Gruppo
Utenti
Linux
Cagliari
h...?

LINUX DAY

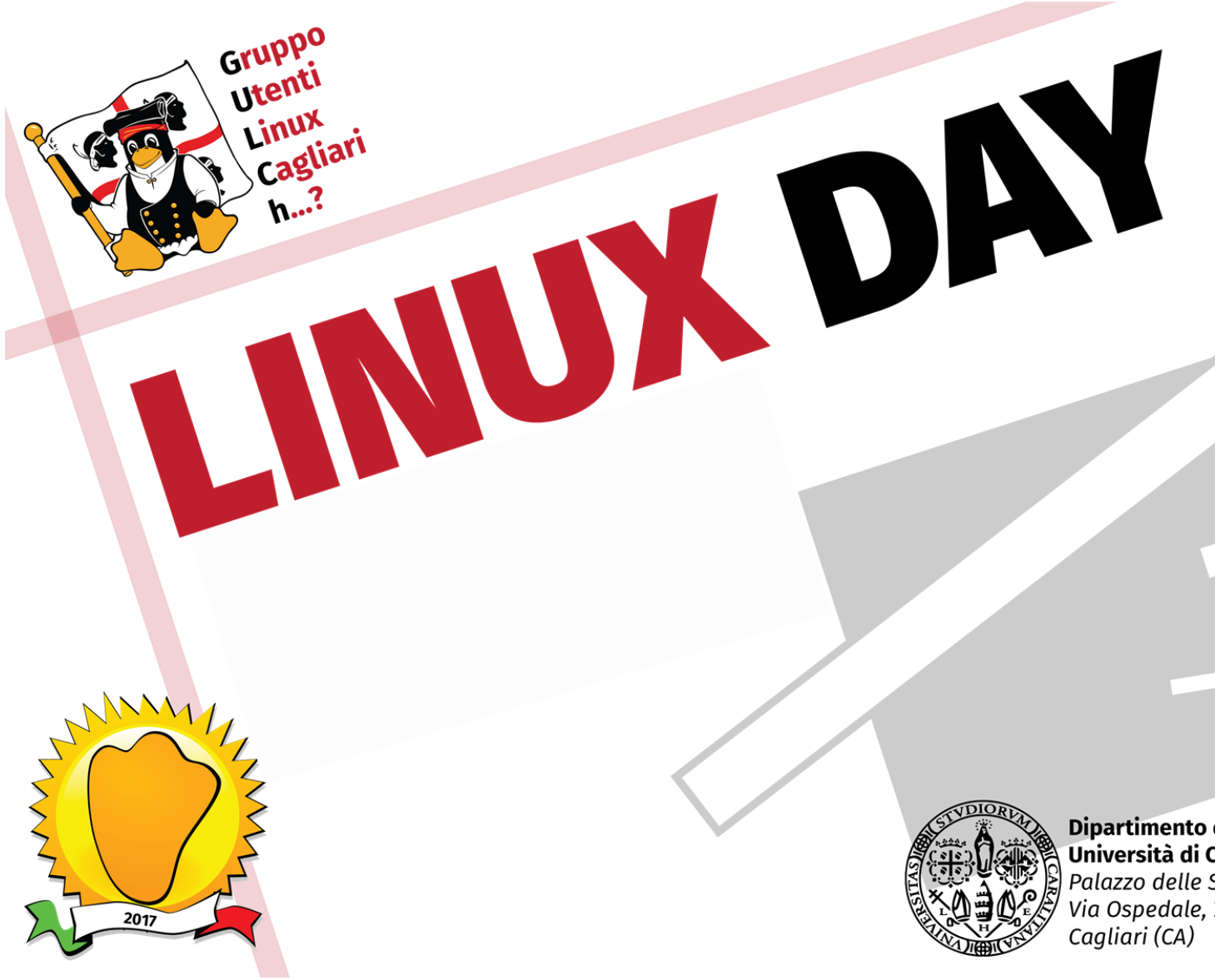
IL PENETRATION TEST

Dipartimento di Informatica
Università di Cagliari
Palazzo delle Scienze
Via Ospedale, 72
Cagliari (CA)

Di cosa parliamo?

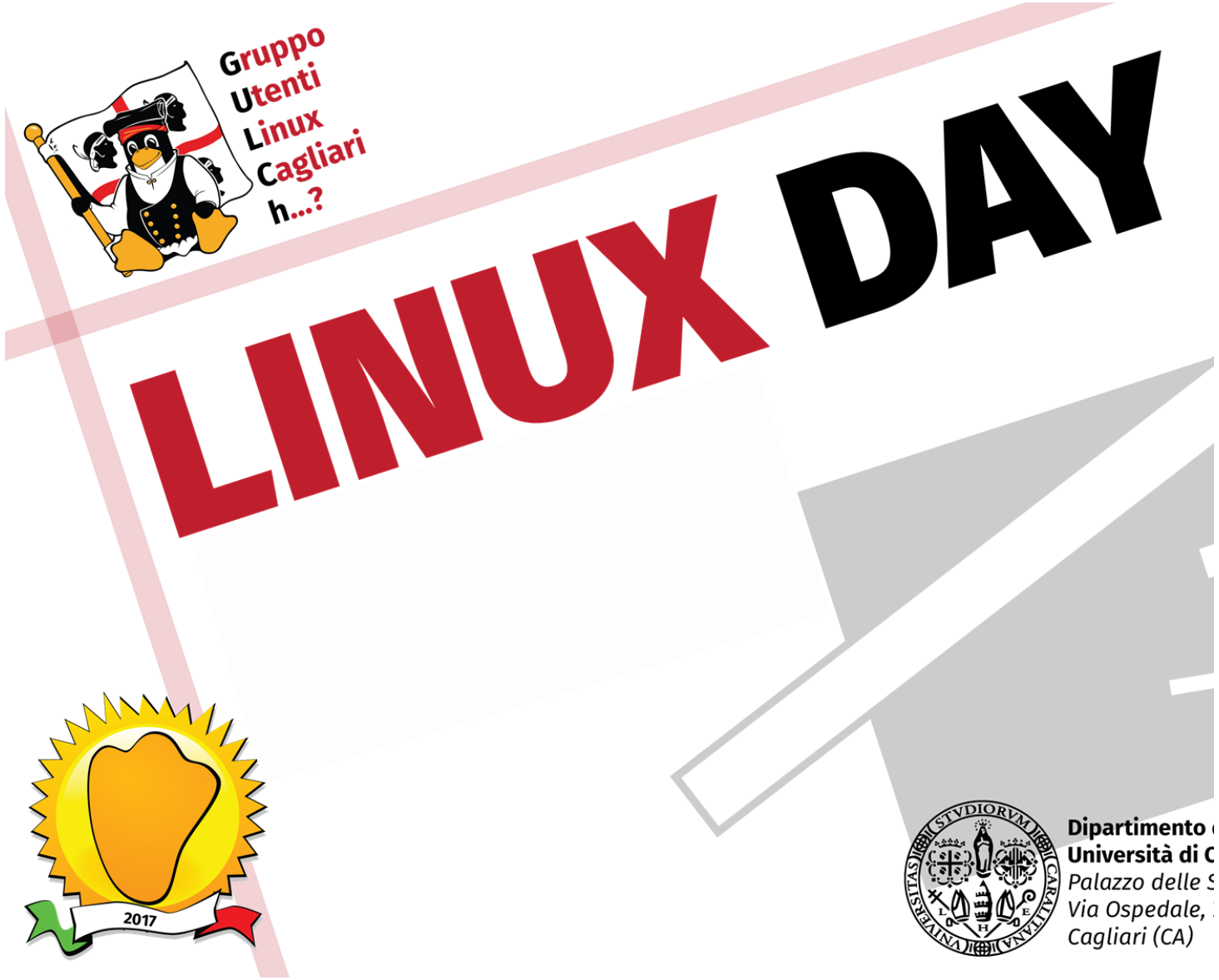
“In informatica, il *penetration test* (o informalmente pen test) è il processo operativo di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato.”

Cit.Wikipedia



In parole più semplici:

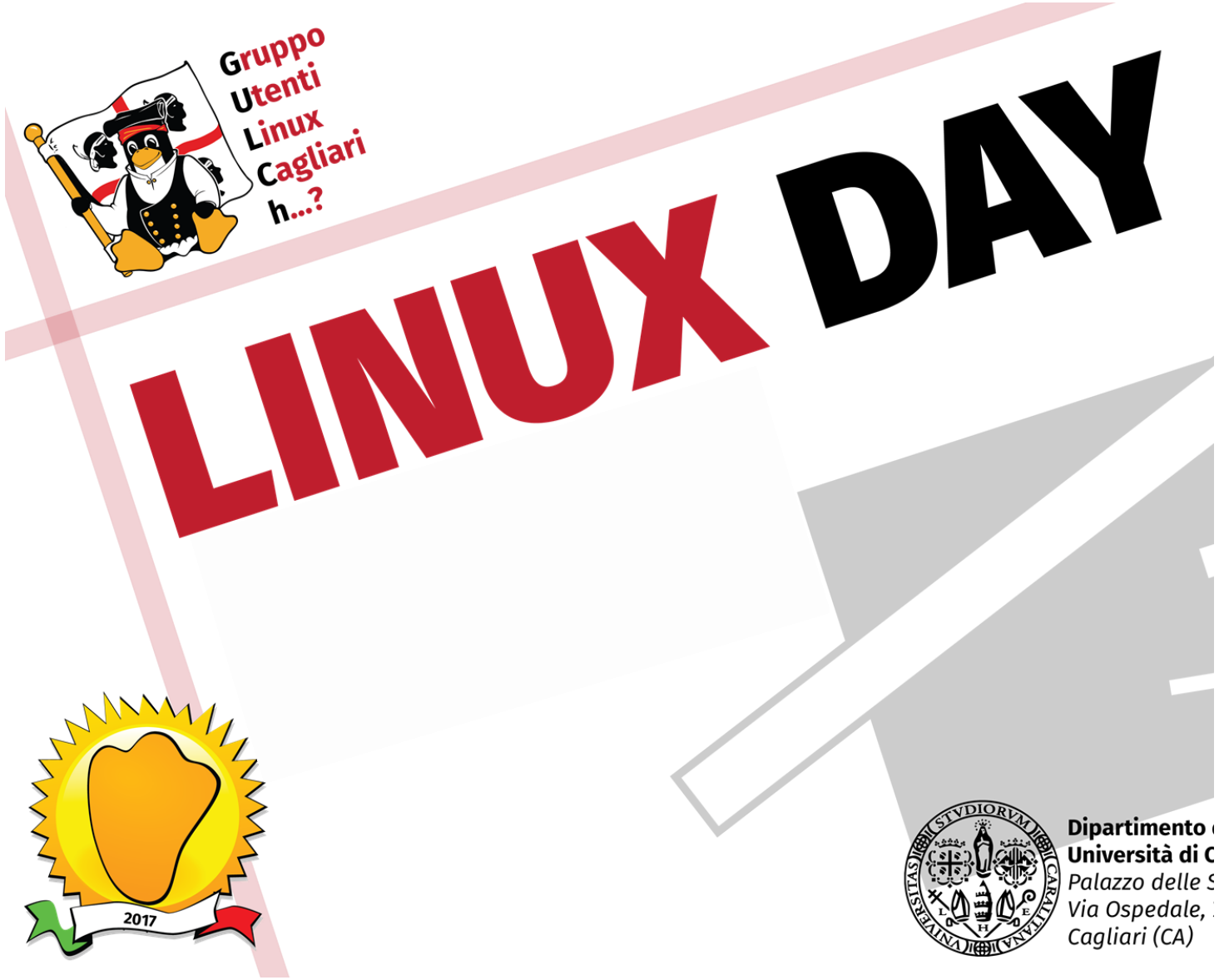
Un pentest è una prova, un’attacco ‘‘simulato’’ per verificare la sicurezza di un qualsiasi sistema (può essere una semplice rete locale, o un grande server online) e appunto migliorarne la stabilità.



Chi lo effettua?

Dipende. Esistono delle figure professionali (sono sempre più presenti nel mercato on-line) che lavorano in questo ambito.

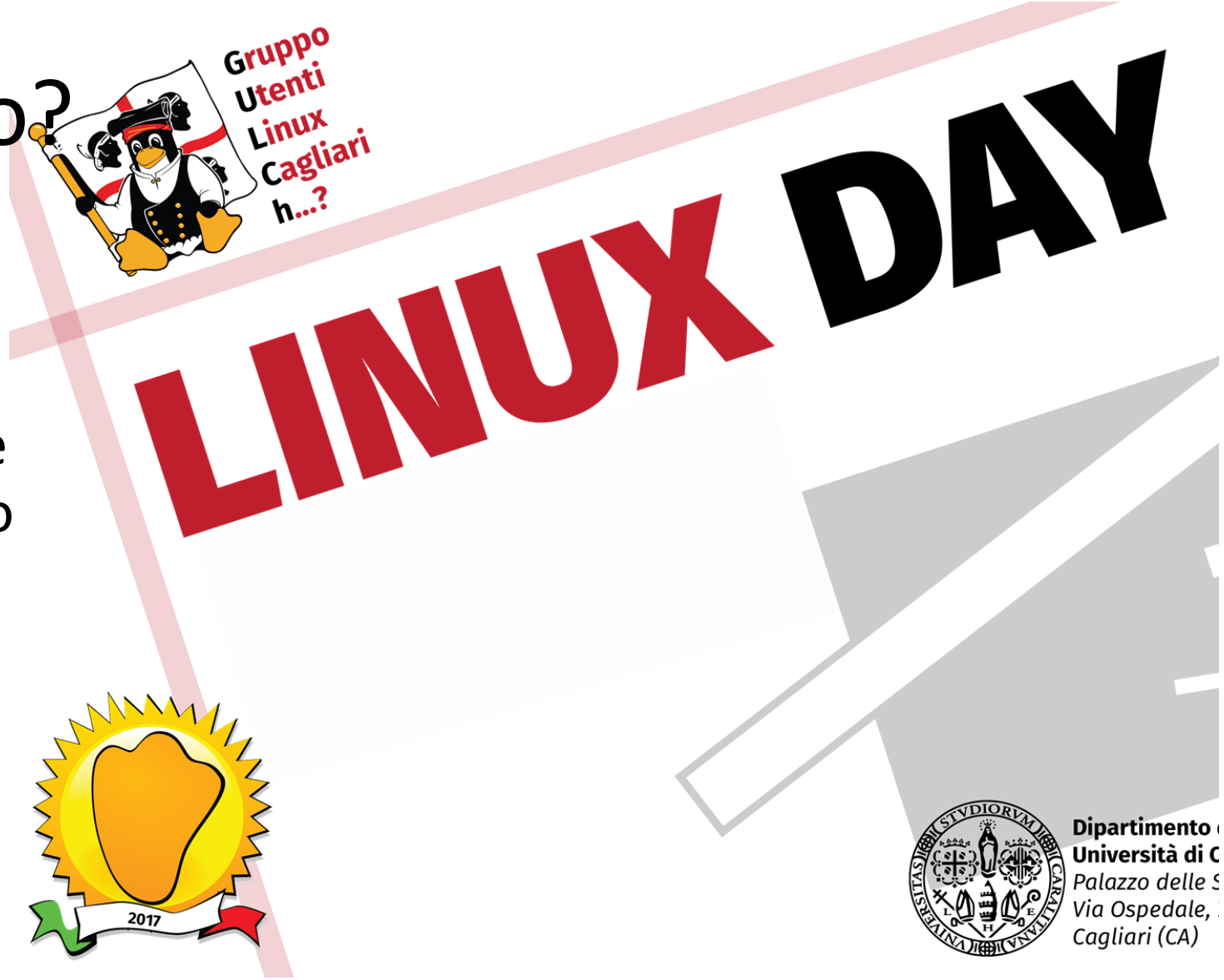
Oppure, tramite alcuni tools, gli utenti possono testare le proprie reti per verificarne la sicurezza, ma per grandi infrastrutture informatiche è sempre meglio contattare uno di questi esperti.



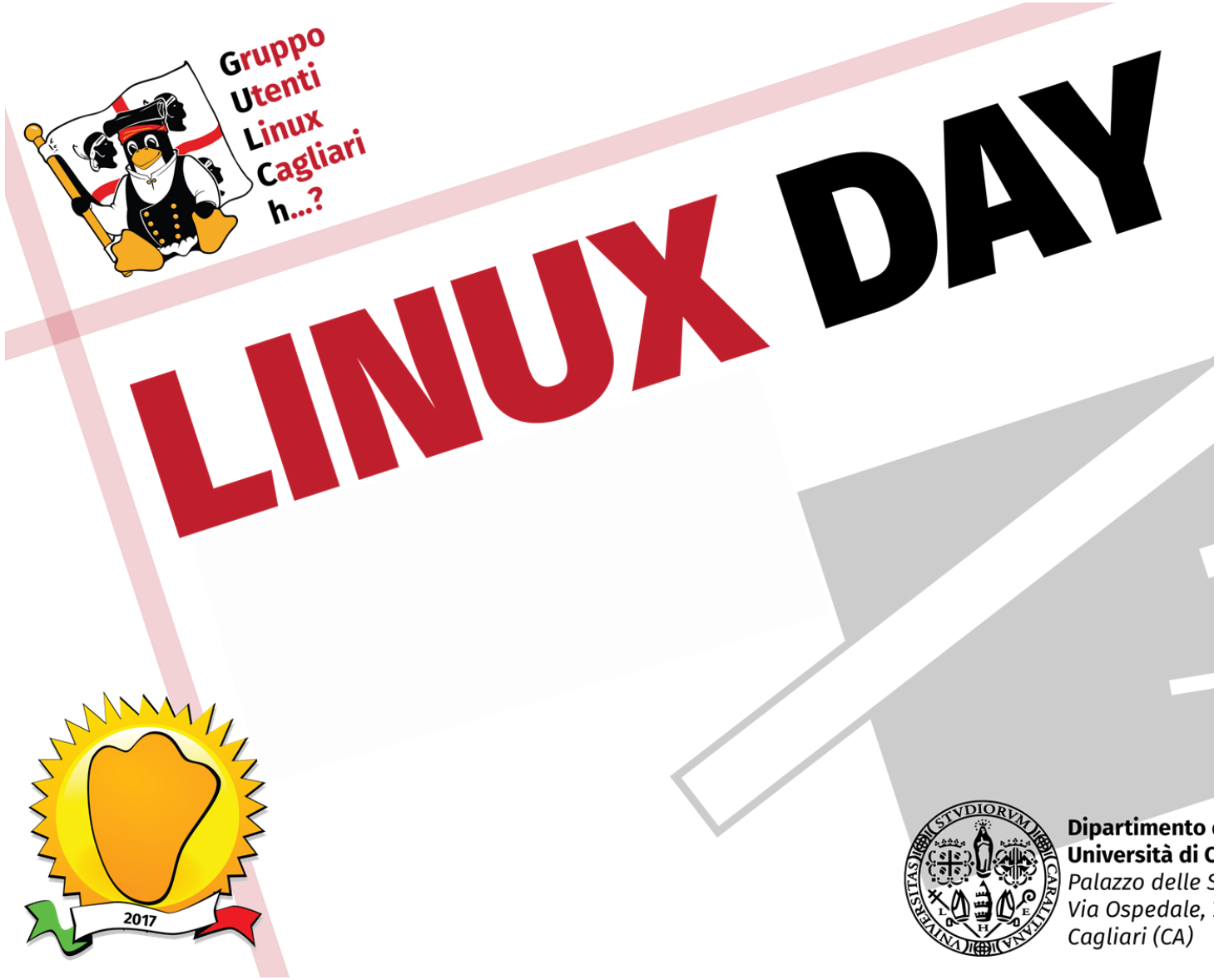
Come parte il tutto?

Troviamo 2 figure principali:

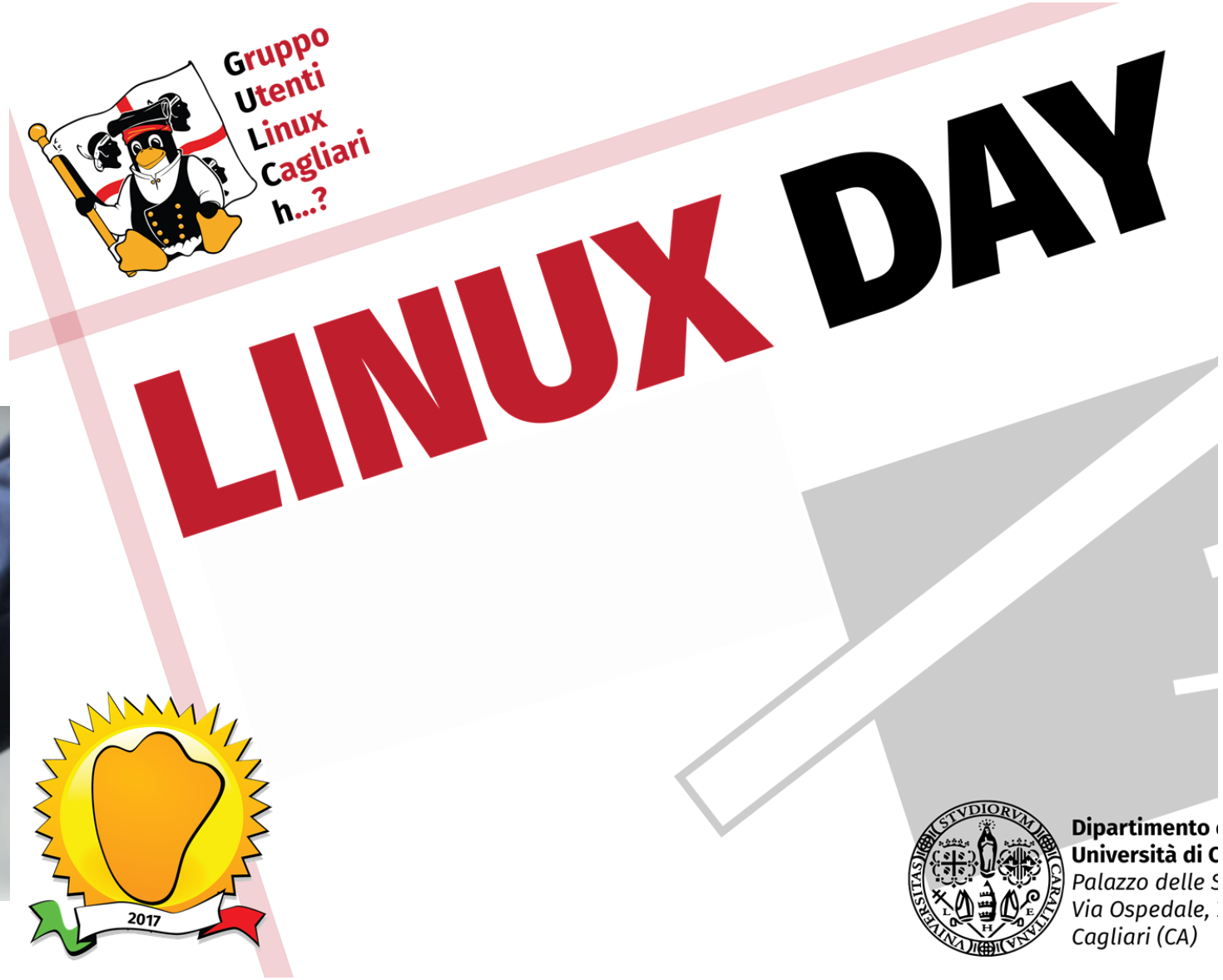
- Uno o un gruppo di dirigenti di una azienda che ha i suoi dati in un’apparato informatico;
- Un esperto o un gruppo di esperti nel trovare falle nei vari sistemi;



Il capo (o un dirigente incaricato alla sicurezza) pensa che sia il momento di fare un test per l'azienda.

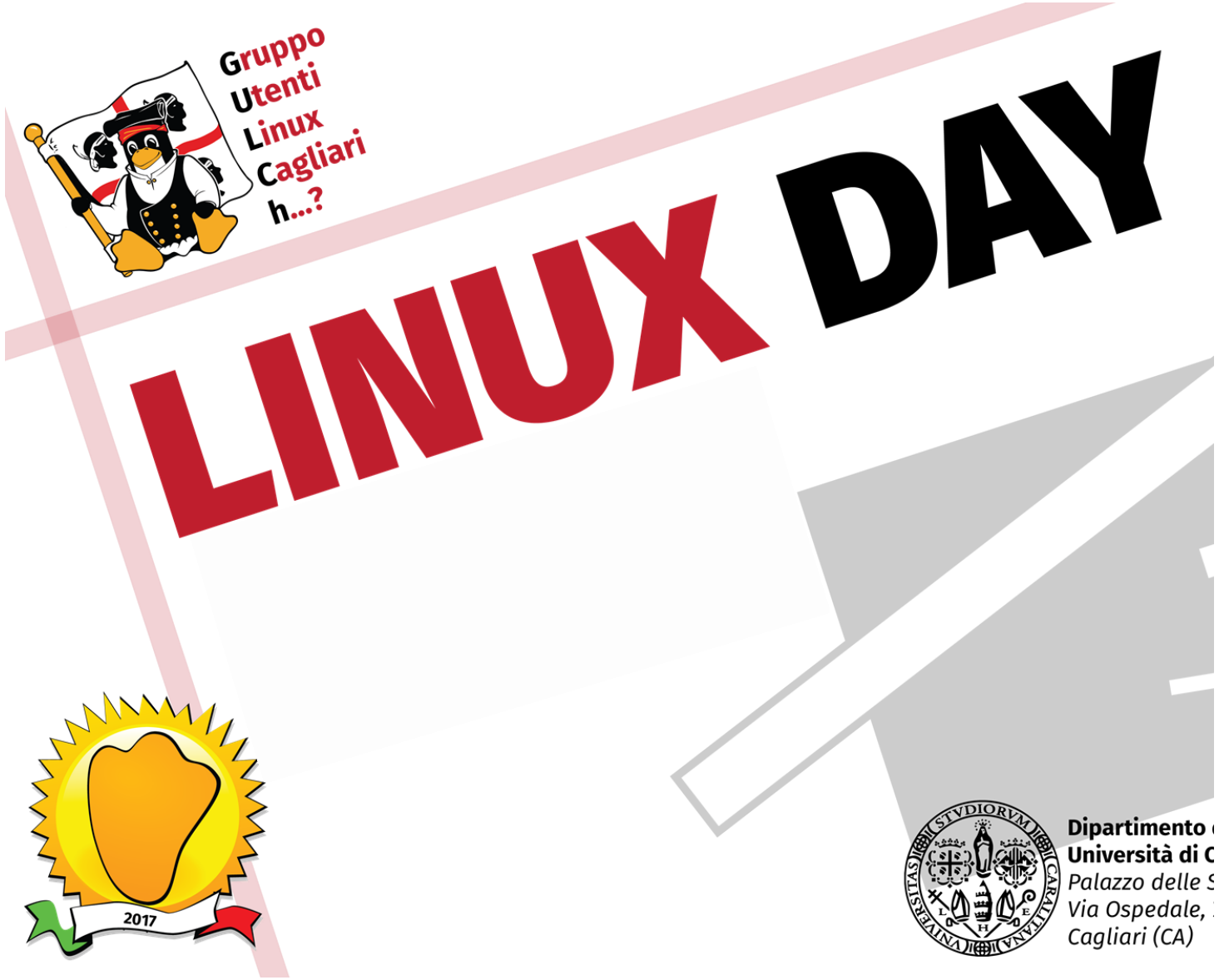


L’azienda stipula un contratto con il gruppo, o conl’esperto indipendente:



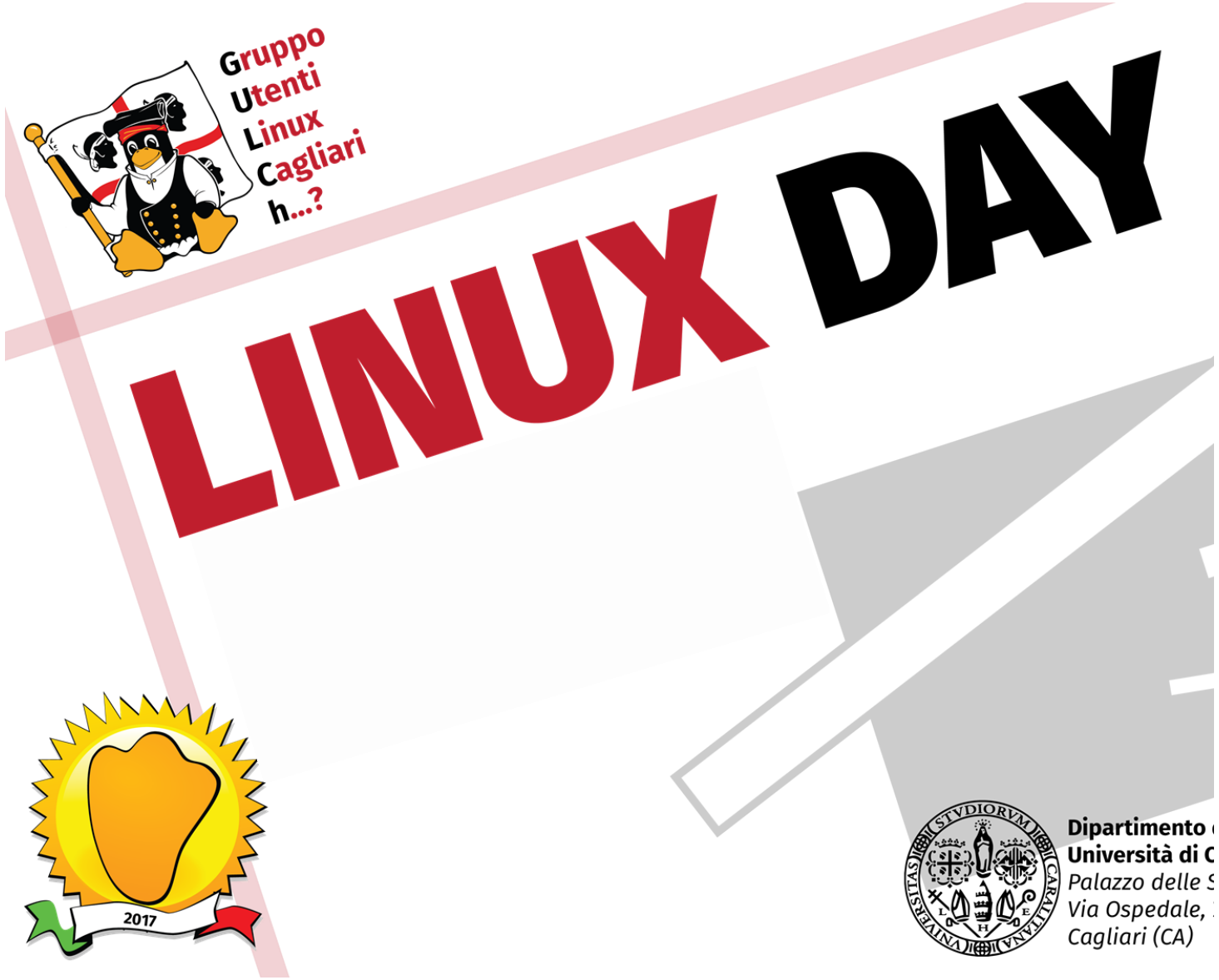
Cosa chiede un’azienda all’esperto?

Cosa chiede un esperto all’azienda?



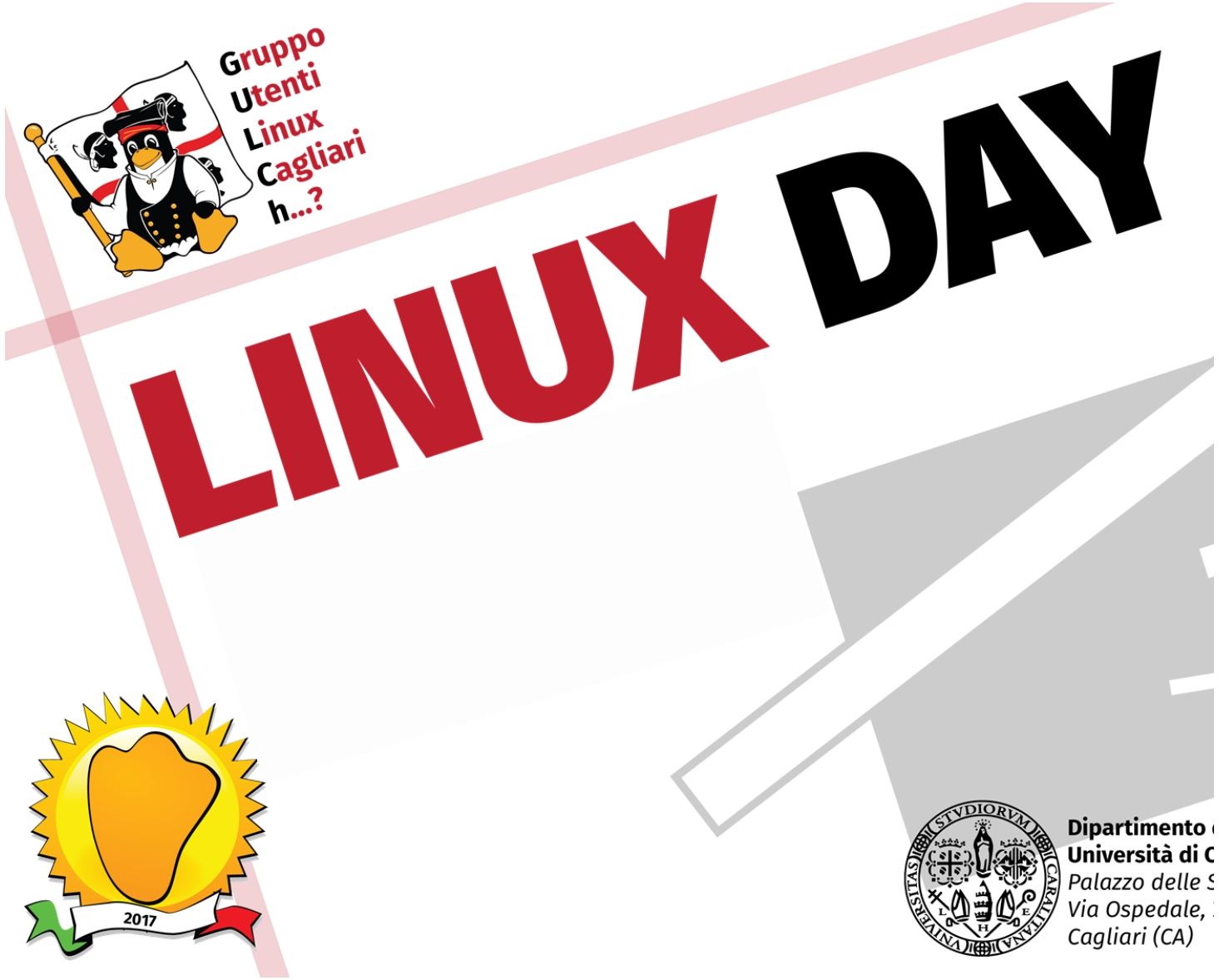
Cosa chiede un’azienda all’esperto?

Può chiedere che venga eseguito un certo tipo di attacco,a una certa posizione o macchina,in un certo tempo,per esempio.

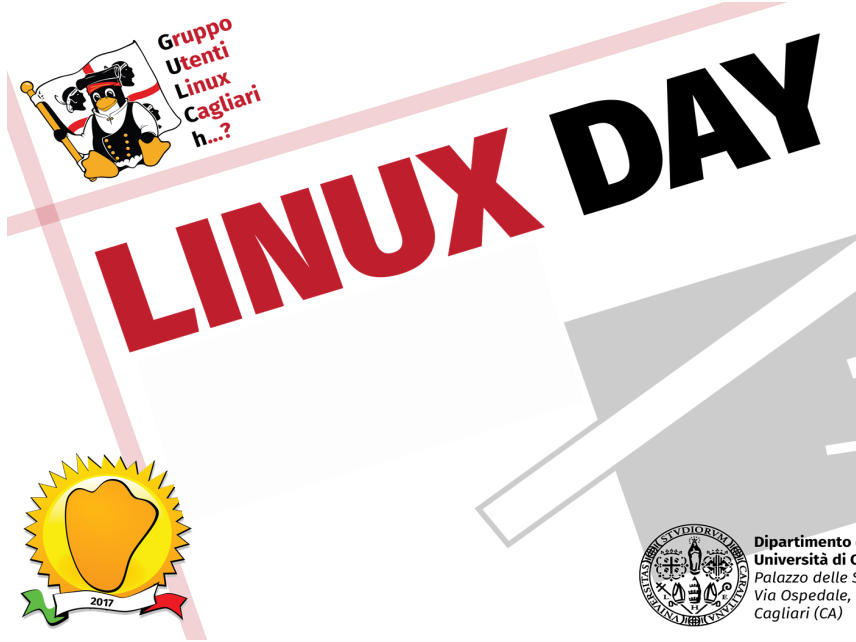


Cosa chiede un esperto all’azienda?

Può chiedere delle informazioni riguardo i sistemi operativi usati,o sulle versioni,per esempio.



Esistono 2 tipi di attacco:

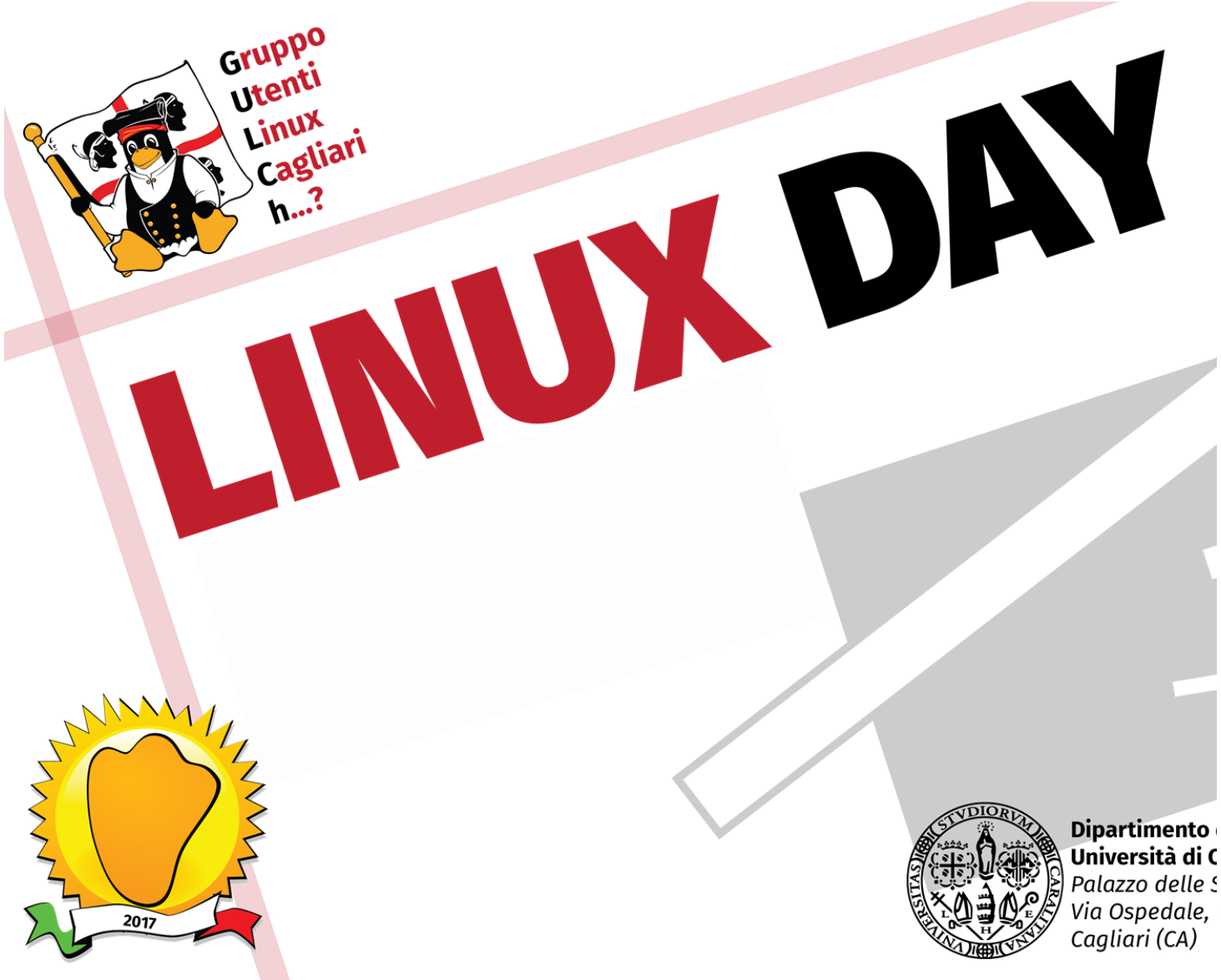


- Attacco sconosciuto,in cui nessuno viene avvisato sull’attacco,ma viene contata anche la reazione del corpo di sicurezza(Black Box);
- Attacco conosciuto,per testare la forza dei firewall o dei sistemi di difesa dell’infrastruttura(White Box);

È il giorno dell’attacco!

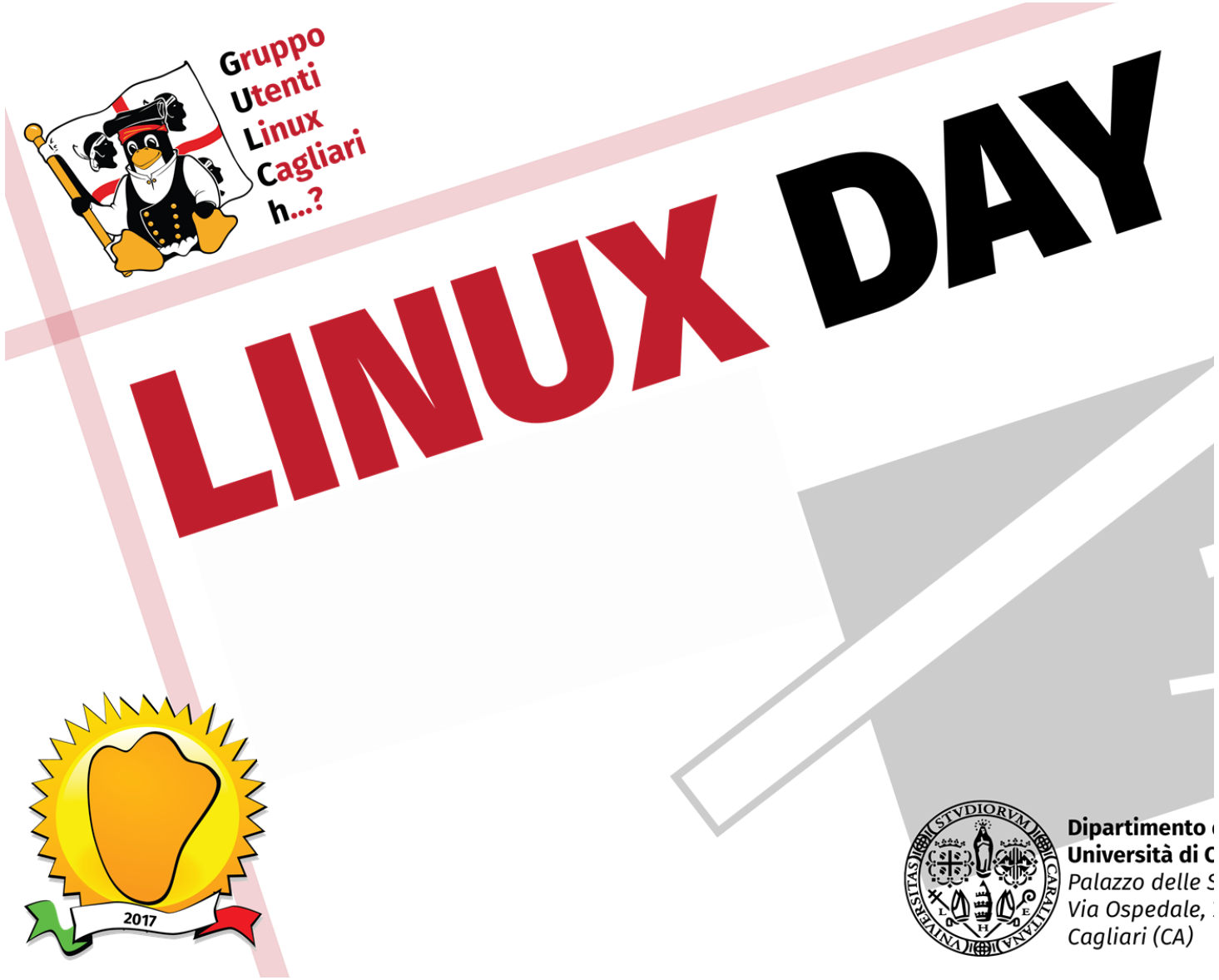
Ovviamente, bisogna seguire un piano:

- Scoprire le falle del sistema;
- Sfruttarle per accedere a dati sensibili o per azioni «malevoli»(exploit)
- Sviluppare un report;



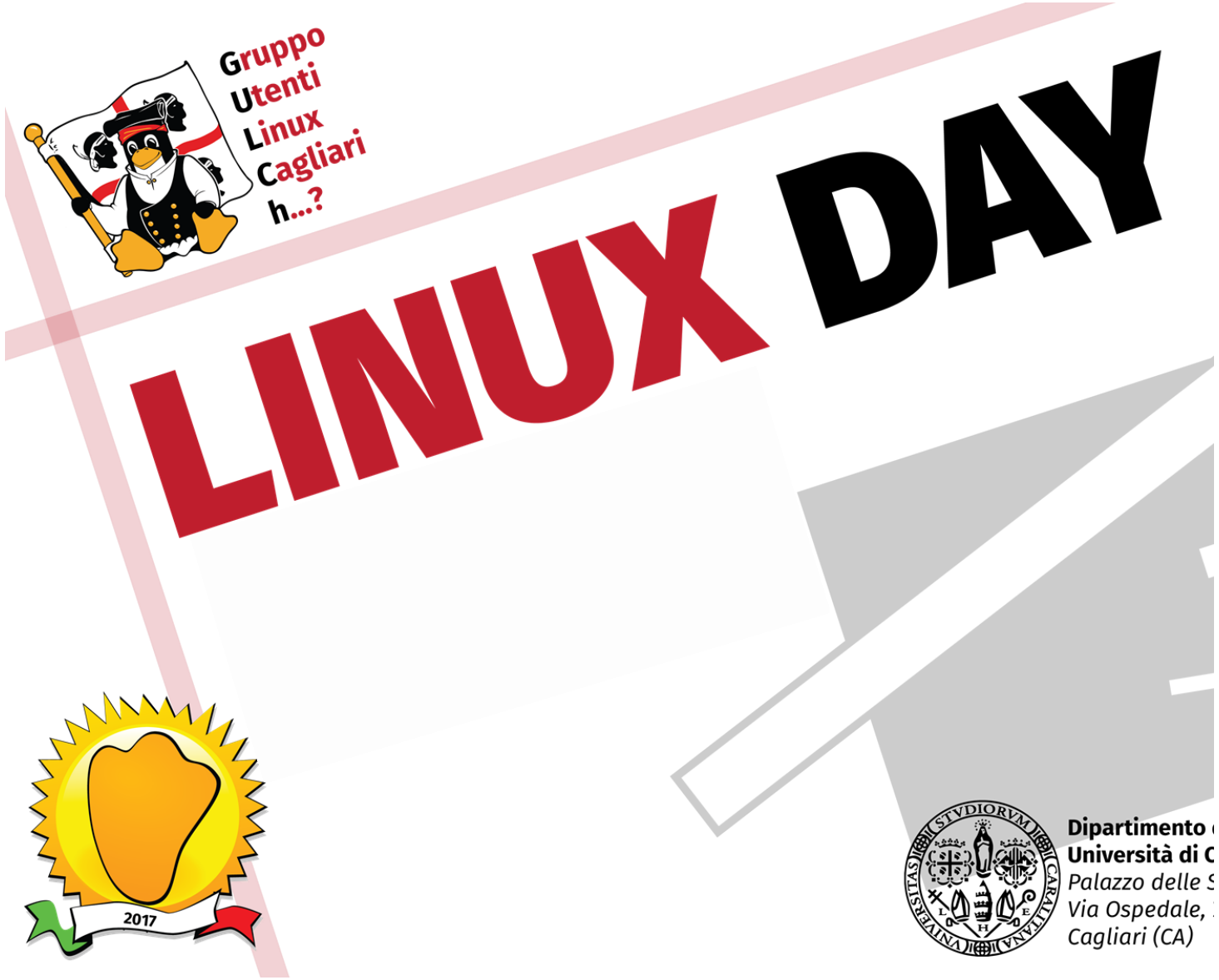
Cosa chiede un’azienda all’esperto?

Può chiedere che venga eseguito un certo tipo di attacco,a una certa posizione o macchina,in un certo tempo,per esempio.

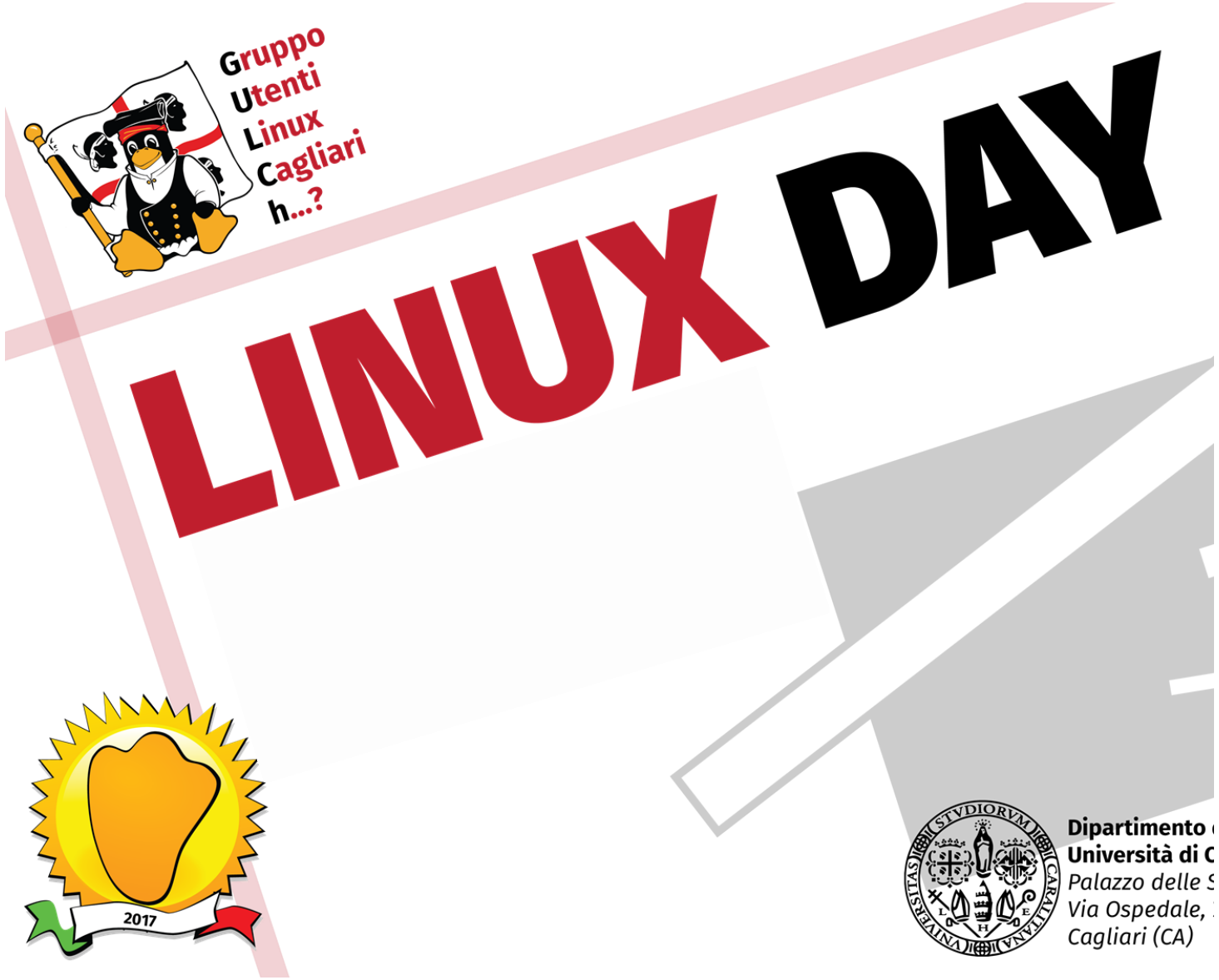


Le fasi dell’attacco

- Ricognizione di base: informazioni dal sito, informazioni sul dominio e sull'amministratore. A volte basta visitare il sito per raccogliere importanti notizie sul software presente sul server, spesso infatti in fondo all'home page i webmaster inseriscono notizie sul sistema operativo, webserver, etc. (Ad esempio Powered by Apache, Linux Inside...).
- Ricostruzione della struttura interna della rete.
- Una volta identificata la struttura della rete e il numero di macchine bisogna raccogliere il maggior numero di informazioni su ognuna di esse. Quindi occorre ricercare i servizi in esecuzione, identificare i sistemi operativi, la versione dei servizi, il tipo di processore, i nomi utente (standard e non), le risorse condivise, etc.



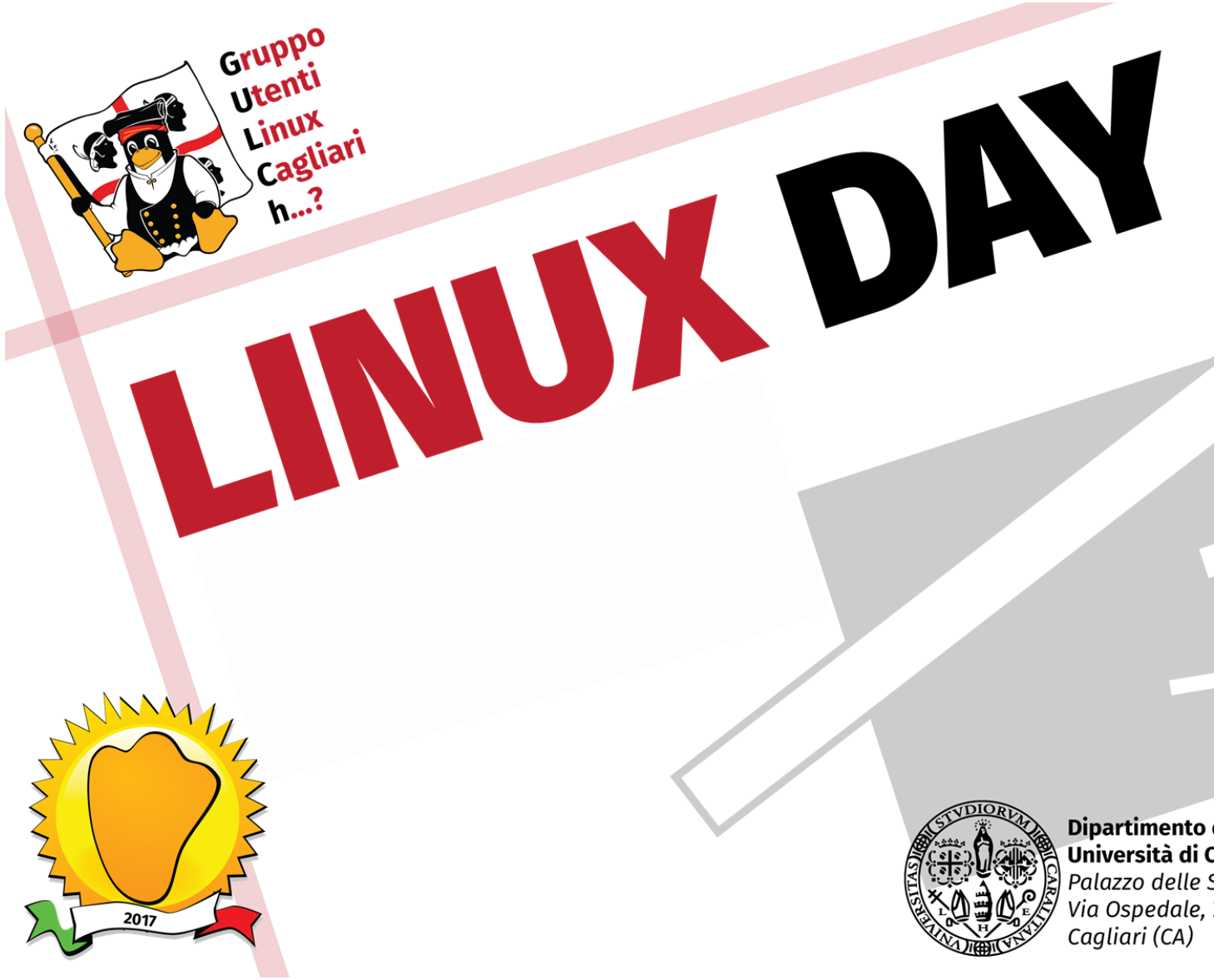
- Ricerca di eventuali misconfigurazioni.
- Dopo aver determinato i tipi di servizi attivi sull'host bersaglio si deve tracciare una mappa delle vulnerabilità, e occorre ricercare (o scrivere) gli exploit applicabili contro i servizi bersaglio.
- Analisi della topologia della rete.
- Applicazione degli exploit.
- Verifica della possibilità di sniffing e tentativi di DOS.
- Test su router e firewall.
- Pulizia delle tracce dell'attacco.
- Stesura del report.



Come scrivere un buon report

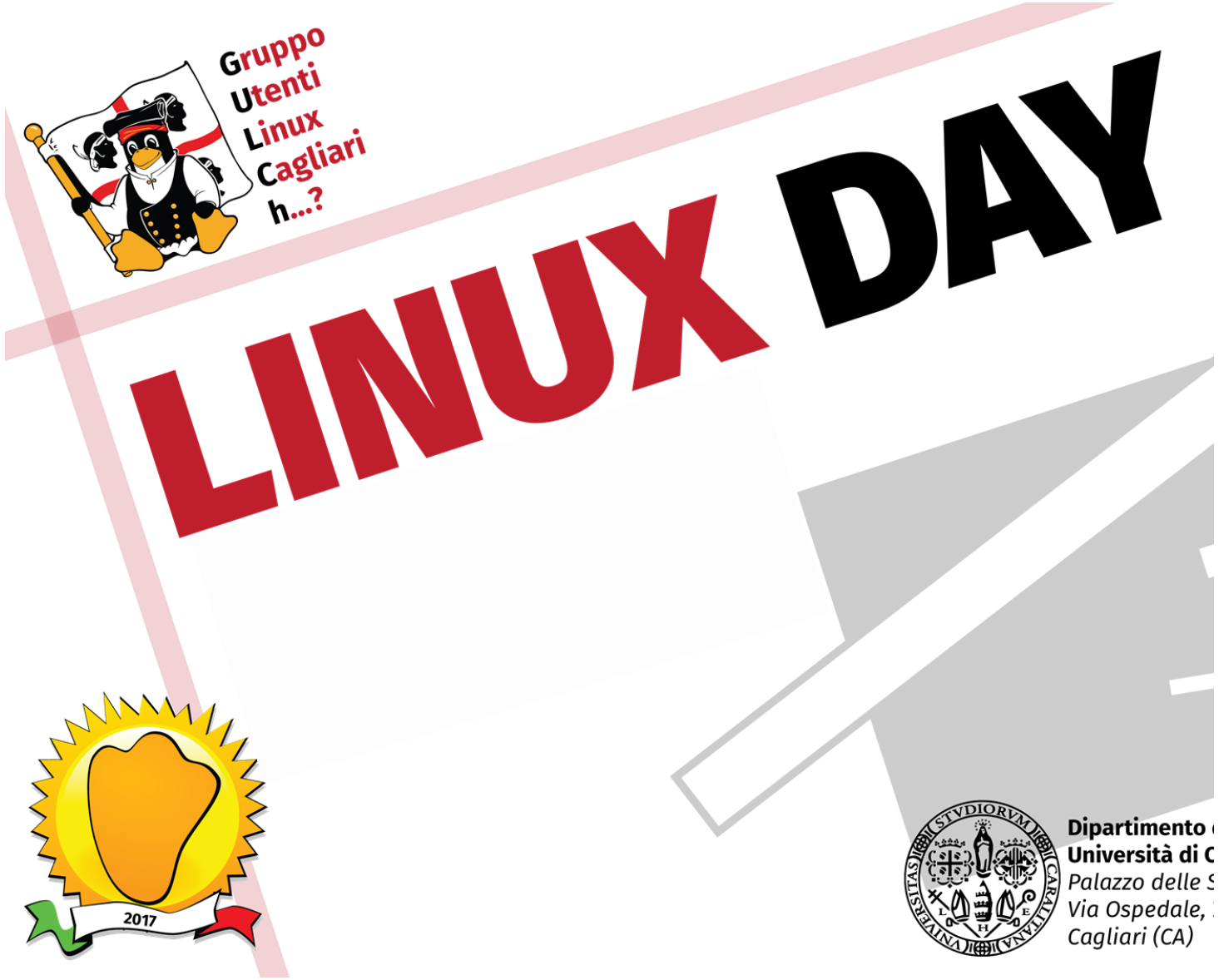
Il report è il documento che il team che esegue il test presenta al committente alla fine della valutazione.
Il report deve indicare per ogni vulnerabilità riscontrata:

- Software/dispositivo affetto dalla vulnerabilità (Nome e versione);
- Tipo di vulnerabilità riscontrata;
- Gravità del bug (Bassa, Media, Alta);
- Esistenza, diffusione e applicabilità dell'exploit relativo alla vulnerabilità;
- Causa (bug, configurazione, etc.);
- Macchine/dispositivi interessati;
- Conseguenze;
- Esistenza e complessità della soluzione del problema;
- Descrizione dettagliata del problema e dei metodi utilizzati per individuarlo;
- Suggerimenti e note.



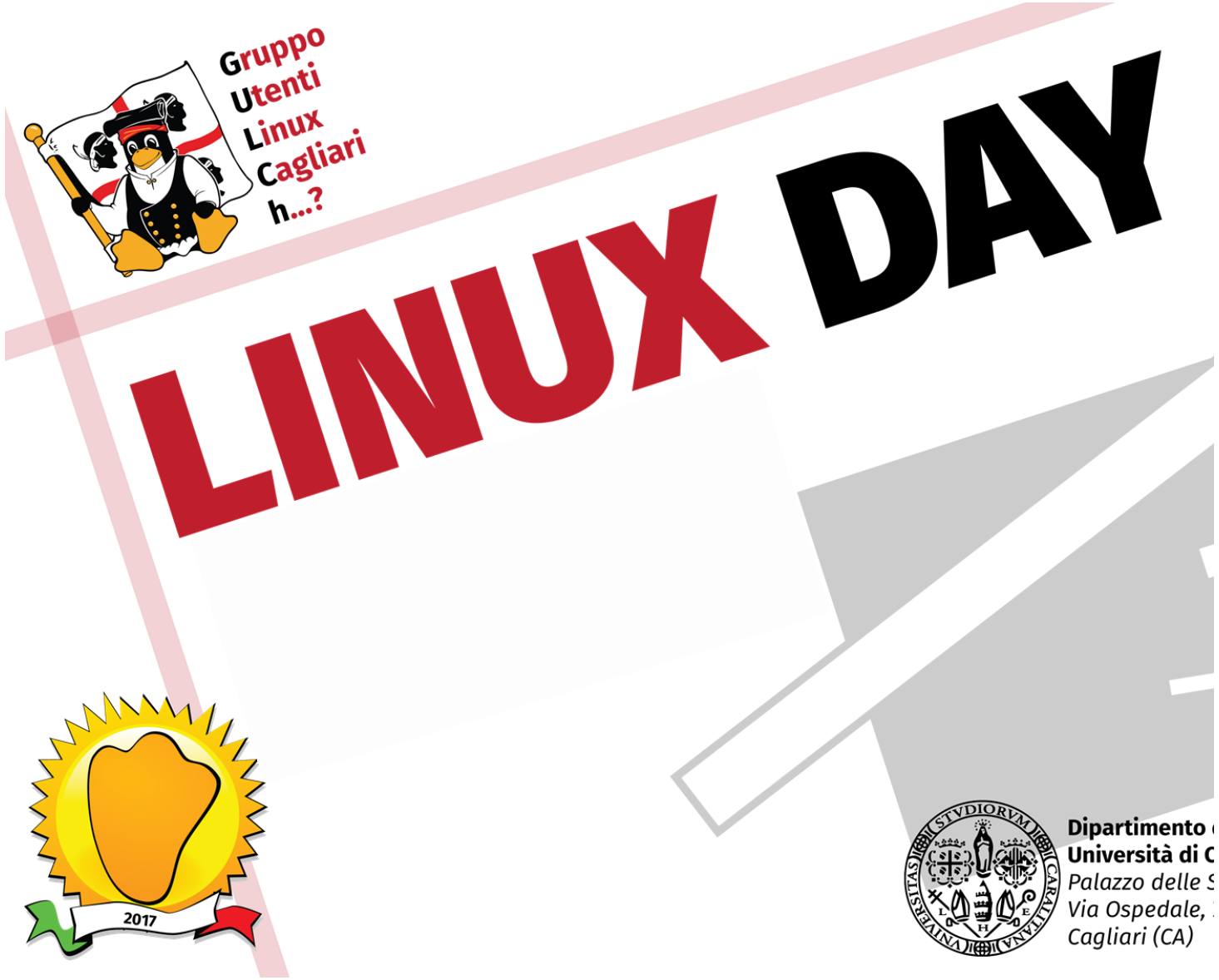
Le mie fonti:

- http://www.siforge.org/articles/2003/09/08-pentester.html
- https://www.slideshare.net/AlessandraZullo/le-fasi-di-un-penetration-testing
- https://onofri.org/security/cose-un-penetration-test/
- http://www.securityfocus.com/pen-test
- https://www.evilsocket.net/2016/10/02/Un-po-di-consigli-per-aspiranti-professionisti-del-settore-della-sicurezza-informatica/



I miei consigli:

- Internet è VOSTRO amico! Qualsiasi cosa non capiate cercatela sul vostro browser, qualsiasi vostro dubbio o qualsiasi cosa vogliate conoscere.
- Siate curiosi di imparare con umiltà.



DOMANDE? CURIOSITA'? SUGGERIMENTI PER L'ESPOSIZIONE PROSSIMA? DUBBI? NOTE?

Gruppo
Utenti
Linux
Cagliari
h...?

LINUX DAY

Dipartimento
Università di C
Palazzo delle S
Via Ospedale,
Cagliari (CA)