Customization of ArcherySec, opensoruce tool:
https://www.archerysec.com/
https://github.com/archerysec/archerysec/releases/
https://docs.archerysec.com/

New sections to be added to the left Menu
1. Shared folders: Nmap list of shared folders on the network, where the path is specified and whether they are protected by password or not
2. Reports: A general report of the vulnerabilities found at the time the report was produced. First page of the document must contain the executive summary, download pdf format, "send to" function to the email address to be entered and saved in the address book
3. Computer Risk Self-Assessment Questionnaire. A form divided into tabs that is filled in by the user with the aim of generating a report to download in pdf, for self-assessment (we will provide you with everything later)
4. Overview emails exposed in data breach by displaying the relative password (service such as google password where it tells you which accounts have been compromised and how / where). The emails to be monitored must be entered by us from the backend
5. User administrator logs: we want to keep track of who logs into archerysec and what they do
6. Network mapping at the graphic level: something that summarizes the structure of the network on a graphic level

Dashboard
1. Function with the possibility of choosing to send reports to an email address (to be entered manually and saved in the address book) with weekly or monthly recurring
2. Alerting new device connected to the network: a snapshot of the network is created and checks if there are new devices connected, if new ones are detected > flag that inserts new devices in the whitelist / new snapshot

Scanning
The result of the scan must be divided by rows containing the various hosts, the row in turn is divided into 4 columns:
- a column indicates the host
- a column indicates the fingerprinting or if it is a pc / printer / etc the type of OS etc open ports etc.
- a column displays the vulnerability CVE nr XXXX and indicates the details of the vulnerability, i.e. by exploiting this vulnerability an attacker can perform an XSS
- a column where the remedy plan is indicated, for example, “update the X-Content Type Options headers to fix this vulnerability”

Backend
1. Ability to enable / disable tools for users who for example do not need a web scan - disable nikto / owasp / etc with consequent integration / deletion from the general pdf report
2. Key activation management: only 1 user can register / access per key
3. In the scans section, replace the names of the tools used with a term that collects a macro-category: for example, replace OpenVas with Internal Network Scan
4. User Management, add-remove, view what they see from their frontend

HW Aspects
1. We will send to the users an T630 HP Thin Client with these specs: quadcore 4 threads 2,2ghz with a 256gb ssd and 8gb ddr4 ram in dual chan, where the tool will be installed. Can we somehow synchronize the devices using them as agents with our central server?
2. What if we want to install the archerysec tool / agent on a VM that the customer provides us?

At a graphic level we can leave everything like this, colors etc., we just have to replace the archerysec logo with our logo