack-ng | Wifite | Kismet | Reaver | Bettercap | Fluxion | Wireshark | Ettercap | Scapy

// NOTA OPERATIVA

> Ogni strumento si usa in ambiente virtualizzato e isolato, solo su bersagli di proprieta o autorizzati. Output e artefatti vanno protetti e, a fine ingaggio, gestiti o distrutti.

root@hacklab:~/lezione-06/lab-1 $

LEZIONE 06 / LABORATORIO 1

Laboratorio 1

$ MITM in laboratorio (Bettercap + Wireshark)

// PROCEDURA

[1] Esegui ARP spoofing (Bettercap) e cattura il traffico (Wireshark)

[!] Verifica: Quali indizi rivelano un MITM?

LEZIONE 06 / LABORATORIO 2

Laboratorio 2

$ Handshake WPA2 su rete dedicata

// PROCEDURA

[1] Cattura l'handshake WPA2 su rete dedicata e cracka con wordlist

[!] Verifica: Perche WPA3 mitiga gli attacchi offline?

LEZIONE 06 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Intrusione originata da un rogue AP / evil twin in azienda, con difese (802.1X).

// ANALISI RICHIESTA

> Ricostruisci la dinamica dei fatti con metodo e tracciabilita
> Individua errori, cause radice e punti di decisione critici
> Proponi contromisure, controlli e lezioni apprese

LEZIONE 06 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] Intercettare comunicazioni altrui = art. 617-quater c.p.; solo reti di laboratorio dedicate.

LEZIONE 06 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

> Protocolli wireless e debolezze
> MITM e sniffing in laboratorio
> Il traffico catturato
> Contromisure (WPA3, HSTS, 802.1X)
> Una relazione di analisi del traffico

LEZIONE 06 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

? Quali indizi rivelano un attacco MITM?

? Perche WPA3 mitiga gli attacchi offline?

? A cosa serve HSTS contro lo SSL stripping?

// VALUTAZIONE

Relazione di analisi del traffico con contromisure.

// LETTURE

Doc. Aircrack-ng; guida a Wireshark.

lezione 06 completata

$ next

Wireless e Network Attacks

[!] Le competenze di questa lezione si impiegano esclusivamente in contesti legali, autorizzati e deontologicamente corretti, entro lo scope e con autorizzazione scritta.

root@hacklab:~# _

root@hacklab:~/contatti $

CONTATTI / RISORSE

Restiamo in contatto

Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it

Inquadra il QR con la fotocamera per aprire il sito.